Beste praktijken voor Catalyst 4500/4000, 5500/5000 en 6500/6000 Series Switches die CatOS-configuratie en -beheer uitvoeren

Inhoud

Gerelateerde informatie

Inleiding

Dit document behandelt de implementatie van de reeks switches van Cisco Catalyst in uw netwerk, in het bijzonder de Catalyst 4500/4000, 5500/5000 en 6500/6000 platforms. Configuraties en opdrachten worden besproken onder de veronderstelling dat u Catalyst OS (CatOS) Algemene implementatiesoftware 6.4(3) of hoger gebruikt. Hoewel een aantal ontwerpoverwegingen worden gepresenteerd, wordt in dit document niet ingegaan op het algehele ontwerp van de campus.

Voorwaarden

Vereisten

Dit document vertrouwt op de Catalyst 6500 Series Opdrachtreferentie, 7.6.

Hoewel in het document verwijzingen naar online openbaar materiaal voor verdere lezing zijn opgenomen, zijn dit andere fundamentele en educatieve verwijzingen:

- Cisco ISP— Essentiële IOS functies die elke ISP moet overwegen.
- Cisco-richtsnoeren voor netwerkbewaking en correlatie van gebeurtenissen
- Gigabit Campus-netwerkontwerp — Principes en architectuur
- Cisco VEILIG: Een security blauwdruk voor ondernemingsnetwerken

Gebruikte componenten

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

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Deze oplossingen vertegenwoordigen jaren ervaring van Cisco ingenieurs die met veel van onze grootste klanten en complexe netwerken 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 de breedste blootstelling in het veld hebben, en dus het laagste risico.
- Oplossingen die eenvoudig zijn, die enige flexibiliteit voor deterministische resultaten verhandelen.
- Oplossingen die eenvoudig te beheren en te configureren zijn door teams van netwerkbewerkingen.
- Oplossingen die een hoge beschikbaarheid en hoge stabiliteit bevorderen.

Dit document bestaat uit de volgende vier delen:

- Basic Configuration: functies die worden gebruikt door een meerderheid van netwerken zoals Spanning Tree Protocol (STP) en trunking.
- Management Configuration: ontwerpoverwegingen in combinatie met systeem- en eventbewaking met behulp van Simple Network Management Protocol (SNMP), Remote Monitoring (RMON), Syscène, Cisco Discovery Protocol (CDP) en Network Time Protocol (NTP).
- Security Configuration: wachtwoorden, poortbeveiliging, fysieke beveiliging en verificatie met behulp van TACACS+.
- Configuratiescherm — samenvatting van de voorgestelde configuratiesjablonen.

Basisconfiguratie

De eigenschappen die met het merendeel van de Catalyst netwerken worden uitgevoerd worden in deze sectie besproken.

Catalyst-besturingsplane-protocollen

In dit hoofdstuk worden protocollen geïntroduceerd die tussen switches worden uitgevoerd bij normaal gebruik. Een basisbegrip van deze protocollen is nuttig voor de aanpak van elk onderdeel.

supervisor traffic

De meeste eigenschappen die in een netwerk van Catalyst worden toegelaten vereisen twee of meer switches om samen te werken, dus moet er een gecontroleerde uitwisseling van de keeplevingsberichten, configuratieparameters, en beheerveranderingen zijn. Of deze protocollen eigen zijn van Cisco, zoals CDP, of op standaarden gebaseerd, zoals IEEE 802.1d (STP), hebben allen bepaalde elementen gemeenschappelijk wanneer geïmplementeerd op de Catalyst serie.

In het basisframe door-sturen komen de gebruikersgegevensframes uit eindsystemen en worden hun bronadres en doeladres niet gewijzigd in Layer 2 (L2) switched domeinen. Content Adresseerbare Memory (CAM) lookup-tafels op elke switch Supervisor Engine zijn bevolkt door een bronadresleerproces en geven aan welke uitgang elk ontvangen frame moet doorsturen. Als het proces van het adresleren onvolledig is (de bestemming is onbekend of het kader is bestemd voor een uitzending of multicast adres) wordt het doorgestuurd (overstroomd) uit alle havens in dat VLAN.

De switch moet ook herkennen welke frames door het systeem moeten worden geschakeld en die op de switch CPU zelf moeten worden gericht (ook bekend als Network Management Processor [NMP]).

Het Catalyst-besturingsplane wordt gemaakt met behulp van speciale items in de CAM-tabel die **systeemitems** worden genoemd, om op een interne switch poort verkeer naar het NMP te ontvangen en te sturen. Dus door protocollen met bekende MAC-adressen van de bestemming te gebruiken, kan het besturingsplane-verkeer worden gescheiden van het gegevensverkeer. Laat de opdracht CAM-systeem **op een switch zien om dit te bevestigen, zoals wordt getoond:**

```
>show cam system

* = Static Entry. + = Permanent Entry. # = System Entry. R = Router Entry.
X = Port Security Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ----------------------------------------
1     00-d0-ff-88-cb-ff  #          1/3
!--- NMP internal port. 1 01-00-0c-cc-cc-cc # 1/3 !--- CDP and so on. 1 01-00-0c-cc-cc-cd # 1/3
!--- Cisco STP. 1 01-80-c2-00-00-00 # 1/3 !--- IEEE STP. 1 01-80-c2-00-00-01 # 1/3 !--- IEEE
flow control. 1 00-03-6b-51-e1-82 R# 15/1 !--- Multilayer Switch Feature Card (MSFC) router. ...
```

Cisco heeft een gereserveerde reeks Ethernet MAC- en protocoladressen, zoals getoond. Elk document wordt later in dit document behandeld. In deze tabel wordt echter een samenvatting gegeven voor het gemak.

Functie	SNAP HDLC-protocoltype	Destination Multicast MAC
Port Aggregation Protocol (PAgP)	0x0104	01-00-0c-cc-cc-cc
Spanning Tree PVSTP+	0x010b	01-00-0c-cc-cc-cd
VLAN-brug	0x010c	01-00-0c-cd-cd-ce
Unidirectional Link Detection (UDLD)	0x011	01-00-0c-cc-cc-cc
Cisco-detectieprotocol	0x2000	01-00-0c-cc-cc-cc
Dynamic Trunking (DTP)	0x2004	01-00-0c-cc-cc-cc
Snel STP-uplinks	0x200a	01-00-0c-cd-cd
IEEE Spanning Tree 802.1d	N.B. - DSAP 42 SAP 42	01-80-c2-00-00-00
Inter Switch Link (ISL)	N.v.t.	01-00-0c-00-00-00
VLAN Trunking (VTP)	0x203	01-00-0c-cc-cc-cc
IEEE Pauze, 802.3x	NVR.: DSAP 81 SAP 80	01-80-C2-00-00-00>0F

De meerderheid van de controleprotocollen van Cisco gebruikt een insluiting van IEEE 802.3, met inbegrip van **LLC 0xAAA03, OUI 0x0000C**, die op een spoor van een LAN-analyzer kan worden gezien. Andere gemeenschappelijke eigenschappen van deze protocollen zijn:

- Deze protocollen gaan uit van point-to-point connectiviteit. Merk op dat het opzettelijke gebruik van multicast doeladressen twee Catalyst's in staat stelt om op transparante wijze te communiceren over niet-Cisco switches, als apparaten die de frames niet begrijpen en onderscheppen ze eenvoudigweg overspoelen. Echter, point-to-multipoint aansluitingen door meerdere leveranciers kunnen leiden tot inconsequent gedrag en moeten over het algemeen worden vermeden.
- Deze protocollen eindigen op Layer 3 (L3) routers; zij werken alleen binnen een switch domein .
- Deze protocollen krijgen prioriteit boven gebruikersgegevens door toepassingsspecifieke

geïntegreerde schakeling (ASIC) te verwerken en te plannen.

Na de invoering van de bestemmingsadressen van het controleprotocol moet het bronadres ook voor de volledigheid worden beschreven. Switch protocollen gebruiken een MAC-adres dat is overgenomen van een bank met beschikbare adressen die door een EPROM op het chassis zijn verstrekt. Geef de opdracht Show module uit **om de adresbereiken die beschikbaar zijn aan elke module weer te geven wanneer het verkeer zoals STP bridge protocol data units (BPDU's) of ISL frames binnenhaalt.**

```
>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
!--- MACs for sourcing traffic. ... VLAN 1
```

VLAN 1

VLAN 1 heeft een speciale betekenis in Catalyst netwerken.

De Catalyst Supervisor Engine gebruikt altijd de standaard VLAN, VLAN 1, om een aantal controle- en beheerprotocollen te taggen bij trunking, zoals CDP, VTP en PAgP. Alle poorten, inclusief de interne sc0 interface, worden standaard ingesteld om leden van VLAN 1 te zijn. Alle stammen dragen VLAN 1 standaard, en in CatOS softwareversies eerder dan 5.4 was het niet mogelijk om gebruikersgegevens in VLAN 1 te blokkeren.

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

- Het beheer VLAN is waar sc0 verblijft; Dit VLAN kan worden gewijzigd.
- Het inheemse VLAN wordt gedefinieerd als VLAN waaraan een haven wanneer niet trunking terugkeert, en is het niet gelabelde VLAN op een 802.1Q stam. Standaard is VLAN 1 het native VLAN.
- Om het native VLAN te veranderen, geeft u de ingestelde VLAN-VLAN-*id mod/poort* opdracht uit.**Opmerking:** Maak het VLAN voordat u dit instelt als het inheemse VLAN van de stam.

Dit zijn verscheidene 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 (vooral vanuit een STP perspectief) te zijn moet het terug worden gedrukt. Dit wordt in het gedeelte In-band beheer van dit document uitvoerig besproken.
- De gegevens van het besturingsplane op VLAN 1 moeten gescheiden worden gehouden van de gebruikersgegevens om de probleemoplossing te vereenvoudigen en de beschikbare CPU-cycli te maximaliseren.
- L2 loops in VLAN 1 moet worden vermeden wanneer de netwerken van de meerlaagse campus zonder STP worden ontworpen, en trunking is nog vereist aan de toegangslaag als er meerdere VLAN's en IP subnetten zijn. Om dit te doen, wissel VLAN 1 van boomstampoorten handmatig uit.

Samengevat kan deze informatie over stammen worden aangetroffen:

- **CDP, VTP en PAgP** updates worden altijd op trunks doorgestuurd met een VLAN 1 tag. Dit is het geval zelfs als VLAN 1 van de trunks wordt ontruimd en niet het inheemse VLAN is. Als VLAN 1 voor gebruikersgegevens wordt gewist, is dit geen invloed op het verkeer van het controlevliegtuig dat nog steeds wordt verzonden met VLAN 1.
- Op een ISL romp, worden de pakketten DTP op VLAN1 verzonden. Dit is de zaak zelfs als VLAN 1 van de boomstam wordt 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 wordt ontruimd.
- In PVST+, worden de **802.1Q IEEE BPDU's** untagged op de gemeenschappelijke Spanning Tree VLAN 1 verzonden voor interoperabiliteit met andere verkopers, tenzij VLAN 1 van de stam wordt gewist. Dit is het geval ongeacht de native VLAN-configuratie. **Cisco PVST+ BPDU's** worden verzonden en gelabeld voor alle andere VLAN's. Raadpleeg de sectie Spanning Tree Protocol in dit document 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 gewist.
- 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-brug kunnen vermijden om haar grenspoorten in de root-inconsistente staat te plaatsen. Raadpleeg het gedeelte Multiple Spanning Tree Protocol (802.1s) voor meer informatie.

Aanbevelingen

Om een VLAN in een **up/up** staat te houden zonder cliënten of hosts die in dat VLAN zijn aangesloten, moet u ten minste één fysiek apparaat hebben dat in dat VLAN is aangesloten. Anders heeft VLAN een **Up/Down** status. Op dit moment is er geen opdracht om een VLAN-interface **omhoog/omhoog** te zetten wanneer er geen actieve poorten in de switch voor dat VLAN zijn.

Als u geen apparaat wilt aansluiten, sluit u een loopback stekker in een poort voor dat VLAN aan. Als alternatief probeer een cross-over kabel die twee poorten in dat VLAN op dezelfde switch verbindt. Met deze methode wordt de haven naar boven geduwd. Raadpleeg het gedeelte Loopback Plug van Loopback Tests voor T1/56K lijnen voor meer informatie.

Wanneer een netwerk aan dienstverleners wordt gemultiformeerd, fungeert het netwerk als een doorvoernetwerk tussen twee dienstverleners. Als het VLAN-nummer dat in een pakket wordt ontvangen, moet worden vertaald of gewijzigd wanneer het van de ene serviceprovider naar de andere wordt doorgegeven, is het raadzaam de QinQ-functie te gebruiken om het VLAN-nummer te vertalen.

VLAN-trunkingprotocol

Voordat u VLAN's maakt, bepaalt u de VTP-modus die in het netwerk wordt gebruikt. VTP maakt het mogelijk om de configuratie van VLAN centraal op een of meer switches te veranderen. Deze veranderingen propageren automatisch voor alle andere switches in het domein.

Overzicht

VTP is een L2 berichtenprotocol dat de configuratie van VLAN constant houdt. VTP beheert de toevoeging, het wissen en het hernoemen van VLAN's op een netwerkbrede basis. VTP minimaliseert foute configuraties en configuratie inconsistenties die een aantal problemen kunnen veroorzaken, zoals duplicaat VLAN-namen, onjuiste VLAN-type specificaties en security schendingen. De VLAN-database is een binair bestand en wordt in NVRAM op VTP-servers afzonderlijk van het configuratiebestand opgeslagen.

Het VTP-protocol communiceert tussen switches die een Ethernet-bestemming multicast MAC-adres (**01-00c-cc-cc**) en SNAP HDLC-protocol type Ox2003 gebruiken. Het werkt niet via niet-kofferpoorten (VTP is een payload van ISL of 802.1Q), zodat berichten niet kunnen worden verstuurd DTP heeft de kofferbak online gezet.

Berichttypen bevatten beknopte advertenties om de vijf minuten, subset advertenties en aanvragen advertenties wanneer er wijzigingen zijn, en sluiten zich aan bij het afdrukken van VTP-uitloop. Het versienummer van de VTP-configuratie wordt met elke verandering op een server verhoogd, dat vervolgens de nieuwe tabel over het domein verspreidt.

Als een VLAN wordt verwijderd, worden poorten die ooit een lid van dat VLAN waren in een inactieve staat geplaatst. Op dezelfde manier worden als een switch in clientmodus niet in staat is de VTP VLAN-tabel bij het opstarten te ontvangen (van een VTP-server of een andere VTP-client) alle poorten in VLAN's anders dan de standaard VLAN 1 gedeactiveerd.

Deze tabel biedt een samenvatting van de functievergelijking voor verschillende VTP-modi:

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

In VTP `transparante` modus worden VTP-updates genegeerd (het VTP multicast MAC-adres wordt verwijderd van het systeem CAM dat normaal gebruikt wordt om controleframes op te halen en deze naar de Supervisor Engine te sturen). Aangezien het protocol een multicast adres gebruikt, wordt het kader door een switch in transparante modus (of een andere switch van een verkoper) simpelweg overspoeld naar andere switches van Cisco in het domein.

[1] CatOS softwarerelease 7.1 introduceert de optie om VTP uit te schakelen met behulp van de

`uit`-modus. In VTP `uit`-modus, gedraagt de switch zich op een manier die sterk lijkt op de VTP `transparante` modus, behalve dat `uit`-modus ook het doorsturen van VTP-updates onderdrukt.

In deze tabel wordt een samenvatting van de configuratie gegeven:

Functie	Standaardwaarde
VTP-domeinnaam	leeg
VTP-modus	Server
VTP-versie	Versie 1 is ingeschakeld
VTP-wachtwoord	None
VTP-trunking	Uitgeschakeld

VTP versie 2 (VTPv2) omvat deze functionele flexibiliteit. Het is echter niet interoperabel met VTP versie 1 (VTPv1):

- Ondersteuning van Token Ring
- Niet-herkende VTP-informatieondersteuning switches propageren nu waarden die ze niet kunnen parseren.
- Versiegerelateerde transparante modus; `de transparante` modus controleert niet langer de domeinnaam. Dit maakt ondersteuning van meer dan één domein via een transparant domein mogelijk.
- vermeerdering van versienummer; als VTPv2 op alle switches mogelijk is, kunnen allen door de configuratie van één enkele switch worden geactiveerd.

Raadpleeg Understanding en het configureren van VLAN Trunk Protocol (VTP) voor meer informatie.

VTP versie 3

CatOS-softwarerelease 8.1 biedt ondersteuning voor VTP versie 3 (VTPv3). VTPv3 biedt verbeteringen via de bestaande versies. Deze verbeteringen maken het mogelijk:

- Ondersteuning voor uitgebreide VLAN's
- Ondersteuning voor de creatie en advertentie van particuliere VLAN's
- Ondersteuning voor VLAN-instanties en MST-mapping-propagatievormen (die worden ondersteund in CatOS-release 8.3)
- Verbeterde serververificatie
- Bescherming tegen accidentele opname van de "verkeerde" database in een VTP-domein
- Interactie met VTPv1 en VTPv2
- De mogelijkheid om per poort te worden ingesteld

Een van de belangrijkste verschillen tussen de VTPv3-implementatie en de eerdere versie is de introductie van een VTP-primaire server. Idealiter moet er slechts één primaire server in een VTPv3 domein zijn als het domein niet gepartitioneerd is. Alle wijzigingen die u aan het VTP-domein aanbrengt, moeten op de VTP-primaire server worden uitgevoerd om naar het VTP-domein te kunnen worden gepropageerd. Er kunnen meerdere servers zijn binnen een VTPv3-domein, dat ook bekend staat als secundaire servers. Wanneer een switch is ingesteld als een server, wordt de switch standaard een secundaire server. De secondaire server kan de configuratie van het domein opslaan maar kan de configuratie niet wijzigen. Een secundaire server kan de primaire server worden met een succesvolle overname van de switch.

Switches die VTPv3 uitvoeren aanvaarden alleen een VTP-database met een hoger revisienummer dan de huidige primaire server. Dit proces verschilt aanzienlijk van VTPv1 en VTPv2, waarin een switch altijd een superieure configuratie van een buurman in hetzelfde domein accepteert. Deze verandering met VTPv3 biedt bescherming. Een nieuwe switch die in het netwerk met een hoger versienummer VTP wordt geïntroduceerd kan de configuratie van VLAN van het volledige domein niet overschrijven.

VTPv3 introduceert ook een verbetering van de manier waarop VTP wachtwoorden verwerkt. Als u de optie voor het verbergen van de wachtwoordconfiguratie gebruikt om het wachtwoord als "verborgen" te configureren, worden deze items uitgevoerd:

- Het wachtwoord wordt niet in onbewerkte tekst in de configuratie weergegeven. Het geheime hexadecimale formaat van het wachtwoord wordt in de configuratie opgeslagen.
- Als u de switch als een primaire server probeert te configureren wordt u om het wachtwoord gevraagd. Als uw wachtwoord met het geheime wachtwoord overeenkomt, wordt de switch een primaire server, waarmee u het domein kunt configureren.

Opmerking: het is belangrijk om op te merken dat de primaire server alleen nodig is als u de VTP-configuratie voor een willekeurig geval moet wijzigen. Een VTP-domein kan zonder actieve primaire server werken omdat de secundaire servers een continue configuratie boven herladingen garanderen. De primaire serverstaat is om deze redenen verlaten:

- Een herlading van de switch
- Een overschakeling op hoge beschikbaarheid tussen de actieve en redundante toezichthouder-motoren
- Een overname van een andere server
- Een verandering in de configuratie van de modus
- Elke verandering in VTP-domeinconfiguratie, zoals een verandering in:VersieDomeinnaamDomain password

VTPv3 stelt de switches ook in staat om deel te nemen aan meerdere gevallen van VTP. In dit geval kan dezelfde switch de VTP-server zijn voor één instantie en een client voor een andere instantie, omdat de VTP-modi specifiek zijn voor verschillende VTP-instanties. Een switch kan bijvoorbeeld in `transparante` modus werken voor een MST-instantie terwijl de switch in `server`-modus is ingesteld voor een VLAN-instantie.

In termen van interactie met VTPv1 en VTPv2 is het standaardgedrag in alle versies van VTP geweest dat de eerdere versies van VTP simpelweg de nieuwe versies van de updates laten vallen. Tenzij de VTPv1- en VTPv2-switches in `transparante` modus zijn, worden alle VTPv3-updates ingetrokken. Aan de andere kant, nadat VTPv3 switches een erfenis VTPv1 of VTPv2 frame op een stam ontvangen, gaan de switches een geschaalde versie van hun database update door naar de VTPv1 en VTPv2 switches. Deze informatie-uitwisseling is echter eenrichtingsgewijs, aangezien geen updates van VTPv1- en VTPv2-switches door de VTPv3-switches worden aanvaard. Op boomstamaansluitingen blijven VTPv3 switches geschaalde updates en volwaardige VTPv3-updates doorsturen om rekening te houden met het bestaan van VTPv2- en VTPv3-buren in de boomstampoorten.

Om VTPv3-ondersteuning te bieden voor uitgebreide VLAN’s wordt het formaat van de VLAN-database, waarin de VTP 70 bytes per VLAN toekent, gewijzigd. Deze wijziging maakt het alleen mogelijk om niet-standaardwaarden te coderen in plaats van ongewijzigde velden voor de legacy-protocollen. Vanwege deze verandering is de ondersteuning van 4K VLAN de grootte van de resulterende VLAN-database.

Aanbeveling

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 wat later vastgestelde overwegingen. De aanbeveling moet twee `server` mode switches in elk domein hebben voor overtolligheid, meestal de twee distributielaag switches. De rest van de switches in het domein moet op de clientmodus worden ingesteld. Wanneer u met behulp van VTPv2 `client`-/`server`-mode implementeert, moet u er rekening mee houden dat een hoger revisienummer altijd in hetzelfde VTP-domein wordt geaccepteerd. Als een switch die is ingesteld in een VTP-`client` of `server`-modus, in het VTP-domein wordt geïntroduceerd en een hoger revisienummer heeft dan de bestaande VTP-servers, overschrijft dit de VLAN-database binnen het VTP-domein. Als de configuratie onbedoeld is gewijzigd en VLAN's worden verwijderd, kan de overschreven betekenen dat er een grote storing in het netwerk optreedt. Om ervoor te zorgen dat `client`- of `server`-switches altijd een configuratieaanpassingsnummer hebben dat lager is dan dat van de server, wijzigt u de client-VTP-domeinnaam in iets anders dan de standaardnaam. Terug naar 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 de voorzichtige benadering van VTP-`transparante` modaliteiten om deze redenen:

- Het stimuleert goede veranderingscontroletaak, aangezien de eis om een VLAN op een switch of een boomhaven aan te passen als één switch tegelijkertijd moet worden beschouwd.
- Het beperkt het risico van een beheerder fout die het volledige domein beïnvloedt, zoals het wissen van een VLAN door ongeluk.
- Er is geen risico dat een nieuwe switch die in het netwerk met een hoger VTP-herzieningsnummer wordt geïntroduceerd de gehele configuratie van het domein VLAN kan overschrijven.
- Het moedigt VLANs aan om te worden gedrukt van trunks die aan switches lopen die geen havens in dat VLAN hebben. Dit maakt het overspoelen van frame meer bandbreedte-efficiënt. Handmatig afdrukken is ook voordelig omdat het de overspannende boomdiameter beperkt (zie de DTP sectie van dit document). Voordat u ongebruikte VLAN's op poortkanaalstammen afdrukt, moet u ervoor zorgen dat alle poorten die op IP-telefoons zijn aangesloten, worden geconfigureerd als toegangspoorten met spraak-VLAN.
- Het uitgebreide VLAN-bereik in CatOS 6.x en CatOS 7.x, nummers 1025 tot 4094, kan alleen op deze manier worden geconfigureerd. Zie het gedeelte Uitgebreid VLAN en MAC-adresbeperking voor meer informatie in dit document.
- VTP `transparante` modus wordt ondersteund in Campus Manager 3.1, een deel van Cisco Works 2000. De oude beperking die minstens één server in een VTP domein vereiste is verwijderd.

Voorbeelden van VTP	**Opmerkingen**
vtp domein*naam* wachtwoord	CDP controleert namen om te helpen controleren of er sprake is van een defect tussen domeinen. Een eenvoudig wachtwoord is een nuttige voorzorgsmaatregel tegen onbedoelde veranderingen. Let op van hoofdletternamen of

x **instelle n**	spaties bij het plakken.
vtp-modus transp arant	
stel vlan *VLAN* numm ernaa m *in*	Per switch die poorten in het VLAN heeft.
Stel *booms tam* in/hav en *VLAN bereik*	Maakt stammen in om VLAN's te dragen waar nodig - de standaard is alle VLAN's.
Vlan *bereik* van *de* stam/*p oort*	Beperkt STP diameter door handdruk, zoals op stammen van distributielaag tot toegangslaag, waar VLAN niet bestaat.

Opmerking: Het specificeren van VLAN's met de **ingestelde** opdracht voegt alleen VLAN's toe en wis deze niet. Bijvoorbeeld, de **vaste x/y 1-10** opdracht van de **stam** stelt de toegestane lijst niet in om slechts VLANs 1-10 te **slechts**. Geef de **duidelijke boomstam x/y 11-1005 opdracht uit om het gewenste resultaat te bereiken.**

Hoewel de symbolische ring buiten het toepassingsgebied van dit document valt, merk op dat VTP `transparante` modus niet wordt aanbevolen voor TR-ISL-netwerken. De basis voor symbolische ringswitching is dat het hele domein één gedistribueerde multi-poorts brug vormt, dus elke switch moet de zelfde informatie van VLAN hebben.

Andere opties

VTPv2 is een vereiste in symbolische ringomgevingen, waar de `client/server` modus sterk wordt aanbevolen.

VTPv3 biedt de mogelijkheid om striktere verificatie- en configuratietoetsing uit te voeren. VTPv3 biedt in wezen hetzelfde niveau van functionaliteit, maar met meer verbeterde beveiliging, zoals VTPv1/VTPv2 `transparante` modus aanbiedt. Bovendien is VTPv3 gedeeltelijk compatibel met de bestaande VTP-versies.

De voordelen van het afdrukken van VLAN's om onnodige frame-overstromingen te beperken worden in dit document bepleit. De **optie VTP-pruning stelt** VLAN's automatisch **op**, waarmee de inefficiënte overstroming van frames kan worden gestopt wanneer deze niet nodig zijn. In tegenstelling tot handmatige VLAN-snoeien beperkt automatische pruning de Spanning Tree diameter niet.

Vanaf CatOS 5.1 kunnen de Catalyst switches 802.1Q VLAN-getallen groter dan 1000 in kaart brengen naar ISL VLAN-getallen. In CatOS 6.x ondersteunen Catalyst 6500/6000 switches 4096 VLAN's in overeenstemming met de IEEE 802.1Q-standaard. Deze VLAN's worden in deze drie bereiken georganiseerd, waarvan er slechts een deel wordt gepropageerd aan andere switches in het netwerk met VTP:

- VLAN's met normaal bereik: 1–1001
- VLAN's met uitgebreid bereik: 1025-4094 (kan alleen worden verspreid door VTPv3)
- gereserveerde VLAN's: 0, 1002—1024, 4095

De IEEE heeft een op standaarden gebaseerde architectuur geproduceerd om gelijkaardige resultaten als VTP te bereiken. Als lid van het 802.1Q Generic Character Registration Protocol (GARP) van 802.1Q biedt het Generic VLAN Registration Protocol (GVRP) interoperabiliteit van het VLAN-beheer tussen leveranciers mogelijk, maar valt buiten de reikwijdte van dit document.

Opmerking: CatOS 7.x biedt de optie om VTP in te stellen op `uit`-modus, een modus die erg vergelijkbaar is met `transparant`. De switch stuurt echter geen VTP-frames door. Dit kan in sommige ontwerpen nuttig zijn wanneer je naar switches buiten je administratieve controle loopt.

Uitgebreide VLAN- en MAC-adresvermindering

De eigenschap van de adresvermindering van MAC maakt uitgebreide bereik VLAN identificatie mogelijk. Inschakelen van MAC-adresvermindering schakelt de pool van MAC-adressen in die worden gebruikt voor de VLAN-omspanningsboom en heeft één MAC-adres. Dit MAC-adres identificeert de switch. CatOS-softwarerelease 6.1(1) introduceert ondersteuning voor MAC-adresvermindering voor Catalyst 6500/6000 en Catalyst 4500/4000 switches om 4096 VLAN's te ondersteunen overeenkomstig de IEEE 802.1Q-standaard.

Overzicht van bediening

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

Catalyst switches met 1024 MAC-adressen maken het standaard niet mogelijk om het MAC-adres te verlagen. MAC-adressen worden achtereenvolgens toegewezen. Het eerste MAC-adres in het bereik wordt aan VLAN 1 toegewezen. Het tweede MAC-adres in het bereik wordt aan VLAN 2 toegewezen, enzovoort. Dit stelt de switches in om 1024 VLAN's met elk VLAN te ondersteunen door een unieke bridge identifier te gebruiken.

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] MAC-adresvermindering wordt standaard ingeschakeld voor switches met 64 MAC-adressen en deze optie kan niet worden uitgeschakeld.

Voor Catalyst serie switches met 1024 MAC adressen, staat een inschakeling van MAC adresvermindering steun van 4096 VLANs die onder PVST+ of 16 Multiple Instance STP (MISTP) lopen toe om unieke identificatoren te hebben zonder een toename in het aantal MAC adressen die op de switch vereist zijn. MAC-adresvermindering reduceert het aantal MAC-adressen die door STP vereist worden van één per VLAN of MISTP-instantie naar één per switch.

Dit getal laat zien dat de bridge identifier MAC-adresvermindering niet is ingeschakeld. De bridge identifier bestaat uit een overbruggingsprioriteit van 2 bytes en een MAC-adres van 6 bytes:

MAC-adresvermindering wijzigt het gedeelte van de STP-bridge-identificator van de BPDU. Het oorspronkelijke prioriteitsveld van 2 bytes is in twee velden verdeeld. Deze splitsingen resulteren in een 4-bits bridge Priority-veld en een 12-bits systeem-ID-uitbreiding die VLAN-nummering van 0 tot 4095 toestaat.

Wanneer u MAC-adresvermindering ingeschakeld hebt op Catalyst switches om uitgebreide bereik VLAN's te benutten, stelt u MAC-adresvermindering in op alle switches binnen hetzelfde STP-domein. Deze stap is nodig om de STP-wortelberekeningen op alle switches consistent te houden. Nadat u MAC-adresvermindering hebt ingeschakeld, wordt de root-brug-prioriteit een veelvoud van 4096 plus de VLAN-id. Switches zonder MAC-adresvermindering kunnen onopzettelijk wortel eisen omdat deze switches een kleinere granulariteit hebben in de selectie van de bridge-ID.

Configuratierichtsnoeren

U moet bepaalde richtlijnen volgen wanneer u uitgebreide VLAN-bereik instelt. De switch kan een blok VLAN's uit het uitgebreide bereik toewijzen voor interne doeleinden. Bijvoorbeeld, kan de switch VLANs voor de routed poorten of Flex WAN modules toewijzen. De toewijzing van het blok VLANs begint altijd van VLAN 1006 en gaat omhoog. Als u om het even welke VLAN's binnen het bereik hebt dat de Flex WAN-module vereist, worden alle vereiste VLAN's niet toegewezen omdat de VLAN's nooit vanuit het VLAN-gebied van de gebruiker worden toegewezen. Geef de opdracht **show VLAN of de samenvatting van de show VLAN op een switch uit om zowel de door de gebruiker toegewezen als interne VLAN's weer te geven.**

```
>show vlan summary

Current Internal Vlan Allocation Policy - Ascending

Vlan status    Count  Vlans
-------------  -----  -----------------------------------------
VTP Active         7   1,17,174,1002-1005
```

```
Internal          7   1006-1011,1016
!--- These are internal VLANs. >show vlan
---- -------------------------------- --------- ------- --------

1    default                          active    7       4/1-48


!--- Output suppressed. 1006 Online Diagnostic Vlan1 active 0 internal 1007 Online Diagnostic
Vlan2 active 0 internal 1008 Online Diagnostic Vlan3 active 0 internal 1009 Voice Internal Vlan
active 0 internal 1010 Dtp Vlan active 0 internal 1011 Private Vlan Internal Vlan suspend 0
internal 1016 Online SP-RP Ping Vlan active 0 internal !--- These are internal VLANs.
```

Bovendien, voordat u de uitgebreide bereik VLANs gebruikt, moet u elke bestaande 802.1Q-to-ISL mappings wissen. Ook moet u, in versies eerder dan VTPv3, het uitgebreide VLAN op elke switch statisch configureren met het gebruik van VTP `transparante` modus. Raadpleeg de sectie van de *configuratierichtsnoeren* van *uitgebreid bereik van VLAN's* van het configureren van VLAN's voor meer informatie.

Opmerking: In software die vroeger is dan softwarerelease 8.1(1), kunt u de VLAN-naam voor VLAN's met uitgebreid bereik niet configureren. Deze mogelijkheid is onafhankelijk van elke VTP-versie of -modus.

Aanbeveling

Probeer een constante configuratie van de MAC-adresvermindering binnen hetzelfde STP-domein te behouden. Het afdwingen van de MAC-adresvermindering op alle netwerkapparaten kan echter onpraktisch zijn wanneer er een nieuw chassis met 64 MAC-adressen wordt toegevoegd aan het STP-domein. MAC-adresvermindering wordt standaard ingeschakeld voor switches met 64 MAC-adressen en deze optie kan niet worden uitgeschakeld. Begrijp dat, wanneer twee systemen met de zelfde overspannende-boomprioriteit worden gevormd, het systeem zonder de vermindering van het adres van MAC een betere overspanning-boomprioriteit heeft. Geef deze opdracht uit om MAC-adresvermindering in of uit te schakelen:

```
set spantree macreduction enable | disable
```

De toewijzing van de interne VLAN's is in oplopende volgorde en begint bij VLAN 1006. Pas de gebruiker VLAN's aan zo dicht mogelijk bij VLAN 4094 om conflicten tussen de gebruiker VLAN's en de interne VLAN's te voorkomen. Met Catalyst 6500 switches die Cisco IOS® systeemsoftware draaien, kunt u de interne VLAN-toewijzing in aflopende volgorde configureren. De Opdracht-Line Interface (CLI)-equivalent voor CatOS-software wordt niet officieel ondersteund.

Automatische onderhandeling

Ethernet/Fast Ethernet

Automatische onderhandeling is een optionele functie van de standaard IEEE Fast Ethernet (FE) (802.3u) die apparaten toelaat om automatisch informatie over een link over **snelheid** en **dubbele** mogelijkheden uit te wisselen. De automatisering werkt bij Layer 1 (L1) en richt zich op de toegangslaag havens waar de **tijdelijke gebruikers** zoals PCs aan het netwerk verbinden.

Overzicht

De meest algemene oorzaak van prestatiekwesties op 10/100 Mbps Ethernet verbindingen komt voor wanneer één poort op de verbinding bij half-duplex werkt terwijl de andere bij volledig-duplex is. Dit gebeurt af en toe wanneer één of beide havens op een verbinding worden teruggesteld en het autonome onderhandelingsproces veroorzaakt niet beide verbindingspartners om de zelfde configuratie te hebben. Het gebeurt ook wanneer de beheerders de ene kant van een link opnieuw configureren en de andere kant vergeten te reconfigureren. De typische symptomen hiervan zijn stijgende frame check sequentie (FCS), cyclische redundantie controle (CRC), uitlijning of runt tellers op de switch.

In deze documenten wordt uitvoerig gesproken over de autonome onderhandelingen. Deze documenten bevatten verklaringen over hoe autonoom onderhandelen werkt en configuratieopties.

- Ondersteuning en probleemoplossing van Ethernet 10/100 MB/100/A Full-Multiservice-onderhandeling
- 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-duplex en autonegotiate aan volledig-duplex met de andere verbindingspartner handmatig te vormen. Een poging om dit voor elkaar te krijgen resulteert in een dubbele wanverhouding. Dit is een gevolg van één verbinding partner autonegotiating, het zien van geen autonome onderhandelingsparameters van de andere verbindingspartner, en het in gebreke blijven aan half-duplex.

De meeste Catalyst Ethernet modules steunen 10/100 Mbps en half/volledig-duplex, maar de **show** van **poortmogelijkheden *mod/haven*** opdracht bevestigt dit.

FEFI

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

Een **ver eindfout** is een fout in de link die het ene station kan detecteren terwijl het andere niet kan, zoals een losgekoppelde TX-draad. In dit voorbeeld kon het verzendende station nog geldige gegevens ontvangen en ontdekken dat de link goed is door de link-integriteit-monitor. Zij heeft niet aangetoond dat de transmissie ervan niet door het andere station wordt ontvangen. Een 100BASE-FX-station dat een dergelijke externe fout detecteert, kan zijn overgebrachte IDLE-stroom wijzigen om een speciaal bit-patroon (aangeduid als het FEFI IDLE-patroon) te verzenden om de buurman op de hoogte te stellen van de externe fout; het FEFI-IDLE patroon zet vervolgens een sluiting van de externe poort (foutmelding) in. Raadpleeg het gedeelte UDLD in dit document voor meer informatie over de foutbescherming.

FEFI wordt ondersteund door deze hardware en deze modules:

- Catalyst 5500/5000: WS-X5201R, WS-X5305, WS-X5236, WS-X5237, WS-U5538 en WS-U5539
- Catalyst 6500/6000 en 4500/4000: Alle 100BASE-FX modules en GE modules

Aanbeveling

Of om autonome onderhandeling op 10/100 links of aan harde codesnelheid en duplex te vormen hangt uiteindelijk af van het type van de verbindingspartner of het eindapparaat dat u aan een haven van de switch van de Catalyst hebt verbonden. Autonome onderhandelingen tussen eindapparaten en Catalyst switches werken over het algemeen goed en Catalyst switches zijn compatibel met de IEEE 802.3u-specificatie. Er kunnen echter problemen ontstaan wanneer switches van een NIS of verkoper niet precies in overeenstemming zijn. Hardware-incompatibiliteit en andere problemen kunnen ook bestaan als gevolg van leverancierspecifieke geavanceerde functies, zoals automatische polariteit of bekabelingsintegriteit, die niet worden beschreven in de IEEE 802.3u-specificatie voor 10/100 Mbps autonomie. Raadpleeg de melding uit het veld: Prestatieprobleem met Intel Pro/1000T-NIC's die aansluiten op CAT4K/6K voor een voorbeeld hiervan.

Voorzien dat er bepaalde situaties zullen zijn die host, poortsnelheid en duplex moeten worden ingesteld. Volg deze basisstappen voor het oplossen van problemen in het algemeen:

- Zorg ervoor dat ofwel de autonomie aan beide kanten van de link is ingesteld, ofwel de harde codering aan beide kanten is ingesteld.
- Controleer de CatOS-opmerkingen op gemeenschappelijke voorbehouden.
- Controleer de versie van het NIC-stuurprogramma of het besturingssysteem dat u gebruikt, aangezien het laatste stuurprogramma of pleister vaak vereist is.

Als regel, probeer eerst autonome onderhandeling te gebruiken voor elk type van verbindingspartner. Er zijn duidelijke voordelen aan het configureren van autonome onderhandeling voor transient apparaten zoals laptops. Idealiter werkt autonegotiation ook goed met niet-transiente apparaten zoals servers en vaste werkstations of van switch-naar-switch en switch-naar-router. Om een aantal van de genoemde redenen kunnen zich onderhandelingskwesties voordoen. In deze gevallen volgt u de basisstappen voor het oplossen van problemen die in de TAC-koppelingen zijn beschreven.

Als de poortsnelheid is ingesteld op `auto` op een 10/100 Mbps Ethernet poort worden zowel snelheid als duplex automatisch geregisseerd. Geef deze opdracht uit om de poort in te stellen op auto:

```
set port speed port range auto
!--- This is the default.
```

Als het hard coderen van de poort, geef deze configuratieopdrachten uit:

```
set port speed port range 10 | 100 set port duplex port range full | half
```

In CatOS 8.3 en later, heeft Cisco het optionele **auto-10-100** sleutelwoord geïntroduceerd. Gebruik het **auto-10-100** sleutelwoord op havens die snelheden van 10/100/1000 Mbps steunen maar waar het autonoom onderhandelen naar 1000 Mbps ongewenst is. Gebruik van het **auto-10-100** sleutelwoord maakt de haven zich op de zelfde manier als een 10/100-Mbps poort die de snelheid aan **auto** heeft ingesteld. De snelheid en duplex worden alleen voor 10/100 Mbps poorten onderhandeld en de 1000 Mbps snelheid neemt niet deel aan de onderhandeling.

```
set port speed port_range auto-10-100
```

Andere opties

Wanneer er geen autonome onderhandeling tussen switches wordt gebruikt, kan de foutmelding L1 ook voor bepaalde problemen verloren gaan. Het is behulpzaam om L2 protocollen te gebruiken om mislukkingsdetectie te vergroten, zoals agressieve UDLD.

Gigabit Ethernet

Gigabit Ethernet (GE) heeft een autonome onderhandelingsprocedure (IEEE 802.3z) die uitgebreider is dan die voor 10/100 Mbps Ethernet en wordt gebruikt om flow-control parameters, informatie over externe fout en duplexinformatie uit te wisselen (ook al ondersteunen Catalyst serie GE poorten alleen full-duplex modus).

Opmerking: 802.3z is vervangen door de specificaties van IEEE 802.3:2000. Raadpleeg het abonnement IEEE Standards on Line LAN/MAN Standards: Archieven voor meer informatie.

Overzicht

GE poort onderhandeling is standaard ingeschakeld en de poorten op beide uiteinden van een GE link moeten dezelfde instelling hebben. Anders dan FE komt de GE link niet naar voren als de autonomie instelling op de poorten aan elk eind van de link verschilt. Nochtans, de enige voorwaarde die voor een autonegotiation-gehandicapte haven om omhoog te verbinden is een geldig Gigabit signaal van het verre eind. Dit gedrag is onafhankelijk van de autonome onderhandelingconfiguratie van het verre einde. Bijvoorbeeld, veronderstel dat er twee apparaten zijn, A en B. Elk apparaat kan autonegotiation aan of uitgeschakeld hebben. Deze tabel bevat een lijst van mogelijke configuraties en respectieve verbindingsstaten:

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

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 faalt" voorwaarde 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 autonomie-onderhandeling op een poort is 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 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 **ingestelde opdracht voor sync-opnieuw starten-vertraging heeft alleen een effect wanneer de autonomie ingesteld is** `om` het `uit` te `schakelen`.

Aanbeveling

Het in staat stellen van autonomie is veel kritischer in een GE omgeving dan in een 10/100 omgeving. Autonome onderhandelingen moeten in feite alleen worden uitgeschakeld op switches-poorten die zich aansluiten bij apparaten die onderhandelingen niet kunnen ondersteunen of waar aansluitingsproblemen voortvloeien uit interoperabiliteitsproblemen. Cisco raadt aan om Gigabit onderhandeling (standaard) op alle switch-to-switch links en over het algemeen alle GE apparaten aan te zetten. Geef deze opdracht uit om autonome onderhandelingen mogelijk te maken:

```
set port negotiation port range enable
!--- This is the default.
```

Eén bekende uitzondering is wanneer er een verbinding is met een Gigabit Switch Router (GSR) die Cisco IOS-software eerder dan release 12.0(10)S runt, de release die stroomcontrole en autonomie toevoegt. Schakel deze twee functies uit, of de switch poortrapporten `zijn niet aangesloten`, en de SR rapporteert fouten. Dit is een sequentie van de steekproefopdracht:

```
set port flowcontrol receive port range off set port flowcontrol send port range off set port
negotiation port range disable
```

Switch-naar-server verbindingen moeten per geval worden bekeken. Cisco-klanten hebben problemen ondervonden met Gigabit onderhandeling op Sun, HP en IBM servers.

Andere opties

Flow control is een optioneel onderdeel van de 802.3x-specificatie en moet indien gebruikt via onderhandelingen tot stand worden gebracht. Apparaten kunnen of kunnen niet in staat zijn om naar een PAUSE-frame te verzenden en/of te reageren (**bekende MAC 01-80-C2-00-00-00F**). Ze kunnen ook niet instemmen met het verzoek om stroomcontrole van de buurman. Een poort met een invoerbuffer die vult stuurt een PAUSE frame naar zijn vennoot, die de transmissie stopt, en om het even welke extra kaders in de de uitvoer van de verbindingspartner buffers houdt. Dit lost geen enkel probleem op van overabonnement op de evenwichtsstaat, maar maakt de invoerbuffer in feite groter door een fractie van de output buffer van de partner tijdens uitbarstingen.

Deze optie wordt het best gebruikt voor koppelingen tussen access-poorten en end hosts, waar de host-uitvoerbuffer potentieel even groot is als hun virtuele geheugen. Switch-tot-switch gebruik heeft beperkte voordelen.

Geef deze opdrachten uit om dit in de switches te controleren:

```
set port flowcontrol mod/port 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, WS-X4306) sturen nooit PAUZE-frames af zelfs als ze onderhandelen om dit te doen, omdat ze niet-blokkerend zijn.

Dynamic Trunking Protocol

Type insluiting

Trunk breidt VLAN's tussen apparaten uit door tijdelijk de originele Ethernet frames te identificeren en te taggen (link-lokaal), zodat ze kunnen worden vermenigvuldigd via één link. Dit waarborgt ook dat de afzonderlijke VLAN-uitzending en de beveiligingsdomeinen tussen switches worden onderhouden. CAM-tabellen onderhouden de frame-naar-VLAN-mapping in de switches.

Trunking wordt ondersteund op verschillende typen L2-media, waaronder ATM LANE, FDDI 802.10 en Ethernet, hoewel alleen het laatste hier wordt gepresenteerd.

ISL-operationeel overzicht

ISL, de bedrijfseigen identificatie- of tagging-regeling van Cisco, is al vele jaren in gebruik. De IEEE 802.1Q-standaard is ook beschikbaar.

Door het originele frame volledig in een tagging-programma met twee niveaus in te kapselen, is

ISL in feite een tunneling-protocol en heeft deze het extra voordeel niet-Ethernet-frames te kunnen vervoeren. Hiermee voegt u een 26-bytes header en 4-bytes FCS toe aan het standaard Ethernet-frame - de grotere Ethernet-frames worden verwacht en verwerkt door poorten die zijn geconfigureerd als trunks. ISL ondersteunt 1024 VLAN's.

ISL frame-indeling

40 bits	4 bits	4 bits	48 bits	16 bits	24 bits	24 bits	15 bits	bit	16 bits	16 bits	Lengte variabele	32 bits
Desten. Adressaat	Type	GEBRUIKER	SA	LEN	SNAP LLC	HSA	VLAN	BPDU	INDEX	Reserve	Inkapseld frame	FCS
01-00-0c-00-00					AAA03	000000C						

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

802.1Q operationeel overzicht

De standaard IEEE 802.1Q specificeert veel meer dan insluitingstypen, waaronder Spanning Tree Verbeteringen, GARP (zie de VTP-sectie van dit document) en QoS-markering (Quality of Service) van 802.1p.

Het 802.1Q frame-formaat behoudt het oorspronkelijke Ethernet bron-adres en het doeladres, maar switches moeten nu verwachten dat er baby-gigantische frames worden ontvangen, zelfs op toegangspoorten waar hosts tagging kunnen gebruiken om 802.1p gebruikersprioriteit voor QoS-signalering uit te drukken. De tag is 4 bytes, zodat 802.1Q Ethernet v2-frames 1522 bytes zijn, een IEEE 802.3ac-werkgroepresultaat. 802.1Q ondersteunt ook de nummerruimte voor 4096 VLAN's.

Alle gegevensframes die worden verzonden en ontvangen, zijn 802.1Q-gelabeld behalve die op het inheemse VLAN (er is een impliciete tag gebaseerd op de ingress switch poortconfiguratie). Frames op het inheemse VLAN worden altijd zonder tag verzonden en normaal ontvangen zonder tag. Ze kunnen echter ook worden gemerkt.

Raadpleeg de standaardisering van VLAN via IEEE 802.10 en krijg IEEE 802 voor meer informatie.

Frame Relay 802.1Q/801.1p frame-indeling

		Leerknop						
		TPID	TCI					
4	48	16	3 bits	1	12	16 bits	Lengte	32

8 bits	bits	**bits**		**bit**	**bits**		variabele	bits
DA	SA	**TPID**	**Prioriteit**	**CFI**	**VLAN-id**	Lengte/type	Gegevens met PAD	FCS
		0x8100	**0-7**	**0-1**	**0-4095**			

Aanbeveling

Aangezien alle nieuwere hardware 802.1Q ondersteunt (en sommige alleen 802.1Q ondersteunt, zoals de Catalyst 4500/4000 Series en CSS 1000), raadt Cisco aan dat alle nieuwe implementaties de IEEE 802.1Q standaard volgen en oudere netwerken geleidelijk van ISL migreren.

De IEEE-standaard maakt verkoopinteroperabiliteit mogelijk. Dit is voordelig voor alle Cisco-omgevingen, aangezien nieuwe host 802.1p-geschikte NIC's en apparaten beschikbaar komen. Hoewel zowel ISL- als 802.1Q-implementaties volgroeid zijn, zal de IEEE-standaard uiteindelijk een grotere blootstelling aan gebieden en meer ondersteuning voor derden hebben, zoals ondersteuning voor netwerkanalyzer. De onderste insluitingsoverhead van 802.1Q in vergelijking met ISL is ook een minder belangrijk punt in het voordeel van 802.1Q.

Aangezien het insluitingstype is overeengekomen tussen switches die DTP gebruiken, met ISL die standaard als de winnaar is geselecteerd als beide eindpunten het ondersteunen, is het nodig deze opdracht uit te geven om dot1q te specificeren:

```
set trunk mod/port mode dot1q
```

Als VLAN 1 van een stam wordt gewist, zoals besproken in het gedeelte In-Band Management van dit document, hoewel er geen gebruikersgegevens worden verzonden of ontvangen, blijft NMP controleprotocollen zoals CDP en VTP op VLAN 1 doorgeven.

Zoals ook in het gedeelte VLAN 1 van dit document wordt besproken, worden de pakketten CDP, VTP en PAgP altijd op VLAN 1 verzonden wanneer u een trunking uitvoert. Wanneer u dot1q insluiting gebruikt, worden deze controleframes getagd met VLAN 1 als het inheemse VLAN van de switch wordt gewijzigd. Als dot1q trunking aan een router wordt toegelaten 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 zicht van de buur CDP op de router te bieden.

Opmerking: Er is een potentiële veiligheidsoverweging met punt1q veroorzaakt door het impliciet taggen van het inheemse VLAN, omdat het mogelijk kan zijn om frames van één VLAN naar een ander te verzenden zonder een router. Raadpleeg Zijn er kwetsbaarheden in VLAN-implementaties? voor nadere bijzonderheden . De workround moet een VLAN ID voor het inheemse VLAN van de boomstam gebruiken die niet voor eindgebruikerstoegang gebruikt wordt. De meerderheid van de klanten van Cisco verlaat VLAN 1 als autochtone VLAN op een boomstam en verdeel toegangshavens aan VLANs anders dan VLAN 1 om dit eenvoudigweg te bereiken.

Trunkmodus

DTP is de tweede generatie van Dynamic ISL (DISL) en bestaat om te verzekeren dat de verschillende parameters die betrokken zijn bij het verzenden van ISL- of 802.1Q-frames, zoals het geconfigureerde insluitingstype, native VLAN en hardware-mogelijkheid, door de switches aan beide uiteinden van een romp zijn overeengekomen. Dit helpt ook te beschermen tegen overstromingen van getagde frames in niet-zeehavens, een potentieel ernstig veiligheidsrisico, door ervoor te zorgen dat havens en hun buren zich in consistente staten bevinden.

Overzicht

DTP is een L2 protocol dat configuratieparameters tussen een haven van de switch en zijn buur bespreekt. Het gebruikt een ander multicast MAC-adres (**10-00-0c-cc-cc-**cc) en een SNAP-protocoltype van 0x2004. Deze tabel is een samenvatting van de configuratie-modi:

Modus	Functie	DTP-frames verzonden	Eindstaat (lokale poort)
`Auto (standaard)`	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
`Aan`	Past de poort in permanente trunking mode en onderhandelt om de link in een boomstam om te zetten. De haven wordt een boomhaven zelfs als de aangrenzende haven niet met de verandering instemt.	Ja, periodiek.	Trunken, **onvoorwaardelijk**.
`nonegotiaans`	Past de poort in permanente trunking modus maar voorkomt dat de poort DTP-frames genereert. U moet de aangrenzende poort handmatig configureren als een boomstampoort om een boomstam verbinding op te zetten. Dit is handig voor apparaten die DTP niet ondersteunen.	Nee	Trunken, **onvoorwaardelijk**.
`wenselijk`	Maakt de poort actief om de link naar een hoofdlink	Ja, periodiek.	Het eindigt

	te converteren. De poort wordt een boomstampoort als de aangrenzende poort is ingesteld op `aan`, `wenselijk`, of `auto` mode.		alleen in trunking toestand als de afstands modus `op staat`, `auto` of `wenselijk` is.
`Uit`	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 de verandering van `in`.	niet-trunking

Dit zijn een paar hoogtepunten van het protocol:

- DTP veronderstelt een point-to-point verbinding en Cisco apparaten steunen alleen 802.1Q boomstampoorten die point-to-point zijn.
- Tijdens DTP-onderhandeling nemen de poorten niet deel aan STP. Alleen nadat de poort een van de drie DTP-typen is geworden (access, ISL of 802.1Q) wordt de poort toegevoegd aan STP. Anders is PAgP, indien geconfigureerd, het volgende proces dat moet worden uitgevoerd voordat de poort aan STP deelneemt.
- Als de poort in ISL modus is trunking, worden DTP-pakketten op VLAN 1 verzonden, anders (voor 802.1Q trunking of niet-trunking poorten) worden ze op het inheemse VLAN verzonden.
- In de `gewenste` modus verplaatsen DTP-pakketten **de VTP-**domeinnaam (die moet overeenkomen met een onderhandelde romp die omhoog moet komen), plus de configuratie van de romp en de **admin-status**.
- Berichten worden elke seconde gestuurd tijdens de onderhandeling, en elke 30 seconden daarna.
- Zorg ervoor dat u begrijpt dat modi `op`, `non-onderhandeling` en `off` expliciet specificeren in welke staat de haven eindigt. Een slechte configuratie kan leiden tot een gevaarlijke/inconsistente toestand waarin de ene kant trunking heeft en de andere niet.
- Een poort in `op`, `auto`, of `gewenste` modus stuurt DTP beelden periodiek. Als een poort in `auto` of `wenselijke` modus in vijf minuten geen DTP-pakket ziet, wordt deze ingesteld op niet-stam.

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.

Aanbeveling

Cisco adviseert een expliciete boomstamconfiguratie van `wenselijk` aan beide uiteinden. In deze modus kunnen netwerkexploitanten de syslog- en de statusberichten van de opdrachtregel vertrouwen dat een haven in en aan trunking is, in tegenstelling `tot de` modus, die een haven kan maken verschijnt zelfs als de buur verkeerd is ingesteld. Daarnaast biedt de `gewenste` modusromp stabiliteit in situaties waar één kant van de link geen stam kan worden of de romp daalt. Geef deze opdracht uit om de `gewenste` modus in te stellen:

```
set trunk mod/port desirable ISL | dot1q
```

Opmerking: Stel de romp op alle niet-kofferpoorten in. Dit helpt verspilling van onderhandelingstijd te voorkomen wanneer u host poorten omhoog brengt. Deze opdracht wordt ook uitgevoerd wanneer de ingestelde port host-opdracht wordt gebruikt; Raadpleeg het gedeelte STP voor meer informatie. Geef deze opdracht uit om een romp op een bereik poorten uit te schakelen:

```
set trunk port range off
!--- Ports are not trunking; part of the set port host command.
```

Andere opties

Een andere algemene klantconfiguratie gebruikt alleen de `gewenste` modus op de distributielaag en de eenvoudigste standaardconfiguratie (`automatische` modus) op de toegangslaag.

Sommige switches, zoals een Catalyst 2900XL, Cisco IOS routers, of andere verkoopapparaten, ondersteunen momenteel geen boomstamonderhandeling door DTP. U kunt de niet-onderhandelingsmodus gebruiken op Catalyst 4500/4000, 5500/5000 en 6500/6000 switches om onvoorwaardelijk een poort in te stellen op de romp met deze apparaten, wat kan helpen om te standaardiseren op een gemeenschappelijk standpunt over de campus. U kunt ook `non-onderhandelate` mode implementeren om de "algemene" tijd voor initialisatie van de link te verminderen.

Opmerking: Factoren zoals de kanaalmodus en de STP-configuratie kunnen ook de initialisatietijd beïnvloeden.

Geef deze opdracht uit om de `niet-onderhandelingsmodus` in te stellen:

```
set trunk mod/port nonegotiate ISL | dot1q
```

Cisco raadt `nonegotiate aan` wanneer er een verbinding met een Cisco IOS router is omdat wanneer het overbruggen wordt uitgevoerd, sommige DTP-frames die van **op** mode worden ontvangen terug in de boomstampoort kunnen komen. Na ontvangst van het DTP frame probeert de switch poort onnodig opnieuw te onderhandelen (of de romp omlaag en omhoog te brengen). Als `nonegotiate` is ingeschakeld, stuurt de switch geen DTP-frames.

Spanning Tree Protocol

Basisoverwegingen

Spanning Tree Protocol (STP) houdt een L2-netvrij milieu in redundante geschakelde en verbonden netwerken in. Zonder STP vermenigvuldigen frames en/of vermenigvuldigen voor onbepaalde tijd, wat een netwerkmeltdown veroorzaakt omdat alle apparaten in het uitgezonden domein continu door hoog verkeer worden onderbroken.

Hoewel STP in sommige opzichten een ontwikkeld protocol is dat aanvankelijk is ontwikkeld voor langzame op software gebaseerde bridge-specificaties (IEEE 802.1d), kan het complex zijn om goed te implementeren in grote geschakelde netwerken met veel VLAN's, veel switches in een domein, ondersteuning van meerdere leveranciers en nieuwere IEEE.

Voor toekomstig referentie blijft CatOS 6.x nieuwe STP-ontwikkeling opnemen, zoals MISTP, loop-Guard, root-bewakers en BPDU-aankomstdetectie van een scheefheid. Bovendien zijn er verdere gestandaardiseerde protocollen beschikbaar in CatOS 7.x, zoals IEEE 802.1s gedeelde Spanning Tree en IEEE 802.1w snelle Spanning Tree.

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, die de BID van elke switch bevatten, evenals de padkosten om die switch te bereiken. Dit maakt het mogelijk de root-brug en de route met de laagste kosten naar de wortel te bepalen. Aanvullende configuratieparameters die in BPDU's van de wortel zijn gebruikt, omzeilen de parameters die lokaal zijn geconfigureerd, zodat het hele netwerk consistente timers gebruikt.

De topologie converteert dan door deze stappen:

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

Raadpleeg Spanning Tree configureren voor meer informatie.

Standaard timer-standaardinstellingen (seconden)	Name	Functie
2	`Hallo`	Bestuurt het verzenden van BPDU's.
15	`Voorgaande vertraging (FWDM-vertraging)`	Bepaalt hoe lang een poort besteed aan het luisteren en het leren van staat en beïnvloedt het proces van de topologie verandering (zie volgende sectie).
20	`Maxage`	Bepaalt hoe lang de switch de huidige topologie handhaaft alvorens het op een

		alternatief pad zoekt. Na de Maxage seconden, wordt een BPDU als oud beschouwd en de switch zoekt een nieuwe wortelhaven van de pool van het blokkeren van havens. Als er geen geblokkeerde haven beschikbaar is, wordt er beweerd dat het de wortel zelf is op de aangewezen havens.

Poort staten	Betekenis	Standaard timing voor de volgende staat
Uitgeschakeld	Administratief omlaag.	N.v.t.
Blokken	Het ontvangen van BPDU's en het stoppen van gebruikersgegevens.	Toezicht op de ontvangst van BPDU's. Wacht 20 seconden op Max. verloopdatums of onmiddellijke verandering als een directe/lokale link is gedetecteerd.
Luisteren	Verzenden of ontvangen van BPDU's om te controleren of terugkeren naar blokkering noodzakelijk is.	Uitgestelde timer (15 seconden wachten)
Leren	Bouwtopologie/CAM -tabel.	Uitgestelde timer (15 seconden wachten)
Doorsturen	Verzenden/ontvangen gegevens.	
	Totale fundamentele topologie-verandering:	**20 + 2 (15) = 50 seconden indien gewacht op het verstrijken van Maxage, of 30 seconden voor een storing van de directe link**

De twee soorten BPDU's in STP zijn BPDU's voor configuratie en Topology Change Kennisgeving (TCN) - BPDU's.

Configuratie BPDU-Flow

De configuratie BPDU's zijn gebaseerd op elk hallo-interval van elke poort op de root-brug en stromen vervolgens naar alle bladeswitches switches om de status van de Spanning Tree te behouden. In steady state is de BPDU-stroom in één richting: wortelpoorten en blokkerende poorten ontvangen alleen configuratie BPDU's, terwijl aangewezen poorten alleen configuratie BPDU's verzenden.

Voor elke BPDU die door een switch van de wortel wordt ontvangen, wordt een nieuwe verwerkt

door het centrale NMP van de Catalyst en verzonden die de wortelinformatie bevat. Met andere woorden, als de root-brug verloren is of alle paden naar de root-brug verloren zijn, worden BPDU's niet ontvangen (totdat de maxage-timer herselecteert).

TCN BPDU-stroom

De GN-BPDU's zijn afkomstig van bladeservers en stromen naar de root-brug wanneer een topologieverandering wordt gedetecteerd in de omspanningsboom. Houtpoorten sturen alleen TCN's, en aangewezen havens ontvangen slechts TCN's.

De GN BPDU reist naar de wortelrand en wordt bij elke stap erkend, dus dit is een betrouwbaar mechanisme. Zodra deze bij de root-brug is aangekomen, waarschuwt de root-brug het gehele domein dat een verandering heeft plaatsgevonden door BPDU's van de configuratie te betrekken terwijl de GN-vlag `is` ingesteld voor **maximum** `+` vertragingstijd (standaard 35 seconden). Dit veroorzaakt dat alle switches hun normale CAM-verouderingstijd van vijf minuten (standaard) veranderen in het interval dat gespecificeerd is door `fwdvertraging` (standaard 15 seconden). Raadpleeg het gedeelte Spanning Tree Protocol voor meer informatie.

Spanning Tree-modi

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

- Eén Spanning Tree Protocol voor alle VLAN's, of alleen-Spanning Tree Protocol, zoals IEEE 802.1Q
- Een Spanning Tree per VLAN of gedeelde Spanning Tree zoals Cisco PVST
- Een Spanning Tree per set VLAN's of meerdere Spanning Tree, zoals Cisco MISTP en IEEE 802.1s

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 bevat geen gegevens.

Eén Spanning Tree per VLAN maakt taakverdeling mogelijk maar vereist meer BPDU CPU-verwerking naarmate het aantal VLAN's toeneemt. De CatOS release opmerkingen bieden advies over het aantal logische poorten dat in de Spanning Tree per switch wordt aanbevolen. Bijvoorbeeld, de formule van Catalyst 6500/6000 Supervisor Engine 1 is als zodanig:

aantal poorten + (aantal stammen * aantal VLAN's op stammen) < 4000

Cisco MISTP en de nieuwe standaard 802.1s staan de definitie van slechts twee actieve STP instanties/topologieën toe, en het in kaart brengen van alle VLAN's aan één van deze twee bomen. Deze techniek staat STP toe om aan vele duizenden VLAN's te schaal terwijl het in evenwicht brengen van de lading wordt toegelaten.

BPDU-formaten

Om de standaard IEEE 802.1Q te ondersteunen, werd de bestaande Cisco STP-implementatie uitgebreid om PVST+ te worden door ondersteuning voor een tunneling in een IEEE 802.1Q mono Spanning Tree-gebied toe te voegen. PVST+ is daarom compatibel met zowel IEEE 802.1Q MST als Cisco PVST-protocollen en heeft geen extra opdrachten of configuratie nodig. Daarnaast voegt PVST+ controlemechanismen toe om te verzekeren dat er geen configuratie inconsistentie van port trunking en VLAN IDs over switches is.

Dit zijn enkele operationele hoogtepunten van het PVST+ protocol:

- PVST+ interopereert met 802.1Q mono-Spanning Tree door de zogeheten Common Spanning Tree (CST) via een 802.1Q stam. CST is altijd op VLAN 1, zodat dit VLAN op de stam moet worden geactiveerd om met andere verkopers samen te werken. CST-BPDU's worden altijd zonder tag overgebracht naar de IEEE-standaard bridge-groep (MAC-adres 01-80-c2-00-00-00, DSAP 42, SSAP 42). Voor de volledigheid van de beschrijving wordt een parallelle reeks BPDU's ook verzonden naar het Cisco gedeelde Spanning Tree MAC-adres voor VLAN 1.
- PVST+ tunnels PVST BPDU's over 802.1Q VLAN's als multicast gegevens. Cisco Shared Spanning Tree BPDU's worden naar MAC-adres 10-00c-cc-cc-cd (SNAP HDLC-protocol type 0x010b) voor elk VLAN in een stam verzonden. BPDU's worden niet op het oorspronkelijke VLAN getagd en voor alle andere VLAN's gemerkt.
- PVST+ controleert poort en VLAN inconsistenties. PVST+ blokkeert die havens die inconsistente BPDU's ontvangen om het verzenden loops te voorkomen. Het informeert gebruikers ook via syslog berichten over elke configuratie mismatch.
- PVST+ is achterwaarts compatibel met bestaande Cisco switches die PVST op ISL trunks draaien. ISL-ingekapselde BPDU's worden nog steeds verzonden of ontvangen met behulp van het IEEE MAC-adres. Met andere woorden: elk BPDU-type is link-plaatselijk; er zijn geen vertaalproblemen .

Aanbeveling

Alle Catalyst switches hebben STP standaard ingeschakeld. Dit wordt zelfs aanbevolen als er een ontwerp wordt gekozen dat geen L2 lijnen omvat zodat STP niet in de zin is dat het actief een geblokkeerde poort aanhoudt.

```
set spantree enable all
!--- This is the default.
```

Cisco raadt aan om STP om deze redenen aan te blijven:

- Als er een lus is (die door mispatching wordt veroorzaakt, slechte kabel, etc.) voorkomt STP schadelijke effecten voor het netwerk veroorzaakt door multicast en uitzending gegevens.
- Bescherming tegen het afbreken van een EtherChannel.
- De meeste netwerken worden ingesteld met STP, waardoor het een maximale blootstelling in het veld krijgt. Meer blootstelling is over het algemeen gelijk aan stabiele code.
- Bescherming tegen dubbel aangesloten NIC's die zich verkeerd gedragen (of overbrugging op servers mogelijk maken).
- De software voor veel protocollen (zoals PAgP, IGMP snooping en trunking) is nauw verbonden met STP. Zonder STP uitvoeren kan leiden tot ongewenste resultaten.

Verandert de timers niet, omdat dit de stabiliteit nadelig kan beïnvloeden. De meeste netwerken die worden ingezet zijn niet aangepast. De eenvoudige STP timers die door de opdrachtregel toegankelijk zijn, zoals hallo-interval en Maxage, bestaan zelf uit een complexe reeks andere veronderstelde en intrinsieke timers, zodat het moeilijk is om timers te stemmen en alle implicaties te overwegen. Bovendien bestaat het gevaar dat de UDLD-bescherming wordt ondermijnd.

Idealiter gebruikersverkeer van het beheer VLAN houden. Vooral met oudere Catalyst switch processors is het best om problemen met STP te voorkomen door het beheer VLAN gescheiden

te houden van gebruikersgegevens. Een eindstation dat zich slecht gedraagt kon de Supervisor Engine processor zo druk houden met uitzending dat het één of meer BPDU's kan missen. Maar nieuwere switches met krachtiger CPU's en wentelende controles verlichten deze overweging. Zie het gedeelte In-band beheer van dit document voor meer informatie.

Sluit niet te veel ontworpen redundantie aan. Dit kan leiden tot een nachtmerrie voor het oplossen van problemen - te veel blokkerende havens hebben een negatieve invloed op de stabiliteit op de langere termijn. **Houd de totale SPT-diameter onder zeven hop**. Probeer het model van Cisco met meerdere lagen, met zijn kleinere geschakelde domeinen, STP driehoeken en deterministische geblokkeerde poorten (zoals uitgelegd in Gigabit Campus Network Design-Principles en Architecture) waar mogelijk te ontwerpen.

Invloed en weet waar de functionaliteit van de Loot en de geblokkeerde havens verblijven, en documenteer ze op het topologie diagram. De geblokkeerde poorten zijn waar het oplossen van STP begint - wat ze van blokkering naar doorsturen heeft veranderd is vaak het sleutelgedeelte van de analyse van de worteloorzaak. **Kies de distributie en de kernlagen als de locatie van root/secondaire Root**, omdat deze als de meest stabiele delen van het netwerk worden beschouwd. Controleer op optimale L3- en HSRP-overlay met L2-pad voor gegevensdoorsturen. Deze opdracht is een macro die de overbruggingsprioriteit vormt; wortel stelt het veel lager dan het standaard(32768), terwijl de basis-secundaire sets redelijk lager zijn dan het standaard:

```
set spantree root secondary vlan range
```

Opmerking: deze macro stelt de hoofdprioriteit in om 8192 (standaard), de huidige hoofdprioriteit minus 1 (als een andere root-brug bekend is) of de huidige hoofdprioriteit (als het MAC-adres lager is dan de huidige wortel) te zijn.

Duw onnodige VLAN's van boompoorten (een bidirectionele oefening). Dit 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. Raadpleeg het gedeelte VTP van dit document voor meer informatie. Standaard VLAN 1 kan ook uit trunks worden verwijderd met CatOS 5.4 en hoger.

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

Andere opties

Cisco heeft een andere STP die **bekend staat als VLAN-bridge**. Dit protocol werkt met behulp van een MAC-adres van de bestemming van **01-00-0c-cd-cd-ce** en een protocol type van 0x010c.

Dit is het meest handig als er een noodzaak is om niet-routeerbare of oudere protocollen tussen VLAN's te overbruggen zonder de Spanning Tree-instantie(s) van IEEE te verstoren die op deze VLAN's actief is. Als VLAN-interfaces voor onoverbrugd verkeer geblokkeerd raken voor L2-verkeer (en dit zou makkelijk kunnen gebeuren als ze deelnemen aan dezelfde STP als IP VLAN's), wordt het overlay L3-verkeer onopzettelijk ook uitgeschakeld - een ongewenst neveneffect. VLAN-bridge is daarom een afzonderlijk geval van STP voor overbrugde protocollen, dat een afzonderlijke topologie biedt die kan worden gemanipuleerd zonder IP-verkeer te beïnvloeden.

De aanbeveling van Cisco is VLAN-bridge te gebruiken als er een overbrugging tussen VLAN's op

Cisco-routers zoals de MSFC is vereist.

PortFast

PortFast wordt gebruikt om normaal Spanning Tree-gebruik op toegangspoorten te omzeilen om connectiviteit tussen eindstations en de services te versnellen die ze nodig hebben om verbinding te maken na initialisatie van de link. Op sommige protocollen, zoals IPX/SPX, is het belangrijk om de toegangspoort in verzendmodus te zien onmiddellijk nadat de verbindingsstaat is gestegen om GNS-problemen te voorkomen.

Raadpleeg Portfast en Overige opdrachten gebruiken om de aansluittijden voor startvertraging bij werkstations voor meer informatie op te slaan.

Overzicht

PortFast slaat de normale `luisterstaat` en `leerstatus` van STP over door een poort rechtstreeks te verplaatsen van `blokkeren` naar `doorsturen` mode nadat bekend is dat de link actief is. 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 kan tot tweemaal de vertragingstijd van `voorwaartse` vertraging in beslag nemen (standaard 30 seconden).

De modus PortFast voorkomt ook dat een STP TCN wordt gegenereerd elke keer dat een havenstaat van het `leren` naar het `verzenden` verandert. TCN's zijn op zichzelf geen probleem, maar als een golf van GN's de root-brug raakt (meestal 's morgens wanneer mensen hun pc's aanzetten), kan de convergentietijd onnodig verlengd worden.

STP PortFast is vooral belangrijk in zowel multicast CGMP als Catalyst 5500/5000 MLS-netwerken. TCN's in deze omgevingen kunnen ervoor zorgen dat de statische CGMP CAM-tabelingangen worden uitgerold, wat resulteert in multicast pakketverlies tot het volgende IGMP-rapport, en/of MLS-cache-items spoelen die dan opnieuw moeten worden opgebouwd en kan resulteren in een CPU-punt, afhankelijk van de grootte van het cache. (Catalyst 6500/6000 MLS implementaties en multicast items die zijn geleerd van IGMP-snooping, worden niet beïnvloed.)

Aanbeveling

Cisco raadt aan om STP PortFast aan te zetten voor alle actieve host-poorten en uitgeschakeld voor switch-switch links en poorten die niet in gebruik zijn.

Trunking en kanalisatie moeten ook voor alle poorten van ontvangst worden uitgeschakeld. Elke toegangspoort is standaard ingeschakeld voor trunking en channeling, maar switch buren worden niet verwacht door design op host-poorten. Als deze protocollen overblijven om te onderhandelen, kan de vertraging in poortactivering leiden tot ongewenste situaties waarin aanvankelijke pakketten van werkstations, zoals DHCP-verzoeken, niet worden doorgestuurd.

CatOS 5.2 introduceerde een macro commando, **stel *port host* host *port range* in** dat deze configuratie implementeert voor access poorten en dat de autonome onderhandeling en verbindingsprestaties aanzienlijk helpt:

```
set port host port range
!--- Macro command for these commands: set spantree portfast port range enable set trunk port
```

```
range off set port channel port range mode off
```

N.B.: PortFast betekent niet dat Spanning Tree helemaal niet op die poorten wordt uitgevoerd. BPDU's worden nog steeds verzonden, ontvangen en verwerkt.

Andere opties

PortFast BPDU-Guard biedt een manier om loops te voorkomen door een niet-trunking poort naar een `foutmelding` te verplaatsen wanneer er een BPDU op die poort wordt ontvangen.

Een BPDU-pakket moet nooit op een toegangspoort worden ontvangen die voor PortFast is geconfigureerd, omdat host-poorten niet aan switches moeten worden gekoppeld. Als een BPDU wordt waargenomen, duidt dit op een ongeldige en mogelijk gevaarlijke configuratie die bestuurlijke actie nodig heeft. Wanneer de BPDU-Guard optie is ingeschakeld, sluit Spanning Tree PortFast-geconfigureerde interfaces af die BPDU's ontvangen in plaats van deze in de STP-`blokkerende` staat te zetten.

De opdracht werkt per switch, niet per poort, zoals wordt aangegeven:

```
set spantree portfast bpdu-guard enable
```

De netwerkbeheerder wordt geïnformeerd door een SNMP val of syslog bericht als de poort naar beneden gaat. Het is ook mogelijk om een automatische hersteltijd te configureren voor onjuist weergegeven poorten. Raadpleeg het gedeelte UDLD-status van dit document voor meer informatie. Raadpleeg voor meer informatie de Verbetering in Spanning Tree Portfast BPDU Guard.

Opmerking: PortFast voor boomstampoorten is geïntroduceerd in CatOS 7.x en heeft geen effect op boomstampoorten in eerdere releases. PortFast voor kofferpoorten is ontworpen om de convergentieturen voor L3-netwerken te verhogen. Ter aanvulling van deze optie, introduceerde CatOS 7.x ook de mogelijkheid van configuratie van PortFast BPDU-Guard per poort.

UplinkFast

UplinkFast voorziet in snelle STP-convergentie na een onderbreking van de directe verbinding in de laag van de netwerktoegang. Het wijzigt STP niet, en het doel is de convergentietijd in een bepaalde omstandigheid te versnellen tot minder dan drie seconden, in plaats van de typische vertraging van 30 seconden. Raadpleeg het begrip van Cisco en het configureren van de snelle optie voor Cisco voor meer informatie.

Overzicht

Gebruik het Cisco meerlaagse ontwerpmodel bij de toegangslaag, als de expediteuplink verloren is, wordt de blokkerende uplink onmiddellijk naar een verzendende staat verplaatst zonder op `het luisteren` en `het leren` van staten te wachten.

Een uplink-groep is een verzameling poorten per VLAN die kan worden beschouwd als een root-poort en een back-upwortelpoort. Onder normale omstandigheden zorgen de wortelpoort(en) voor connectiviteit van de toegang naar de wortel. Als deze primaire basisverbinding om wat voor

reden dan ook faalt, klokt de backup root link direct in zonder dat ze door typische 30 seconden van convergentievertraging hoeven te gaan.

Omdat dit effectief het normale proces van het veranderen van de topologie van STP (het `luisteren` en het `leren`) voorbij gaat, is een afwisselend correctiemechanisme van de topologie nodig om switches in het domein bij te werken dat de lokale eindstations door een afwisselend pad bereikbaar zijn. De switch van de toegangslaag die UplinkFast runt genereert ook frames voor elk MAC-adres in zijn CAM naar een multicast MAC-adres (100-0c-cd-cd, HDLC-protocol 0x200a) om de CAM-tabel in alle switches in het domein met de nieuwe topologie bij te werken.

Aanbeveling

Cisco raadt aan om UplinkFast aan te zetten voor switches met geblokkeerde poorten, meestal op de toegangslaag. Gebruik deze niet op switches zonder de impliciete topologie kennis van een backup root link - distributieproducten en core switches in het Cisco meerlaagse ontwerp. Het kan zonder verstoring aan een productienetwerk worden toegevoegd. Geef deze opdracht uit om UplinkFast in te schakelen:

```
set spantree uplinkfast enable
```

Deze opdracht stelt ook de **overbruggingsprioriteit** hoog in om het risico dat dit een root-brug wordt te minimaliseren en de **havenprioriteit** hoog om te minimaliseren dat het een aangewezen haven wordt, die de functionaliteit breekt, wordt. Wanneer u een switch herstelt die UplinkFast ingeschakeld had, moet deze functie worden uitgeschakeld, moet de uplink-database worden gewist met "duidelijke uplink" en moeten de bridge prioriteiten handmatig worden hersteld.

Opmerking: het **alle protocollen** sleutelwoord voor de opdracht UplinkFast is nodig wanneer de protocol filterfunctie is ingeschakeld. Aangezien 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 de** snelheid wijst op de pakketten per seconde van de uplinkfast topologie update frames. Deze standaard wordt aanbevolen. U hoeft Backbone Fast niet te configureren met Rapid STP (RSTP) of IEEE 802.1w omdat het mechanisme automatisch in RSTP is opgenomen en automatisch ingeschakeld.

BackboneFast

BackboneFast zorgt voor snelle convergentie van indirecte blunders. Met de extra functionaliteit voor STP kunnen de convergentietijden doorgaans worden verkort van de standaard 50 seconden tot 30 seconden.

Overzicht

Het mechanisme wordt van start gegaan wanneer een wortelhaven of een geblokkeerde haven op een switch inferieure BPDU's van zijn aangewezen brug ontvangt. Dit kan gebeuren wanneer een switch downstream zijn verbinding met de wortel heeft verloren en zijn eigen 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 normale regels van de Spanning Tree negeert de ontvangende switch inferieure BPDU's voor de ingestelde maximale verouderingstijd, 20 seconden standaard. Echter, met BackboneFast, ziet de switch de inferieure BPDU als een signaal dat de topologie had kunnen veranderen, en probeert te bepalen of het een afwisselend pad naar de root-brug heeft met Root Link Query (RLQ) BPDU's. Deze protocoltoevoeging stelt een switch in staat om te controleren of de wortel nog beschikbaar is, beweegt een `geblokkeerde` poort naar `verzending` in minder tijd, en waarschuwt de geïsoleerde switch die de inferieure BPDU heeft verstuurd dat de wortel er nog is.

Dit zijn een paar hoogtepunten van de protocolhandeling:

- Een switch geeft het RLQ-pakket alleen het basispoort over (in de richting van de root-brug).
- Een switch die een RLQ ontvangt kan of beantwoorden als het de switch van de wortel is, of als het weet dat het verbinding met de wortel heeft verloren. Als het deze feiten niet kent, moet het de vraag zijn wortelhaven uitzenden.
- Als een switch een verbinding met de wortel heeft verloren, moet deze in het negatieve antwoord op deze vraag beantwoorden.
- Het antwoord moet alleen worden verstuurd naar 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 niet-wortelhaven wordt ontvangen, wordt het verworpen.

STP-convergentietijden kunnen daarom met maximaal 20 seconden worden verkort, aangezien maxage niet hoeft te verlopen.

Raadpleeg het gedeelte Inzicht en backbone Fast configureren op Catalyst-Switches voor meer informatie.

Aanbeveling

De aanbeveling van Cisco is BackboneFast op alle switches die STP uitvoeren in te schakelen. Het kan zonder verstoring aan een productienetwerk worden toegevoegd. Geef deze opdracht uit om BackboneFast mogelijk te maken:

```
set spantree backbonefast enable
```

Opmerking: Deze opdracht op mondiaal niveau moet op alle switches in een domein worden geconfigureerd omdat deze functionaliteit toevoegt aan het STP-protocol dat alle switches moeten begrijpen.

Andere opties

Backbone Fast wordt niet ondersteund op 2900XL's en 3500s. Het moet niet worden ingeschakeld als het switch-domein deze switches bevat naast Catalyst 4500/4000, 5500/5000 en 6500/6000 switches.

U hoeft Backbone Fast niet te configureren met RSTP of IEEE 802.1w, 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 L2 netwerken tegen lijnen die worden veroorzaakt door:

- Netwerkinterfaces die defect zijn
- Zakelijke CPU’s
- Alles wat het normale doorsturen van BPDU's verhindert

Een STP lijn komt voor wanneer een blokkerende haven in een overtollige topologie ten onrechte overschakelt naar de door:sturen staat. Deze overgang gebeurt gewoonlijk omdat een van de havens in een fysisch redundante topologie (niet noodzakelijk de blokkerende haven) ophoudt BPDU's te ontvangen.

Loop Guard is alleen handig in geschakelde netwerken waar switches verbonden zijn door point-to-point links. De meeste moderne campus en datacenternetwerken zijn dit soort netwerken. Op een point-to-point link kan een aangewezen brug niet verdwijnen tenzij hij een inferieure BPDU verstuurt of de link naar beneden brengt. De functie STP loop Guard is geïntroduceerd in CatOS versie 6.2(1) voor Catalyst 4000- en Catalyst 5000-platforms, en in versie 6.2(2) voor Catalyst 6000-platform.

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

Overzicht

Loop Guard controles om te bepalen of een wortelpoort of een alternatieve/backup root poort BPDU's ontvangt. Als de poort geen BPDU's ontvangt, zet loop Guard de poort in een inconsistente staat (blokkerend) tot de poort begint om BPDU's opnieuw 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 loop-inconsistente voorwaarde wordt uit de haven verwijderd, en STP bepaalt de havenstaat omdat zulk herstel automatisch is.

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 in gebruik. Er is geen afhankelijkheid van STP zelf (802.1d of 802.1w) of wanneer de STP-timers worden aangepast. Om deze redenen, gebruik loop Guard in combinatie met UDLD in topologieën die op STP vertrouwen en waar de software de eigenschappen ondersteunt.

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

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state.
```

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

```
SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

Interactie met andere STP-functies

- **Root Guard**Root Guard dwingt een haven aan te wijzen. Loop Guard is alleen effectief als de haven de wortelhaven of een alternatieve haven is. Deze functies sluiten elkaar uit. Loop Guard en root Guard kunnen niet tegelijkertijd in een haven worden ingeschakeld.
- **UplinkFast**Loop Guard is compatibel met UplinkFast. Als loop Guard een wortelpoort in een blokkerende staat zet, zet UplinkFast een nieuwe wortelhaven in door:sturen staat. Ook selecteert UplinkFast geen loop-inconsistente poort als wortelpoort.
- **BackboneFast**Loop Guard is compatibel met Backbone Fast. De ontvangst van een inferieure BPDU die van een aangewezen brug komt leidt tot BackboneFast. Omdat BPDU's van deze link worden ontvangen, wordt loop Guard niet geactiveerd, zodat BackboneFast en loop Guard compatibel zijn.
- **PortFast**PortFast overschakelt een poort naar de verzendende aangewezen staat onmiddellijk na verbinding. Omdat een PortFast-enabled poort geen wortel of alternatieve poort kan zijn, 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. Om echter een kanaal te vormen, moeten alle fysieke poorten die in het kanaal zijn gegroepeerd, compatibele configuraties hebben. PAgP dwingt de uniforme configuratie van de lus op alle fysieke poorten om een kanaal te vormen.**Opmerking:** dit zijn voorbehouden bij het configureren van loop bewaken op een EtherChannel:STP kiest 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 poorten die al geblokkeerd zijn door loop Guard gegroepeerd zijn om een kanaal te vormen, verliest STP alle staatsinformatie voor die poorten. De nieuwe kanaalpoort kan de verzendende staat bereiken met een aangewezen rol.Als een kanaal wordt geblokkeerd door loop Guard en het kanaal breekt, verliest STP alle staatsinformatie. De individuele fysieke havens kunnen de verzendende staat bereiken met een specifieke rol, zelfs als één of meer van de verbindingen die het kanaal vormden eenrichtings zijn.In de laatste twee gevallen in deze lijst is er een mogelijkheid van een lus tot UDLD de storing detecteert. Maar loop Guard kan de lus niet detecteren.

Loop Guard en UDLD-functievergelijking

De functie Loop Guard en de functie UDLD overlappen elkaar gedeeltelijk. Beveiliging tegen STP-fouten die worden veroorzaakt door unidirectionele koppelingen. Deze twee kenmerken verschillen echter van aanpak tot probleem en ook van functionaliteit. Met name zijn er bepaalde 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 waarin de link zich sinds de koppeling in één richting heeft bevonden. In het geval dat de link sinds de koppeling in één richting is gericht, ontvangt de haven nooit BPDU's en wordt aangewezen. Dit gedrag kan normaal zijn, dus loop Guard doet dit specifieke geval niet. UDLD biedt bescherming tegen een dergelijk scenario.

Schakel zowel UDLD als loop Guard in om het hoogste beschermingsniveau te bieden. Raadpleeg de Loop Guard *vs. Unidirectional Link Detection* sectie van Spanning-Tree Protocol-verbeteringen met Loop Guard en BPDU Skew Detectie-functies voor een lus Guard en UDLD-functievergelijking.

Aanbeveling

Cisco raadt u aan om lusbeveiliging wereldwijd op een netwerk van de switch met fysieke lijnen toe te laten. In versie 7.1(1) van de Catalyst software en later kunt u loop Guard wereldwijd inschakelen op alle poorten. Deze optie is ingeschakeld voor alle point-to-point links. De duplexstatus van de link detecteert de point-to-point link. Als duplex vol is, wordt de link beschouwd als point-to-point. Geef deze opdracht uit om global loop Guard in staat te stellen:

```
set spantree global-default loopguard enable
```

Andere opties

Voor switches die de configuratie van het globale netwerk niet ondersteunen, schakelt u deze functie in op alle afzonderlijke poorten, die poortkanaalpoorten omvatten. Hoewel er geen voordelen zijn voor het inschakelen van loop Guard op een aangewezen haven, is deze mogelijkheid geen probleem. Bovendien kan een geldige oversparing boomreconversie een aangewezen haven in een wortelhaven in feite veranderen, wat de eigenschap op deze haven nuttig maakt. Geef deze opdracht uit om loop Guard in staat te stellen:

```
set spantree guard loop mod/port
```

Netwerken met lus-vrije topologieën kunnen nog steeds van loopGuard profiteren in het geval dat de loops per ongeluk worden geïntroduceerd. Echter, het inschakelen van loop Guard in dit type topologie kan tot problemen van de netwerkisolatie leiden. Om lus-vrije topologieën te bouwen en netwerk isolatieproblemen te vermijden, geven deze opdrachten uit om loopGuard of afzonderlijk uit te schakelen. Schakel lusbeveiliging niet op gedeelde koppelingen in.

- ```
  set spantree global-default loopguard disable
  !--- This is the global default.
  ```
  of
- ```
  set spantree guard none mod/port
  !--- This is the default port 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 root-brug haar positie behoudt. Root Guard is beschikbaar in CatOS voor Catalyst 29xx, 4500/4000, 5500/5000 en 6500/6000 in softwareversie 6.1.1 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. Wanneer root Guard wordt toegepast op een haven, laat root Guard geen poort toe om een root port te worden. Als ontvangst van een BPDU een omspannend boomconvergentie veroorzaakt die een aangewezen haven een wortelhaven wordt, wordt de haven in een wortel-inconsistente staat gezet. Dit slogan-bericht laat de actie zien:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated
in VLAN 77. Moved to root-inconsistent state
```

Nadat de poort is gestopt om superieure BPDU's te verzenden, wordt de poort opnieuw ontgrendeld. Door STP, gaat de haven van de luisterstaat naar de leerstaat, en uiteindelijk gaat de overstap naar de staat van het verzenden. Herstel is automatisch en menselijke interventie is niet nodig. Dit syslogbericht geeft een voorbeeld:

```
%SPANTREE-2-ROOTGUARDUNBLOCK: Port 1/1 restored in VLAN 77
```

Root Guard dwingt een aan te wijzen haven en loop Guard is alleen effectief als de haven de wortelhaven of een alternatieve haven is. Daarom sluiten beide functies elkaar uit. Loop Guard en root Guard kunnen niet tegelijkertijd in een haven worden ingeschakeld.

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

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. Geef deze opdracht uit om root Guard te configureren:

```
set spantree guard root mod/port
```

EtherChannel

EtherChannel-technologieën maken het inverse multiplexing van meerdere kanalen (tot acht op Catalyst 6500/6000) mogelijk in één logische link. Hoewel bij de implementatie ieder platform van het volgende verschilt, is het belangrijk om de gemeenschappelijke vereisten te begrijpen:

- Een algoritme om statistisch multiplex frames via meerdere kanalen te vermenigvuldigen
- Creatie van een logische poort zodat één exemplaar van STP kan worden uitgevoerd
- Een kanaalbeheerprotocol zoals PAgP of Link Aggregation Control Protocol (LACP)

Frame Multiplexing

EtherChannel omvat een frame-distributiealgoritme dat efficiënt kaders over de component 10/100 of 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 belastingsdistributie is een globale optie voor beide kanaalcontroleprotocollen. PAgP en LACP gebruiken het frame distributiealgoritme omdat de IEEE-standaard geen specifieke distributie algoritmen toestaat. Echter, 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.

Opmerking: Deze informatie moet in aanmerking worden genomen:

- Catalyst 6500/6000 heeft meer recente switching-hardware dan Catalyst 5500/5000 en kan IP Layer 4 (L4) informatie via draad lezen om een intelligenter multiplexing-besluit te nemen dan eenvoudige MAC L2-informatie.
- De Catalyst 5500/5000-functies hangen af van de aanwezigheid van een Ethernet Bundling Chip (EBC) op de module. De **show port mogelijkheden *mod/port*** opdracht bevestigt wat mogelijk is voor elke poort.

Raadpleeg deze tabel, die het frame-distributiealgoritme in detail aangeeft voor elk vermeld platform:

platform	Taaltaakverdeling
Catalyst 5500/5000 Series switch	Een Catalyst 5500/5000 met de nodige modules maakt het mogelijk per FEC[1] twee tot vier koppelingen te vertonen, hoewel zij op dezelfde module moeten staan. Bron en van de bestemming MAC adresparen bepalen de verbinding die voor het frame door te sturen wordt gekozen. Een X-OR bewerking wordt uitgevoerd op de minst significante twee bits van het bron-MAC-adres en het doeladres van MAC. Deze bewerking levert één van de vier resultaten op: (0 0), (0 1), (1 0), of (1 1). Elk van deze waarden wijst op een link in de FEC bundel. In het geval van een twee-poorts Fast EtherChannel wordt slechts één bit gebruikt in de X-OR bewerking. De omstandigheden kunnen voorkomen waar één adres in het bron/doelpaar een constante is. De bestemming kan bijvoorbeeld een server of, nog waarschijnlijker, een router zijn. In dat geval wordt een statistische taakverdeling gezien omdat het bronadres altijd anders is.
Catalyst 4500/4000 Series-switches	Catalyst 4500/4000 EtherChannel verspreidt frames via de koppelingen in een kanaal (via één module) op basis van de laagorder bits van de bron- en doeladressen van elk frame. In vergelijking met Catalyst 5500/5000 is de algoritme meer betrokken en gebruikt een deterministische hash van deze velden van de MAC DA (bytes 3, 5, 6), SA (bytes 3, 5, 6), ingress poort en VLAN-ID. De frame distributiemethode is niet configureerbaar.
Catalys	Er zijn twee mogelijke hashing algoritmen,

t 6500/6000 Series-switches	afhankelijk van de hardware van de Supervisor Engine. De hash is een polynominaal van 17 graden geïmplementeerd in hardware die, in alle gevallen, het MAC-adres, IP-adres of IP TCP/UDP[2]-poortnummer neemt en het algoritme toepast om een waarde van drie bits te genereren. Dit gebeurt afzonderlijk voor zowel bron- als doeladressen. De resultaten zijn dan XORd om een andere waarde met drie bits te genereren die wordt gebruikt om te bepalen welke poort in het kanaal wordt gebruikt om het pakket door te sturen. Kanalen op Catalyst 6500/6000 kunnen tussen poorten op elke module worden gevormd en kunnen tot 8 poorten zijn.

[1] FEC = Fast EtherChannel

[2] UDP = User Datagram Protocol

Deze tabel geeft de distributiemethoden aan die worden ondersteund op de verschillende modellen van Catalyst 6500/6000 Supervisor Engine en hun standaardgedrag.

Hardware	Beschrijving	Distributiemethoden
WS-F6020 (L2-motor)	Early Supervisor Engine 1	L2 MAC: SA; DA; SA & DA
WS-F6020A (L2-motor) WS-F6K-PFC (L3-motor)	Later Supervisor Engine 1 en Supervisor Engine 1a/PFC1	L2 MAC: SA; DA; SA & DA L3 IP: SA; DA; SA en DA (standaard)
WS-F6K-PFC2	Supervisor Engine 2/PFC2 (behoeften: CatOS 6.x)	L2 MAC: SA; DA; SA & DA L3 IP: SA; DA; SA & DA (standaard) L4 sessie: S-poort; D-poort; S & D-poort (standaard)
WS-F6K-PFC3BXL WS-F6K-PFC3B WS-F6K-PFC3A	Supervisor Engine 720/PFC3A (behoeften CatOS 8.1.x) Supervisor Engine 720/Supervisor Engine 32/PFC3B (behoeften CatOS 8.4.x) Supervisor Engine 720/PFC3BXL (behoeften CatOS 8.3.x)	L2 MAC: SA; DA; SA & DA L3 IP: SA; DA; SA & DA (standaard) L4 sessie: S-poort; D-poort; S & D poort op IP-VLAN-L4 sessie: SA & VLAN & S poort;

		DA- en VLAN- en D-poort; SA & DA & VLAN EN S poort en D

Opmerking: bij L4-distributie gebruikt het eerste gefragmenteerde pakje L4-distributie. Alle volgende pakketten gebruiken L3 distributie.

Meer informatie over de EtherChannel-ondersteuning op andere platforms en de manier waarop u deze kunt configureren en oplossen, is in deze documenten te vinden:

- De betekenis van EtherChannel-taakverdeling en redundantie op Catalyst-Switches
- EtherChannel configureren tussen Catalyst 4500/4000, 5500/5000 en 6500/6000 Switches die CatOS-systeemsoftware uitvoeren
- LACP configureren (802.3ad) tussen een Catalyst 6500/6000 en een Catalyst 4500/4000
- Layer 3 en Layer 2 EtherChannel configureren

Aanbeveling

Catalyst 6500/6000 Series switches voeren een taakverdeling door IP-adres standaard uit. Dit wordt aanbevolen in CatOS 5.5, ervan uitgaande dat IP het dominante protocol is. Geef deze opdracht uit om de taakverdeling in te stellen:

```
set port channel all distribution ip both
!--- This is the default.
```

Catalyst 4500/4000 en 5500/5000 Series frame-distributie door L2 MAC-adres is aanvaardbaar in de meeste netwerken. Echter, de zelfde verbinding wordt gebruikt voor al verkeer als er slechts twee hoofdapparaten zijn die over een kanaal spreken (zoals SMAC en DMAC constant zijn). Dit kan meestal een probleem zijn voor back-up van servers en andere grote bestandsoverdrachten of voor een doorvoersegment tussen twee routers.

Hoewel het logische aggregaat poort (poort) door SNMP als afzonderlijk geval en geaggregeerde doorvoerstatistieken kan worden beheerd die kunnen worden verzameld, raadt Cisco nog steeds aan elk van de fysieke interfaces afzonderlijk te beheren om te controleren hoe de frame distributiesystemen werken en of er een statistisch taakverdeling wordt bereikt.

Een nieuwe opdracht, de opdracht van het verkeersnet van het kanaal tonen, in CatOS 6.x kan de statistieken van de procentuele distributie makkelijker weergeven dan als u individuele poorttellers met de opdracht Mod/poort van de show tellers of de *mac mod/port* in CatOS 5.x controleert. Een andere nieuwe opdracht, de **opdracht** Show Channel Hash**,** in CatOS 6.x staat u toe om, op basis van de distributiemodus, te controleren welke poort als de vertrekpoort voor bepaalde adressen en/of poortnummers wordt geselecteerd. De equivalente opdrachten voor LACP-kanalen zijn de show lacp-kanaalverkeersopdracht **en de** show **hap-opdracht.**

Andere opties

Dit zijn mogelijke stappen om te zetten indien de relatieve beperkingen van Catalyst 4500/4000 of Catalyst 5500/5000 MAC-gebaseerde algoritmen een probleem zijn en er geen goed statistisch taakverdeling wordt bereikt:

- IP-telefoon 6500/6000 switches
- Vergroot de bandbreedte zonder het kanaliseren door bijvoorbeeld van verschillende FE-poorten naar één GE-poort te schakelen, of van verschillende GE-poorten naar één 10 GE-poort
- Paren van eindstations met grote volumestromen opnieuw adresseren
- Voorziening voor speciale links/VLAN's voor hoge bandbreedte-apparaten

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. Volg de richtsnoeren om problemen bij bundeling te voorkomen. Als QoS bijvoorbeeld is ingeschakeld, vormen EtherChannel niet bij het bundelen van Catalyst 6500/6000 Series switchmodules met verschillende QoS-functies. In Cisco IOS-software kunt u de QoS poortcontrole op de EtherChannel-bundeling uitschakelen met de **opdracht no-mls QoS kanaalconsistentie-**interface. Een equivalente opdracht om de QoS poortcontrole uit te schakelen is niet beschikbaar in CatOS. U kunt de opdracht poortcapaciteit/*poort* geven om de QoS poortmogelijkheden weer te geven en bepalen of poorten compatibel zijn.

Volg deze richtlijnen voor verschillende platforms om configuratieproblemen te voorkomen:

- Het *gedeelte EtherChannel Configuration Guidelines* van de configuratie van EtherChannel (Catalyst 6500/6000)
- Het *gedeelte-configuratierichtlijnen en -beperkingen* van de configuratie van Fast EtherChannel en Gigabit EtherChannel (Catalyst 4500/4000)
- Het *gedeelte-configuratierichtlijnen en -beperkingen* van de configuratie van Fast EtherChannel en Gigabit EtherChannel (Catalyst 5000)

Opmerking: Het maximale aantal poortkanalen dat door Catalyst 4000 wordt ondersteund, is 126. Met softwarerelease 6.2(1) en eerder, ondersteunen de switches van Catalyst 6500-serie met zes en negen sleuven maximaal 128 EtherChannel. In softwarerelease 6.2(2) en latere releases verwerkt de omspannende boomfunctie de poort-ID. Daarom is het maximale aantal EtherChannel met ondersteuning 126 voor een chassis met zes of negen sleuven en 63 voor een chassis met 13 sleuven.

Poortaggregatieprotocol

PAgP is een beheerprotocol dat op een van de eindpunten van de link de parameter consistent controleert en het kanaal helpt bij het aanpassen aan een fout of toevoeging. Let op deze feiten over 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, zijn ze niet in EtherChannel-deelname opgenomen.)
- Wanneer een bundel reeds bestaat en de configuratie van één haven wordt aangepast (zoals veranderen VLAN of trunking mode), worden alle havens in de bundel aangepast om die configuratie aan te passen.
- 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 wordt gegroepeerd. PAgP-pakketten worden verzonden met behulp van hetzelfde multicast MAC-adres dat voor CDP-pakketten wordt gebruikt, **01-00-0c-cc-cc-cc**. 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.
- Het protocol luistert naar PAgP-pakketten waaruit blijkt dat de fysieke poort een bidirectionele verbinding heeft met een ander PAgP-compatibel apparaat.
- Als gegevenspakketten maar geen PAgP pakketten worden ontvangen, wordt aangenomen dat de poort is aangesloten op een niet-PAgP geschikt apparaat.
- Zodra twee PAgP pakketten op een groep fysieke poorten zijn ontvangen, probeert het om een geaggregeerde poort te vormen.
- Als de PAgP-pakketten een periode worden geblokkeerd, wordt de PAgP-status `afgebroken`.

Normale verwerking

Deze concepten moeten worden gedefinieerd om inzicht te geven in het gedrag van het protocol:

- **Voorwaarde**: een logische poort samengesteld uit alle fysieke poorten in dezelfde aggregatie, kan het geïdentificeerd worden door zijn eigen SNMP als Index. Daarom bevat een agentschap geen niet-operationele havens.
- **Kanaal**: een aggregatie die voldoet aan de formatiecriteria; het zou derhalve niet-operationele havens kunnen omvatten (de havens zijn een deelgroep van kanalen). Protocols zoals STP en VTP, maar exclusief CDP en DTP, draaien boven PAgP via de poorten. Geen van deze protocollen kan pakketten verzenden of ontvangen tot PAgP hun poorten aan een of meer fysieke poorten bevestigt.
- **De capaciteit** van de **groep**—elke fysieke poort en de agport heeft een configuratieparameter die de groep-vermogen wordt genoemd. Een fysieke poort kan met een andere fysieke poort worden geaggregeerd indien en alleen indien deze dezelfde groepscapaciteit hebben.
- **Aggregatieprocedure** - wanneer een fysieke poort de `UpData` of `UpPAgP` staten bereikt, wordt de poort aangesloten op een geschikte instantie. Als het een van deze staten voor een andere staat verlaat, is het los van de steun.

In deze tabel worden de definities van de staten en de creatieprocedures gegeven:

Staat	Betekenis
`UpData`	Er zijn geen PAgP-pakketten ontvangen. PAgP-pakketten worden verzonden. De fysieke poort is de enige die aangesloten is op de poort. De niet-PAgP pakketten worden binnen en uit tussen fysieke haven en haven doorgegeven.
`BiDi`	Er is precies één pakje PAgP ontvangen dat bewijst

r	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 binnen en uit tussen fysieke haven en haven doorgegeven.

Beide uiteinden van beide verbindingen moeten het eens worden over wat de groepering zal zijn, gedefinieerd als de grootste groep havens in de haven die door beide uiteinden van de verbinding wordt toegestaan.

Wanneer een fysieke poort de staat `UpPAgP` bereikt, wordt deze 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` of `UpPAgP` staten zijn. (Al deze BiDir-poorten worden tegelijkertijd naar de UpPAgP verplaatst.) Als er geen instantie is waarvan de samenstellende fysieke poortparameters compatibel zijn met de nieuw gereed fysieke poort, wordt deze toegewezen aan een instantie met geschikte parameters die geen bijbehorende fysieke poorten heeft.

Een PAgP tijd kan op de laatste buur voorkomen die op de fysieke haven bekend is. De haventiming uit de haven wordt verwijderd. Tegelijkertijd worden alle fysieke poorten op dezelfde poort waarvan de timers ook zijn uitgetimed, 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 bestaand kanaal niet is ingeschakeld (bijvoorbeeld poort unplugged, Gigabit-interfaceconvertor [GBIC] verwijderd of glasvezel kapot), wordt de pagina bijgewerkt en wordt het verkeer binnen één seconde over de resterende links ingedrukt. Elk verkeer dat niet hoeft te worden aangehouden na de mislukking (verkeer dat op dezelfde link blijft verzenden) lijdt niet onder enig verlies. Herstel van de mislukte verbinding leidt tot een andere update aan de haven, en het verkeer wordt opnieuw gehashed.

Opmerking: het gedrag wanneer een link in een kanaal mislukt als gevolg van een stroomuitval of de verwijdering van een module kan anders zijn. Per definitie moeten er twee fysieke poorten zijn naar een kanaal. Als een poort van het systeem verloren is in een twee-poorts kanaal, wordt de logische poort naar beneden gehaald en wordt de oorspronkelijke fysieke poort opnieuw geïnitialiseerd met betrekking tot Spanning Tree. Dit betekent dat verkeer kan worden weggegooid totdat STP de poort beschikbaar maakt voor gegevens opnieuw.

Er is een uitzondering op deze regel op Catalyst 6500/6000. In versies eerder dan CatOS 6.3 wordt een subsidie niet `afgebroken` tijdens het verwijderen van de module indien het kanaal is samengesteld uit havens op modules 1 en 2.

Dit verschil in de twee mislukkingsmodi is belangrijk wanneer onderhoud van een netwerk gepland is, aangezien er een STP TCN kan zijn die moet overwegen bij het uitvoeren van on-line verwijdering of plaatsing van een module. Zoals gezegd, is het belangrijk elke fysieke verbinding in het kanaal met de MNS te beheren, aangezien de MNS niet door een storing kan worden

verstoord.

Dit zijn voorgestelde stappen om een ongewenste verandering van topologie op Catalyst 6500/6000 te verminderen:

- Als per module één poort wordt gebruikt om een kanaal te vormen, moeten er drie of meer modules worden gebruikt (drie poorten of meer totaal).
- Als het kanaal twee modules uitslaat, moeten twee poorten op elke module worden gebruikt (vier poorten totaal).
- Als een twee-poorts kanaal nodig over twee kaarten is, gebruik dan alleen de poorten van de Supervisor Engine.
- upgrade naar CatOS 6.3, waarmee moduleverwijdering zonder STP-herberekening wordt verwerkt voor kanalen die over modules zijn verdeeld.

Configuratieopties

EtherChannel kan in verschillende modi worden geconfigureerd, zoals in deze tabel wordt samengevat:

Modus	Configureerbare opties
`Aan`	PAgP niet in bedrijf. De haven verandert ongeacht hoe de buurhaven wordt gevormd. Als de buurhavenmodus is ingeschakeld, wordt er een kanaal gevormd.
`Uit`	De haven verandert niet ongeacht hoe de buur wordt gevormd.
`Auto (standaard)`	Aggregatie valt onder de controle van het PAgP-protocol. Plaatst een poort naar een passieve `onderhandelingsstatus` en er worden geen PAgP-pakketten op de interface verzonden tot ten minste één PAgP-pakket ontvangen is dat aangeeft dat de zender in de `gewenste` modus werkt.
`wenselijk`	Aggregatie valt onder de controle van het PAgP-protocol. Plaatst een haven in een actieve `onderhandelingsstaat`, waarin de haven onderhandelingen met andere havens initieert door PAgP pakketten te verzenden. Een kanaal wordt gevormd met een ander havengroep in of gewenst of automodus.
`Niet-stil` (standaard op Catal	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

yst 5500/ 5000 glasv ezel FE- en GE- poort en)	werd verstrekt voor specifieke hardware van Catalyst 5500/5000, aangezien sommige fouten van de link ertoe hebben geleid dat het kanaal wordt afgebroken. Omdat de `niet-stille` modus is ingeschakeld, mag een terugwinnende buurpoort nooit onnodig terugkomen en het kanaal uit elkaar breken. Flexibele bundeling en verbeterde bidirectionaliteitscontroles zijn standaard aanwezig in de hardware van de Catalyst 4500/4000- en 6500/6000-series.
`Silent` (stan daard op alle Catal yst 6500/ 6000 en 4500/ 4000 poort en en 5500/ 5000 koper en poort en)	Een `auto` of `wenselijk` mode sleutelwoord. Indien geen gegevenspakketten op de interface worden ontvangen, wordt na een periode van 15 seconden de interface op zichzelf aan een instantie gekoppeld en kan deze dus worden gebruikt voor gegevensoverdracht. `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 unidirectioneel verkeer veroorzaken of hoe zij faalderen. Wanneer een haven niet kan overbrengen (wegens een mislukte fysieke sublaag [PHY] of een gebroken vezel of kabel, bijvoorbeeld), kan dit de buurhaven in een operationele staat nog achterlaten. De partner blijft gegevens verzenden, maar de gegevens gaan verloren, omdat het retourverkeer niet kan worden ontvangen. Spanning Tree lusjes kunnen ook vanwege de unidirectionele aard van de link vormen.

Sommige glasvezelhavens hebben de gewenste mogelijkheid om de haven naar een niet-operationele staat te brengen wanneer het zijn ontvangstsignaal (FEFI) verliest. Dit zorgt ervoor dat de partnerhaven niet-operationeel wordt en zorgt er effectief voor dat de havens aan beide uiteinden van de verbinding naar beneden gaan.

Wanneer gebruik wordt gemaakt van apparatuur die gegevens (zoals BPDU's) doorgeeft en geen unidirectionele voorwaarden kan detecteren, moet `niet-stille` modus worden gebruikt om de havens niet-operationeel te laten blijven totdat er gegevens zijn ontvangen en is geverifieerd dat de link bidirectioneel is. De tijd die PAgP nodig heeft om een unidirectionele link te detecteren is ongeveer 3,5 * 30 seconden = 105 seconden, waar 30 seconden de tijd is tussen twee opeenvolgende PAgP-berichten. UDLD wordt aanbevolen als een snelle detector voor uni-directionele koppelingen.

Wanneer u apparaten gebruikt die geen gegevens verzenden, moet u de `stille` modus gebruiken.

Dit dwingt de haven om aangesloten en operationeel te worden ongeacht of ontvangen gegevens aanwezig zijn of niet. Daarnaast wordt de stille modus standaard gebruikt voor poorten die de aanwezigheid van een eenrichtingsvoorwaarde kunnen detecteren, zoals nieuwere platforms met L1 FEFI en UDLD.

Verificatie

In de tabel wordt een samenvatting gegeven 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 de `foutmelding` plaatst (dat wil zeggen, sommige combinaties sluiten de poorten aan de kantelzijde).

Switch-A-kanaalmodus	Switch-B-kanaalmodus	Kanaalstaat
Aan	Aan	Kanaal (niet-PAgP)
Aan	Uit	Niet kanaliseren (uitschakelen)
Aan	Automatisch	Niet kanaliseren (uitschakelen)
Aan	wenselijk	Niet kanaliseren (uitschakelen)
Uit	Aan	Niet kanaliseren (uitschakelen)
Uit	Uit	Geen kanaal
Uit	Automatisch	Geen kanaal
Uit	wenselijk	Geen kanaal
Automatisch	Aan	Niet kanaliseren (uitschakelen)
Automatisch	Uit	Geen kanaal
Automatisch	Automatisch	Geen kanaal
Automatisch	wenselijk	PAgP-kanaal
wenselijk	Aan	Niet kanaliseren (uitschakelen)
wenselijk	Uit	Geen kanaal
wenselijk	Automatisch	PAgP-kanaal
wenselijk	wenselijk	PAgP-kanaal

Aanbeveling

Cisco raadt aan om PAgP aan te zetten op alle switch-to-switch kanaalverbindingen, waarbij `wordt` vermeden `in` de modus. De geprefereerde methode is om `gewenste` modus in beide eindpunten van een link in te stellen. De aanvullende aanbeveling is om het `stille/niet-stille` sleutelwoord te laten achterwege - `stil` op Catalyst 6500/6000 en 4500/4000 switches, `niet-stil` op Catalyst 5500/5000 glasvezelpoorten.

Zoals in dit document wordt besproken, is de expliciete configuratie van het kanaliseren van gegevens op alle andere havens behulpzaam voor snelle gegevensverzending. Wachten tot 15 seconden voor PAgP op een poort die niet gebruikt zal worden voor het kanaliseren, moet vermeden worden, vooral omdat de haven dan aan STP wordt overgedragen, die zelf 30 seconden kan kosten om het doorsturen van gegevens mogelijk te maken, plus mogelijk 5 seconden voor DTP voor een totaal van 50 seconden. De opdracht **Port Host** wordt in detail besproken in het STP-gedeelte van dit document.

```
set port channel port range mode desirable

set port channel port range mode off
!--- Ports not channeled; part of the set port hostcommand.
```

Deze opdracht wijst een admingroep-nummer toe, gezien met de opdracht van een **showkanaal-groep**. Toevoeging en verwijdering van kanaliserende havens aan de zelfde instantie kunnen dan indien gewenst met het adminenummer worden beheerd.

Andere opties

Een andere gezamenlijke configuratie voor klanten die een model van minimaal beheer bij de toegangslaag hebben is om de modus in te stellen op `wenselijk` bij de distributie en kernlagen en de switches van de toegangslaag bij de standaard `automatische` configuratie te laten.

Wanneer u naar apparaten gaat die PAgP niet ondersteunen, moet het kanaal harde gecodeerd zijn. Dit is van toepassing op apparaten zoals servers, Local Director, content switches, routers, switches met oudere software, Catalyst XL switches en Catalyst 8540s. Deze opdracht geven:

```
set port channel port range mode on
```

De nieuwe 802.3ad IEEE LACP-standaard, beschikbaar in CatOS 7.x, zal PAgP op lange termijn waarschijnlijk vervangen omdat deze de voordelen van platform- en verkoopinteroperabiliteit oplevert.

Link Aggregation Control Protocol

LACP is een protocol dat havens met gelijkaardige eigenschappen toelaat om een kanaal door dynamische onderhandeling met aangrenzende switches te vormen. PAgP is een protocol dat eigendom is van Cisco dat alleen op Cisco-switches en die switches kan worden uitgevoerd die door erkende verkopers worden vrijgegeven. 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. CatOS 7.x-softwarereleases introduceerden LACP-ondersteuning.

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 haveneigenschappen worden gecontroleerd vóór de vorming van de bundel. Deze poorteigenschappen omvatten:

- Speed
- Duplex
- Native VLAN
- Type trunking

De opvallende verschillen tussen de LACP en de PAgP zijn:

- LACP kan slechts op volledig-duplex havens lopen, en LACP steunt geen half-duplex havens.
- LACP ondersteunt hot standby poorten. LACP probeert altijd het maximum aantal compatibele havens in een kanaal te vormen, tot het maximum aantal dat de hardware toestaat (acht havens). Als LACP niet in staat is om alle compatibele havens samen te voegen, worden alle havens die niet actief in het kanaal kunnen worden opgenomen in hete stand-by staat geplaatst en slechts gebruikt als één van de gebruikte havens faalt. Een voorbeeld van een situatie waarin LACP niet alle compatibele havens kan samenvoegen is wanneer het afstandssysteem meer beperkingen van de hardware kent.

Opmerking: In CatOS is het maximale aantal poorten dat dezelfde administratieve sleutel kan worden toegewezen acht. In Cisco IOS-software probeert LACP het maximale aantal compatibele poorten in een EtherChannel te configureren, tot het maximale aantal 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) haven die moet worden gebundeld. LACP-pakketten worden verzonden met gebruik van het multicast group MAC-adres, **01-80-c2-00-00-02**. De type-/veldwaarde is 0x8809 met een subtype van 0x01. Hier is een samenvatting van de protocolhandeling:

- Het protocol is gebaseerd op de middelen om hun aggregatiekansen en de overheidsinformatie bekend te maken. De transmissies worden regelmatig en periodiek verzonden ***op elke "aggregeerbare" link.***
- 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 acties zij moeten ondernemen.
- Compatibele poorten worden ingesteld in een kanaal, tot het maximum aantal 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 (bijvoorbeeld als gevolg van een koppelingsstoring), nemen de protocol partners tijd uit en nemen ze passende 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 partner toe. De partners van het protocol nemen de passende maatregelen op basis van de nieuwe stand van het systeem.

LACP-parameters

Om 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, is het nodig deze parameters vast te stellen:

- Een wereldwijd unieke identificator voor elk systeem dat deelneemt aan de aggregatie van de linkElk LACP-systeem moet een prioriteit krijgen die automatisch of door de beheerder kan worden gekozen. De systeemprioriteit is 32768. 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 bij elke poort en bij elke aggregator worden geassocieerd, zoals een bepaald systeem ze begrijptElke poort in het systeem moet een prioriteit krijgen, hetzij automatisch, hetzij door de beheerder. De standaardinstelling is 128. De prioriteit wordt gebruikt in combinatie met het havennummer om de havenidentificator te vormen.
- Een middel om een linkaggregatiegroep en de daarmee verbonden aggregator te identificerenDe 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. Deze parameter wordt de "toets" genoemd. Elke toets wordt bepaald door verschillende factoren, zoals:De fysieke eigenschappen van de haven, waaronder:GegevenspercentageduplexiteitPoint-to-Point of gedeeld mediumConfiguratiebeperkingen die de netwerkbeheerder vaststeltElke poort bevat twee toetsen:Een administratieve sleutel - Deze sleutel staat voor de manipulatie van zeer belangrijke waarden door het beheer toe. Een gebruiker kan deze toets kiezen.Een operationele sleutel—het systeem gebruikt deze toets om aggregaties te vormen. Een gebruiker kan deze toets niet kiezen of rechtstreeks wijzigen.De reeks havens in een systeem met dezelfde operationele hoofdwaarde zou deel uitmaken van dezelfde sleutelgroep.

Als je twee systemen en een set havens hebt met dezelfde administratieve sleutel, probeert elk systeem de havens samen te voegen. Elk systeem begint met de haven met de hoogste prioriteit in het systeem met de hoogste prioriteit. Dit gedrag is mogelijk omdat elk systeem zijn eigen prioriteit kent, die de gebruiker of het systeem heeft toegewezen, en zijn partnerprioriteit, die door LACP-pakketten werd ontdekt.

Gedrag in falen

Het mislukkingsgedrag van de LACP is hetzelfde als dat van de PAgP. Als een link in een bestaand kanaal is mislukt, wordt de verbinding bijgewerkt en wordt het verkeer binnen één seconde over de resterende links gehakt. Een link kan om deze en andere redenen falen:

- Een poort is verwijderd
- Een GBIC wordt verwijderd
- Een vezel is kapot
- Hardware storing (interface of module)

Elk verkeer dat niet hoeft te worden aangehouden na de mislukking (verkeer dat op dezelfde link blijft verzenden) lijdt niet onder enig verlies. Herstel van de mislukte verbinding leidt tot een andere update aan de haven, en het verkeer wordt opnieuw gehashed.

Configuratieopties

LACP EtherChannel kan in verschillende vormen worden gevormd, 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 buurpoortmodus is `ingeschakeld`, wordt een kanaal gevormd.
`Uit`	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) opent onderhandeling door een LACP-pakket te verzenden. De switch ontvangt het pakje en antwoordt daarop en vormt uiteindelijk het aggregatiekanaal met de peer.
`Actief`	Dit lijkt op de `gewenste` modus in PAgP. De switch start de onderhandeling om een 'aglink' te vormen. Het verbindingsaggregaat wordt gevormd indien het andere uiteinde in de LACP `actieve` of `passieve` modus loopt.

Verificatie (LACP en LACP)

In de tabel in dit deel wordt een samenvatting gegeven van alle mogelijke scenario's voor de kanaalmodus van de LACP tussen twee direct verbonden switches (Switch-A en Switch-B). Sommige van deze combinaties kunnen STP veroorzaken om de poorten aan de kantelzijde in de staat `foutloos` te zetten. Dit betekent dat sommige combinaties de havens aan de kanaalkant afsluiten.

Switch-A-kanaalmodus	Switch-B-kanaalmodus	Switch-A-kanaalstaat	Switch-B-kanaalstatus
`Aan`	`Aan`	`Kanaal` (niet-LACP)	`Kanaal` (niet-LACP)
`Aan`	`Uit`	`Niet kanaliseren` (uitschakelen)	`Geen kanaal`
`Aan`	`passief`	`Niet kanaliseren` (uitschakelen)	`Geen kanaal`
`Aan`	`Actief`	`Niet kanaliseren` (uitschakele	`Geen kanaal`

		n)	
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

Verificatie (LACP en PAgP)

In de tabel in dit deel wordt een samenvatting gegeven van alle mogelijke scenario's voor LACP-to-PAgP-kanalisatie tussen twee direct verbonden switches (Switch-A en Switch-B). Sommige van deze combinaties kunnen STP veroorzaken om de poorten aan de kantelzijde in de staat `foutloos` te zetten. Dit betekent dat sommige combinaties de havens aan de kanaalkant afsluiten.

Switch-A-kanaalmodus	Switch-B-kanaalmodus	Switch-A-kanaalstaat	Switch-B-kanaalstatus
Aan	Aan	`Kanaal` (niet-LACP)	`Kanaal` (niet-PAgP)
Aan	Uit	`Niet kanaliseren` (uitschakelen)	Geen kanaal
Aan	Automatisch	`Niet kanaliseren` (uitschakelen)	Geen kanaal
Aan	wenselijk	`Niet kanaliseren` (uitschakelen)	Geen kanaal
Uit	Aan	Geen kanaal	`Niet kanaliseren` (uitschakelen)
Uit	Uit	Geen kanaal	Geen kanaal
Uit	Automatisch	Geen kanaal	Geen kanaal
Uit	wenselijk	Geen kanaal	Geen kanaal
passief	Aan	Geen kanaal	`Niet kanaliseren` (uitschakelen)
passief	Uit	Geen kanaal	Geen kanaal
passief	Automatisch	Geen kanaal	Geen kanaal
passief	wenselijk	Geen kanaal	Geen kanaal
Actief	Aan	Geen kanaal	`Niet kanaliseren` (uitschakelen)
Actief	Uit	Geen kanaal	Geen kanaal
Actief	Automatisch	Geen kanaal	Geen kanaal
Actief	wenselijk	Geen kanaal	Geen kanaal

Aanbeveling

Cisco raadt u aan PAgP op kanaalverbindingen tussen Cisco-switches in te schakelen. Wanneer u naar apparaten kanaliseert die geen PAgP ondersteunen maar LACP ondersteunen, schakelt u LACP in door de configuratie van LACP `actief` op beide uiteinden van de apparaten. Als een van de uiteinden van de apparaten geen LACP of PAgP steunt, moet u hard het kanaal `aan` coderen.

- **set channelprotocol lacp** *module*

  Op switches die CatOS in werking stellen, gebruiken alle poorten op Catalyst 4500/4000 en een Catalyst 6500/6000 kanaalprotocol PAgP standaard en draaien als zodanig geen LACP. 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.

- **set port lacp-channel** *port_range admin-key*

  Een **admin key** (administratieve sleutel) parameter wordt uitgewisseld in het LACP-pakket. Een kanaal vormt alleen formulieren tussen poorten die dezelfde admintoets hebben. De **ingestelde poort**--kanaal port_range **admin-key- opdracht** kent zenders en admin-sleutelnummer toe. De opdracht **Show lacp-kanaal toont het nummer.** De **ingestelde port lacp-kanaal** ***port_range admin-key*** **opdracht wijst dezelfde admin-toets toe aan alle poorten in het poortbereik.** De admin-toets wordt willekeurig toegewezen indien een specifieke toets niet is ingesteld. Vervolgens kunt u, indien gewenst, naar de admin-toets verwijzen om de toevoeging en verwijdering van kanaliserende poorten naar dezelfde poort te beheren.

- **set port lacp-channel** *port_range* **mode active**

  De **ingestelde port lacp-kanaal** ***port_range*** **mode actieve** opdracht verandert de kanaalmodus in `actief` voor een set poorten die eerder dezelfde admin-toets kregen toegewezen.

Daarnaast maakt LACP gebruik van een 30-seconden interval timer (Slow_Periodic_Time) nadat de LACP EtherChannel is gevestigd. Het aantal seconden voor de ongeldigverklaring van ontvangen LACPDU-informatie met het gebruik van lange time-outs (3 x Slow_Periodic_Time) is 90. Gebruik UDLD, wat een snellere detector van unidirectionele koppelingen is. U kunt de LACP-timers niet aanpassen en vandaag kunt u de switches niet configureren om de snelle PDU-transmissie (elke seconde) te gebruiken om het kanaal te onderhouden nadat het kanaal is gevormd.

Andere opties

Als u een model van minimaal beheer bij de toegangslaag hebt, is een gemeenschappelijke configuratie om de modus in te stellen op `actief` bij de distributie en de kernlagen. Laat de switches van de toegangslaag bij de standaard `passieve` configuratie.

Unidirectionele linkdetectie

UDLD is een bedrijfseigen, lichtgewicht protocol van Cisco dat werd ontwikkeld om gevallen van unidirectionele communicatie tussen apparaten te detecteren. Hoewel er andere methoden zijn om de bidirectionele toestand van transmissiemedia te detecteren, zoals FEFI, zijn er bepaalde gevallen waarin de L1-detectiemechanismen niet volstaan. Deze scenario's kunnen in een van deze voorvallen resulteren:

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

De functie UDLD is bedoeld om deze foutvoorwaarden op glasvezel- en koperEthernet-interfaces aan te pakken:

- Beoordeel fysieke bekabelde configuraties en sluit om het even welke misbedrade poorten als `foutmelding` af.
- Bescherm tegen uni-directionele koppelingen. Wanneer een uni-directionele link wordt gedetecteerd, als gevolg van een media- of poort/interface-storing, wordt de getroffen poort uitgeschakeld als `foutmelding` en wordt een corresponderend syslig-bericht gegenereerd.
- Bovendien controleert de agressieve modus van UDLD of een link die eerder werd gezien als bidirectioneel, de connectiviteit tijdens de congestie niet verliest en onbruikbaar wordt. UDLD voert doorlopende connectiviteitstests over de link uit. Het primaire doel van de agressieve modus van de UDLD is het zwart bekleden van verkeer in bepaalde mislukte omstandigheden te voorkomen.

Spanning Tree, met zijn steady-state unidirectionele BPDU-stroom, was een acuut lijden door deze tekortkomingen. Het is gemakkelijk om te zien hoe een haven plotseling niet in staat kan zijn om BPDU's over te brengen, wat een STP staatsverandering van `blokkering` aan `doorsturen` op de buur veroorzaakt. Deze verandering creëert een lus, aangezien de haven nog kan ontvangen.

Overzicht

UDLD is een L2-protocol dat boven de LLC-laag werkt (bestemmings-MAC 100-0c-cc-cc, SNAP HDLC-protocol type 0x011). Wanneer UDLD in combinatie met FEFI en autonome L1-mechanismen wordt uitgevoerd, is het mogelijk de fysieke (L1) en logische (L2) integriteit van een verbinding te valideren.

UDLD beschikt over bepalingen voor functies en bescherming die FEFI en autonomie niet kunnen uitvoeren, namelijk de detectie en caching van buurinformatie, de mogelijkheid om onjuist aangesloten poorten te sluiten en logische interface/poort-storingen of fouten op verbindingen die geen punt-tot-punt zijn (die doorlopende media-converters of knooppunten) te detecteren.

UDLD gebruikt twee basismechanismen; Ze leert over de buren, houdt de informatie bij in een lokaal cache en stuurt een trein van UDLD-sonde/echo-berichten wanneer ze een nieuwe buurman detecteert of wanneer een buur om hersynchronisatie van de cache vraagt.

UDLD stuurt constant sonde berichten op alle poorten waarop UDLD is ingeschakeld. Wanneer een specifiek "triggerend" UDLD-bericht in een poort wordt ontvangen, beginnen een detectiefase en validatieproces. Indien aan het einde van dit proces aan alle geldige voorwaarden is voldaan, wordt de havenstaat niet gewijzigd. Om aan de voorwaarden te voldoen, moet de haven in twee richtingen en op de juiste wijze worden aangesloten. Anders wordt de poort `niet` ingeschakeld en worden de displays van het syslogbericht weergegeven. Het slogbericht lijkt op deze berichten:

- `UDLD-3-UITGESCHAKELD: Unidirectionele link gedetecteerd op poort [dec]/[dec].`

Poortuitgeschakeld
- UDLD-4-ONEWAYPAD: Een unidirectionele verbinding van poort [dec]/[dec] naar poort [dec]/[dec] van het apparaat [tekens] werd gedetecteerd

Raadpleeg Berichten en herstelprocedures (Catalyst series switches, 7.6) voor een volledige lijst van systeemberichten per faciliteit, die UDLD-gebeurtenissen omvat.

Nadat een link is ingesteld en als bidirectioneel is ingedeeld, blijft UDLD probe/echo-berichten adverteren met een standaardinterval van 15 seconden. Deze tabel geeft de geldige UDLD-verbindingsstaten weer zoals gerapporteerd in de uitvoer van de opdracht **van de** udld-poort:

Poortstaat	Opmerking
onbepaald	Detectie gestart, of een naburige UDLD-entiteit is uitgeschakeld of de overdracht ervan is geblokkeerd.
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-sonde/echo-pakketten op elke actieve interface om de integriteit van het UDLD buurcache te behouden. Wanneer een hallo bericht wordt ontvangen, wordt het gecached en in het geheugen gehouden gedurende een maximum periode die als de Hold-tijd wordt bepaald. Wanneer de houdtijd verstrijkt, is de respectieve cache-ingang verouderd. Als er een nieuw hallo-bericht wordt ontvangen binnen de hold-time periode, vervangt het nieuwe de oudere ingang en de overeenkomstige tijd-to-live timer wordt gereset.
- Om de integriteit van het UDLD-cache te behouden, worden alle bestaande cache-items voor de interfaces die door de configuratie worden beïnvloed, gewist wanneer een door UDLD-enabled ingestelde interface wordt uitgeschakeld of wanneer een apparaat wordt gereset, en geeft UDLD ten minste één bericht door om de respectieve buren te informeren om de corresponderende cache-items te spoelen.
- **Het Echo Detection Mechanisme** - het echomechanisme vormt de basis van het detectie algoritme. Wanneer een UDLD-apparaat over een nieuw buurland leert of een resynchronisatieverzoek van een out-of-synch buurman ontvangt, begint/herstart het detectievenster aan de zijkant van de verbinding en stuurt het een barst van echo-berichten in antwoord. Aangezien dit gedrag in alle buren hetzelfde moet zijn, verwacht de echo zender de echo's terug te ontvangen in antwoord. Als het detectievenster eindigt en er geen geldig antwoordbericht is ontvangen, wordt de link beschouwd als een eenrichtingsverkeer en kan er een koppelingsvenster of poortshutdown-proces worden geactiveerd.

Convergentietijd

Om STP loops te voorkomen, verminderde CatOS 5.4(3) het standaardberichtinterval van UDLD van 60 seconden tot 15 seconden om een unidirectionele verbinding te sluiten vóórdat een geblokkeerde poort naar een verzendende staat kon overgaan.

Opmerking: De waarde van het berichtinterval bepaalt de snelheid waarmee een buurman UDLD-

sondes na de koppeling- of detectiefase verstuurt. Het berichtinterval hoeft niet op beide uiteinden van een verbinding aan te passen, alhoewel de consistente configuratie waar mogelijk wenselijk is. Wanneer UDLD-buren worden ingesteld, wordt het geconfigureerde bericht interval verzonden en wordt het timeout interval voor dat peer berekend om te zijn (3 * bericht_interval). Daarom wordt een peer-relatie tijd uit na drie opeenvolgende hellos (of sondes) gemist. Met de berichtintervallen die aan elke kant verschillend zijn, is deze timeout waarde verschillend aan elke kant.

De geschatte tijd die nodig is voor UDLD om een unidirectionele mislukking te detecteren is ongeveer (2,5 * bericht_interval + 4 seconden), of ongeveer 41 seconden met gebruik van het standaardberichtinterval van 15 seconden. Dit is ver onder de 50 seconden die normaal nodig zijn voor STP om te converteren. Als de NMP CPU bepaalde reservecycli heeft en u het benuttingsniveau zorgvuldig controleert, kunt u het berichtinterval (zelfs) tot een minimum van 7 seconden beperken. Dit berichtinterval helpt de detectie te versnellen met een belangrijke factor.

Daarom heeft UDLD een veronderstelde afhankelijkheid van het standaard overspuiten van boomtimers. Als u STP afstelt om sneller samen te komen dan UDLD, overweeg dan een afwisselend mechanisme, zoals de eigenschappen van CatOS 6.2 lijn Guard. Overweeg ook een afwisselend mechanisme wanneer u RSTP (IEEE 802.1w) implementeert omdat RSTP convergentiekenmerken in de milliseconden heeft, wat van de topologie afhangt. Voor deze gevallen, gebruik loop Guard in combinatie met UDLD, wat de meeste bescherming biedt. Loop Guard voorkomt STP-lijnen met de snelheid van de STP-versie die in gebruik is en UDLD detecteert unidirectionele verbindingen op individuele EtherChannel-koppelingen of in gevallen waarin BPDU’s niet in de gebroken richting lopen.

Opmerking: UDLD vangt niet elke STP-mislukkingssituatie, zoals fouten die worden veroorzaakt door een CPU die BPDU's niet voor een grotere tijd dan verzenden (2 * FwdDelay + Max). Om deze reden, raadt Cisco aan om UDLD in combinatie met loop Guard (dat in CatOS 6.2 werd geïntroduceerd) in topologieën toe te passen die op STP vertrouwen.

Waarschuwing: Let op van eerdere releases van UDLD die een niet-configureerbare 60-seconde standaardberichtinterval gebruiken. Deze releases zijn vatbaar voor in-boom-lusvoorwaarden.

UDLD Aggressive Mode

Aggressieve UDLD werd gecreëerd om specifiek die (weinige) gevallen aan te pakken waarin een voortdurende 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 eindtijd uit, wordt geen van beide poorten geannuleerd.
- Eén kant van een link zit vast in een poort (beide verzenden [Tx] en Rx).
- De ene kant van de link blijft omhoog, de andere kant van de link is omlaag gegaan.
- Automatische onderhandeling, of een ander L1-mechanisme voor het opsporen van fouten, is uitgeschakeld.
- Een vermindering van het vertrouwen op L1 FEFI - mechanismen is wenselijk.
- Er is maximale bescherming nodig tegen fouten door unidirectionele koppelingen op point-to-point FE/GE-links. In het bijzonder, waar geen falen tussen twee buren toegestaan is, kunnen de agressieve sondes van de UDLD beschouwd worden als een "hartslag", waarvan de aanwezigheid de gezondheid van de link garandeert.

Het meest voorkomende geval voor een implementatie van een agressieve UDLD is om de aansluitingscontrole uit te voeren op een lid van een bundel wanneer autonome onderhandelingen of een ander L1-foutdetectiemechanisme uitgeschakeld of onbruikbaar is. Dit geldt vooral voor EtherChannel-verbindingen, omdat PAgP/LACP, ook al is dat mogelijk, geen zeer lage hallo-timers gebruiken in stabiele toestand. In dit geval heeft agressieve UDLD het extra voordeel van preventie van mogelijke overspannen-boomloops.

De omstandigheden die bijdragen aan het symmetrische verlies van UDLD sonde pakketten zijn moeilijker te karakteriseren. U moet begrijpen dat normale UDLD controleert op een unidirectionele voorwaarde, zelfs nadat een verbinding bidirectionele status bereikt. De bedoeling van UDLD is L2-problemen te detecteren die STP-loops veroorzaken, en die problemen zijn doorgaans in één richting gericht, omdat BPDU's in één richting lopen bij steady state. Daarom is het gebruik van normale UDLD in combinatie met autonegotiation en loop Guard (voor netwerken die op STP vertrouwen) vrijwel altijd voldoende. De agressieve UDLD-modus is echter nuttig in situaties waarin de congestie in beide richtingen gelijk wordt beïnvloed, hetgeen het verlies van UDLD-sondes in beide richtingen veroorzaakt. Dit verlies van UDLD-sondes kan bijvoorbeeld voorkomen als CPU-gebruik op elk einde van de verbinding verhoogd is. Andere voorbeelden van bidirectioneel verlies van connectiviteit omvatten de schuld van één van deze apparaten:

- Een Dense Wavelength Division Multiplexing (DWDM) transponder
- Een mediaconverters
- Een hub
- Een ander L1-apparaat**Opmerking:** de fout kan niet worden gedetecteerd door autonome onderhandelingen.

De agressieve UDLD-fout schakelt de poort in deze mislukkingssituaties uit. Overweeg de implicaties zorgvuldig wanneer u UDLD agressieve modus op links inschakelen die geen punt-to-point zijn. De verbindingen met mediaconverters, knooppunten, of gelijksoortige apparaten zijn geen punt-aan-punt. Intermediate apparaten kunnen het verzenden van UDLD pakketten verhinderen en een verbinding dwingen om onnodig te worden gesloten.

Nadat alle buren van een haven uitgeput zijn, herstart de agressieve modus van UDLD (als deze wordt geactiveerd) de linkup volgorde in een poging om opnieuw te synchroniseren met om het even welke potentieel uit-van-sync buren. Deze inspanning vindt plaats in de advertentiefase of in de detectiefase. Als na een snelle trein van berichten (acht mislukte herhalingen) de link nog steeds als "onbepaald" wordt gezien, wordt de poort dan in `foutloze` status gezet.

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

UDLD op Routed Links

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

- Point-to-Point tussen twee routerknooppuntenDeze link wordt ingesteld met een 30-bits subnetmasker.
- Een VLAN met meerdere poorten, maar dat alleen routekaarten ondersteuntEen voorbeeld is een gesplitste L2 kerntopologie.

Elk Interior Gateway Routing Protocol (IGRP) heeft unieke kenmerken met betrekking tot de manier waarop het buurrelaties en routeconvergentie hanteert. De eigenschappen, die deze sectie

bespreekt, zijn relevant wanneer u twee van de meer prevalente routingprotocollen die vandaag worden gebruikt, Open Shortest Path First (OSPF) Protocol en Enhanced IGRP (DHCP) contrasteert.

Merk eerst op dat een storing van L1 of L2 op elk punt-tot-punt routed netwerk resulteert in de bijna onmiddellijke uitschakeling van de L3 verbinding. Omdat de enige poort op de switch in dat VLAN overschakelt naar een niet-verbonden staat bij de L1/L2-storing, synchroniseert de automatische-state optie van MSFC de L2 en L3 poortstaten in ongeveer twee seconden. Deze synchronisatie plaatst de L3 VLAN-interface in een omhoog/omlaag status (met het lijnprotocol omlaag).

Standaard timer waarden aannemen. OSPF verstuurt hallo-berichten elke 10 seconden en heeft een dode interval van 40 seconden (4 * hallo). Deze timers zijn consistent voor OSPF point-to-point en broadcast netwerken. Omdat OSPF communicatie in twee richtingen vereist om een nabijheid te vormen, is de best-case overlooptijd 40 seconden. Deze failover is het geval zelfs als de L1/L2 mislukking niet puur is op een punt-to-point verbinding, wat een half operationeel scenario achterlaat waar het L3-protocol mee moet omgaan. Omdat de detectietijd van UDLD zeer vergelijkbaar is met de tijd van een OSPF-dode timer die verloopt (ongeveer 40 seconden), zijn de voordelen van configuratie van UDLD normale modus op een OSPF L3-point-to-point link beperkt.

In veel gevallen, converteert EHRM sneller dan OSPF. Houd er echter rekening mee dat communicatie in twee richtingen niet nodig is voor buren om routeinformatie uit te wisselen. In zeer specifieke half-operationele mislukkingsscenario's, is DHCP kwetsbaar voor het zwart houden van verkeer dat duurt tot een andere gebeurtenis de routes door die buur "actief" maakt. Met de normale UDLD-modus kunnen de omstandigheden worden verzacht die in deze sectie worden aangegeven. De normale modus van UDLD detecteert de unidirectionele fout van de link en de fout schakelt de poort uit.

Voor L3-routed connecties die een routingprotocol gebruiken, biedt UDLD-standaard nog steeds bescherming tegen problemen bij de initiële linkactivering. Zulke kwesties omvatten het misleiden of defecte hardware. Daarnaast biedt de agressieve modus van UDLD deze voordelen voor L3-verbindingen:

- Voorkomt onnodig zwart roken van verkeer**Opmerking:** In sommige gevallen zijn timers minimaal vereist.
- Plaatst een flappende link in de status `foutmelding`
- Bescherm tegen lijnen die uit L3 EtherChannel-configuraties voortvloeien

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. Koperen poorten worden meestal gebruikt voor host-toegang.

Opmerking: UDLD moet mondiaal en op interfaceniveau ingeschakeld zijn voordat buren bidirectionele status kunnen bereiken. In CatOS 5.4(3) en hoger is het standaardberichtinterval 15 seconden en kan het worden ingesteld tussen 7 en 90 seconden.

Terugwinning opnieuw uitschakelen is normaal gesproken uitgeschakeld. Nadat deze wereldwijd is geactiveerd, als een poort `failliet` gaat, wordt de poort 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. U kunt een poort handmatig voorkomen als u de foutmelding voor die poort instelt om `uit` te `schakelen`. Geef de **ingestelde** opdracht voor uitschakelen van poort uit. *mod/poort* blokkeer.

Opmerking: het gebruik van deze opdracht is afhankelijk van de softwareversie.

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.

Zie Ethernet, Fast Ethernet, Gigabit Ethernet en 10-Gigabit Ethernet-switching configureren voor meer informatie over het instellen van een tijdelijke uitvoer voor poorten die in de status van de `foutmelding` staan.

Aanbeveling

De normale modus UDLD is in de meeste gevallen voldoende als u deze correct en in combinatie met de juiste functies en protocollen gebruikt. Deze functies/protocollen omvatten:

- FEFI
- Automatische onderhandeling
- Loop Guard

Wanneer u UDLD implementeert, bedenk dan of een doorlopende test van bidirectionele connectiviteit (agressieve modus) noodzakelijk is. Meestal, als autonegotiation is geactiveerd, is de agressieve modus niet nodig omdat autonome onderhandeling de foutdetectie bij L1 compenseert.

Cisco raadt aan om UDLD-modus in te schakelen op alle point-to-point FE/GE-koppelingen tussen Cisco-switches waarin het UDLD-berichtinterval is ingesteld op de 15-seconden-standaard. Deze configuratie is gebaseerd op de standaard 802.1d voor het overspannen van boomtimers. Gebruik bovendien UDLD in combinatie met loop Guard in netwerken die voor redundantie en convergentie op STP vertrouwen. Deze aanbeveling is van toepassing op netwerken waarin er één of meer havens in de STP-blokkeringsstaat in de topologie zijn.

Geef deze opdrachten uit om UDLD in staat te stellen:

```
set udld enable
!--- After global enablement, all FE and GE fiber !--- ports have UDLD enabled by default. set udld enable port range
!--- This is for additional specific ports and copper media, if needed.
```

U moet poorten handmatig inschakelen die door de unidirectionele symptomen zijn uitgeschakeld. Geef de **ingestelde poort op**.

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

Andere opties

Voor maximale bescherming tegen symptomen die het gevolg zijn van unidirectionele koppelingen, moet u agressieve modus UDLD configureren:

```
set udld aggressive-mode enable port_range
```

Daarnaast kunt u de waarde van het UDLD-berichtinterval tussen 7 en 90 seconden aan elk eind instellen, indien ondersteund, voor een snellere convergentie:

```
set udld interval time
```

Overweeg gebruik van de foutmelding optie op elk apparaat dat in geval van een foutmelding van het netwerk kan worden geïsoleerd. Deze situatie is typisch waar voor de toegangslaag en wanneer u UDLD agressieve modus zonder out-of-band netwerkbeheerfuncties implementeert.

Als een poort in `error` state wordt geplaatst, blijft de poort standaard plat. U kunt deze opdracht uitgeven, die havens na een timeout interval opnieuw toelaat:

Opmerking: het timeout interval is standaard 300 seconden.

```
>set errdisable-timeout enable ?
bpdu-guard
!--- This is BPDU port-guard. channel-misconfig !--- This is a channel misconfiguration. duplex-
mismatch udld other !--- These are other reasons. all !--- Apply errdisable timeout to all
reasons.
```

Als het partnerapparaat niet UDLD-Geschikt is, zoals een eindhost of router, voer het protocol niet uit. Deze opdracht geven:

```
set udld disable port_range
```

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 eenvoudige test uitvoert en één streng van een vezel koppelt om de gewenste `foutmelding` te zien, moet u L1 autonegotiation hebben uitgeschakeld. Anders gaat de fysieke poort naar beneden, waarmee de UDLD-berichtcommunicatie wordt hersteld. Het verre uiteinde beweegt naar de onbepaalde status in UDLD normaal. Als u de agressieve modus van UDLD gebruikt, beweegt het externe uiteinde naar de `foutmelding` status.

Er is een aanvullende testmethode om PDU-verlies van de buur voor UDLD te simuleren. Gebruik MAC-Layer filters om het UDLD/CDP hardwareadres te blokkeren maar laat andere adressen toe om door te geven.

Om UDLD te controleren geeft u deze opdrachten uit:

```
>show udld

UDLD              : enabled
```

```
Message Interval  : 15 seconds
```

```
>show udld port 3/1

UDLD              : enabled
Message Interval  : 15 seconds
Port      Admin Status  Aggressive Mode  Link State
--------  ------------  ---------------  ----------------
3/1      enabled       disabled         bidirectional
```

U kunt ook de verborgen **show udld buurland** opdracht geven om de inhoud van het UDLD cache te controleren (zoals CDP dat doet). Een vergelijking van het UDLD-cache naar het CDP-cache om te controleren of er een protocol-specifieke anomalie is, is vaak nuttig. Wanneer ook CDP wordt beïnvloed, worden alle PDU's/BPDU's doorgaans beïnvloed. Controleer daarom ook STP. Controleer bijvoorbeeld op recente wijzigingen in de wortelidentiteit of wortel/aangewezen poortplaatsing.

```
>show udld neighbor 3/1

Port  Device Name            Device ID    Port-ID OperState
----- -------------------- ------------ ------- ----------
3/1   TSC07117119M(Switch)   000c86a50433 3/1     bidirectional
```

Bovendien kunt u de status en de configuratie consistentie van UDLD met gebruik van de Cisco UDLD SNMP MIB-variabelen controleren.

Jumboframe

De standaard maximale grootte van Transmission Unit (MTU) is 1518 bytes voor alle Ethernet poorten, die GE en 10 GE omvatten. De eigenschap van het kader jumbo maakt interfaces in staat om frames te switches die groter zijn dan de standaard Ethernet frame grootte. Deze functie is handig om de prestaties van server-to-server te optimaliseren en toepassingen te ondersteunen zoals Multi-Protocol Label Switching (MPLS), 802.1Q tunneling en L2 Tunneling Protocol, versie 3 (L2TPv3), die de grootte van de oorspronkelijke frames vergroot.

Overzicht

De standaardspecificatie IEEE 802.3 definieert een maximale Ethernet-frame-grootte van 1518 bytes voor normale frames en 1522 bytes voor 802.1Q ingesloten frames. De 802.1Q ingekapselde frames worden soms "baby giants" genoemd. In het algemeen, worden pakketten geclassificeerd als gigantische frames wanneer de pakketten de gespecificeerde maximum lengte Ethernet voor een specifieke Ethernet verbinding overschrijden. Reuzenpakketten worden ook wel jumboframes genoemd.

Er zijn verschillende redenen waarom de grootte van een MTU van bepaalde frames de 1518 bytes kan overschrijden. Dit zijn een paar voorbeelden:

- selfspecifieke vereisten-toepassingen en bepaalde NIC's kunnen een grootte van MTU specificeren die buiten de standaard 1500 bytes valt. De neiging om dergelijke MTU-groottes te specificeren is het gevolg van studies die zijn uitgevoerd, die bewijzen dat een vergroting van de omvang van een Ethernet-frame de gemiddelde doorvoersnelheid kan verhogen.
- Trunking-Om de informatie van VLAN ID tussen switches of andere netwerkapparaten te dragen, is trunking gebruikt om het standaard Ethernet kader te vergroten. Vandaag de dag

zijn de twee meest gebruikelijke vormen van trunking de eigen ISL-insluiting van Cisco en IEEE 802.1Q.
- MPLS - Nadat MPLS op een interface is ingeschakeld, kan het de grootte van een pakketje vergroten. Deze vergroting is afhankelijk 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* x 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 tag per keer aan de hardware zichtbaar is. Daarom voegt de interne tag 4 bytes toe aan de MTU-waarde (payload size).
- Universele transport Interface (UTI)/L2TPv3-UTI/L2TPv3 kapselt L2-gegevens in die via het IP-netwerk moeten worden doorgestuurd. De insluiting kan de oorspronkelijke grootte van het frame met maximaal 50 bytes vergroten. Het nieuwe frame bevat een nieuwe IP-header (20-bytes), een L2TPv3-header (12-bytes) en een nieuwe L2-header. De L2TPv3 lading bestaat uit het volledige L2 frame, dat de L2 header bevat.

Het vermogen van de verschillende Catalyst switches om verschillende frame groottes te ondersteunen hangt af van vele factoren, waaronder de hardware en software. Bepaalde modules kunnen een grotere beeldgrootte ondersteunen dan andere, zelfs binnen hetzelfde platform.

- De Catalyst 5500/5000 switches bieden ondersteuning voor een jumboframe in de CatOS 6.1 release. Wanneer de optie voor jumboframes is ingeschakeld op een poort, wordt de grootte van de MTU verhoogd naar 9216 bytes. Op 10/100-Mbps niet-afgeschermde getwiste paarkaarten (UTP) gebaseerd, is de maximale grootte van een kader die wordt ondersteund slechts 8092 bytes. Deze beperking is een ASIC-beperking. Over het algemeen zijn er geen beperkingen in de mogelijkheid van de functie voor de grootte van een jumbo - frame. U kunt deze optie gebruiken met trunking/non-trunking en kantelen/nonchanneling.
- De Catalyst 4000 switches (Supervisor Engine 1 [WS-X4012] en Supervisor Engine 2 [WS-X4013]) ondersteunen jumboframes niet vanwege een ASIC-beperking. De uitzondering is echter 802.1Q trunking.
- Het Catalyst 6500 Series platform kan de grootte van een jumbo-frame ondersteunen in CatOS release 6.1(1) en hoger. Deze ondersteuning is echter afhankelijk van het type lijnkaarten dat u gebruikt. Over het algemeen zijn er geen beperkingen in de mogelijkheid van de functie voor de grootte van een jumbo - frame. U kunt deze optie gebruiken met trunking/non-trunking en kantelen/nonchanneling. De standaard MTU grootte is 9216 bytes nadat de ondersteuning van het frame-jumbo op de afzonderlijke poort is ingeschakeld. De standaard MTU kan niet worden ingesteld met CatOS. Cisco IOS-softwarerelease 12.1(13)E heeft echter de opdracht **systeemjumbomtu** geïntroduceerd om de standaard MTU te omzeilen.

Raadpleeg de Ondersteuning van Jumbo/Giant frame voor Catalyst Switches Configuration voor meer informatie.

In deze tabel worden de maten van MTU's beschreven die door verschillende lijnkaarten worden ondersteund voor Catalyst 6500/6000 Series switches:

Opmerking: De grootte van de MTU of de pakketgrootte heeft alleen betrekking op Ethernet-lading.

Lijnkaart	MTU-grootte

Standaard	9216 bytes
WS-X6248-RJ-45, WS-X6248A-RJ-45 WS-X6248-TEL, WS-X6248A-TEL WS-X6348-RJ-45(V), WS-X634 8-RJ-21(V)	8092 bytes (beperkt door de PHY-chip)
WS-X6148-RJ-45(V), WS-X6148-RJ-21(V) WS-X6148-45AF, WS-X6148-21AF	9100 bytes (@ 100 Mbps) 9216 bytes (@ 10 Mbps)
WS-X6148A-RJ-45, WS-X6148A-45AF, WS-X6148-FE-SFP switch	9216 bytes
WS-X6324-100FX-M, -SM, WS-X6024-10FL-MT	9216 bytes
WS-X6548-RJ-45, WS-X6548-RJ-21, WS-X6524-100FX-M WS-X6148X2-RJ-45, WS-X6148X2-45WS X6196-RJ-21, WS-X6196-21AF WS-X6408-GBIC, WS-X6316-GE-TX, WS-X6416-GBIC WS-X6516-GBIC, WS-X6 516A-GBIC, WS-X6816-GBIC uplinks van Supervisor Engine 1, 2, 32 en 720	9216 bytes
WS-X6516 GE-TX switch	8092 bytes (@ 100 Mbps) 9216 bytes (@ 10 of 1000 Mbps)
WS-X6148-GE-TX, WS-X6148V-GE-TX, WS-X6148-GE-45AF, WS-X6548-GE-TX, WS-X6548V-GE-TX, WS-X6548 1 GE-45AF	1500 bytes (jumboframe niet ondersteund)
WS-X6148A-GE-TX, WS-X6148A-GE-45AF, WS-X6502-10GE, WS-X67xx Series	9216 bytes
ATM optische servicesmodule (OC12c)	9180 bytes
CHOC3, CHOC12, CHOC48, CT3	9216 bytes (OCx en DS3) 7673

	bytes (T1/E1)
Flex WAN	7673 bytes (CT3 T1/DS0) 9216 bytes (OC3c POS) 7673 bytes (T1)
CSM (WS-X606-SLB-APC)	9216 bytes (vanaf CSM 3.1(5) en 3.2(1))
OSM POS OC3c, OC12c, OC48c; OSM DPT OC48c, optische servicesmodule met GE WAN	9216 bytes

Ondersteuning van Layer 3 Jumbo-frame

Met CatOS dat op de Supervisor Engine en Cisco IOS-software die op de MSFC loopt, bieden de Catalyst 6500/6000 switches ook L3 jumbo-frame ondersteuning in Cisco IOS® Software release 12.1(2)E en later met het gebruik van PFC/MSFC2, PFC2/MSFC2 of later hardware. Als zowel ingress als Groot VLANs voor jumboframes zijn geconfigureerd, zijn alle pakketten hardware die door de PFC is geschakeld via draadsnelheid. Als het ingress VLAN is geconfigureerd voor jumboframes en het ress VLAN niet is geconfigureerd, zijn er twee scenario's:

- Een jumboframe dat door de eindhost wordt verzonden terwijl het DF-bit (Don't Fragment) niet is ingesteld (voor path MTU discovery) - het pakket wordt verwijderd en een onbereikbaar Internet Control Message Protocol (ICMP) wordt naar de eindhost verzonden met het `benodigde` berichtcodefragment `en DF-set`.
- Een jumboframe dat tegen de eindhost wordt verzonden met het DF-bit dat niet is ingesteld—Packets worden gepunteerd op MSFC2/MSFC3 om te worden gefragmenteerd en in software geschakeld.

Deze tabel vat de L3 jumbo-ondersteuning voor verschillende platforms samen:

L3-Switch of -module	Maximaal L3 MTU-grootte
Catalyst 2948G-L3/4908G-L3 Series switches	Jumboframes worden niet ondersteund.
Catalyst 5000 RSM[1]/RSFC[2]	Jumboframes worden niet ondersteund.
Catalyst 6500 MSFC1-module	Jumboframes worden niet ondersteund.
Catalyst 6500 MSFC2 en	Cisco IOS-softwarerelease

hoger	12.1(2)E: 9216 bytes

[1] RSM = Route Switch-module

[2] RSFC = routefunctiekaart

Naleving van netwerkprestaties

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

- Het maximale segment Segment Size (MSS), dat is de MTU-lengte minus de lengte van de TCP/IP-headers
- De Ronde Trip Tijd (RTT)
- Het pakketverlies

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

Volgens deze formule is de maximale TCP-doorvoersnelheid die bereikt kan worden, rechtstreeks evenredig met de MSS. Met constante RTT- en pakketverlies kunt u de TCP-doorvoersnelheid 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.

Ten tweede, de steeds grotere prestatiebehoeften van serverboerderijen vereisen een efficiëntere manier om hogere gegevenssnelheden te garanderen met UDP-datagrammen (Network File System, NFS). NFS is het meest gebruikte opslagmechanisme voor data om bestanden tussen UNIX-gebaseerde servers over te brengen en biedt 8400-byte datagrammen. Gezien de uitgebreide 9 KB MTU of Ethernet is één jumboframe groot genoeg om een 8 KB applicatie datagram (bijvoorbeeld NFS) plus de pakketheader-overhead te dragen. Deze mogelijkheid maakt overdracht van efficiënter direct memory access (DMA) op de hosts mogelijk omdat software niet meer nodig heeft om NFS-blokken te kunnen splitsen in afzonderlijke UDP-datagrammen.

Aanbeveling

Wanneer u ondersteuning voor jumboframes wilt hebben, beperkt u het gebruik van jumboframes naar gebieden van het netwerk waar alle switch modules (L2) en interfaces (L3) jumboframes ondersteunen. Deze configuratie voorkomt fragmentatie waar dan ook op het pad. De configuratie van jumboframes die groter zijn dan de ondersteunde frame-lengte in het pad heft elke winst op die wordt behaald door het gebruik van de functie omdat fragmentatie vereist is. Zoals de tabellen in deze sectie van Jumbo Frame tonen kunnen verschillende platforms en lijnkaarten met betrekking tot de maximum pakketgrootte variëren die worden ondersteund.

Configureer de jumbo frame-bewuste host-apparaten met een grootte van een MTU die de minimale gemene deler is die door netwerkhardware wordt ondersteund, voor het gehele L2 VLAN waar het host-apparaat zich bevindt. Geef deze opdracht uit om de ondersteuning van jumbo-frames voor modules met ondersteuning van jumbo-frames in te schakelen:

```
set port jumbo mod/port enable
```

Als u bovendien de ondersteuning van jumboframes over L3-grenzen wilt instellen, moet u de grootste beschikbare MTU-waarde van 9216 bytes op alle toepasbare VLAN-interfaces configureren. Geef de **mtu** opdracht onder de VLAN-interfaces uit:

```
interface vlan vlan# mtu 9216
```

Deze configuratie zorgt ervoor dat de L2 jumbo frame MTU die door de modules wordt ondersteund, altijd kleiner is dan of gelijk aan de waarde die is geconfigureerd voor de L3 interfaces die het verkeer oversteekt. Dit voorkomt fragmentatie wanneer het verkeer van het VLAN over de L3 interface wordt geleid.

Configuratie van beheer

De overwegingen om te helpen een netwerk van de Catalyst te controleren, voorzien, en problemen oplossen worden in deze sectie besproken.

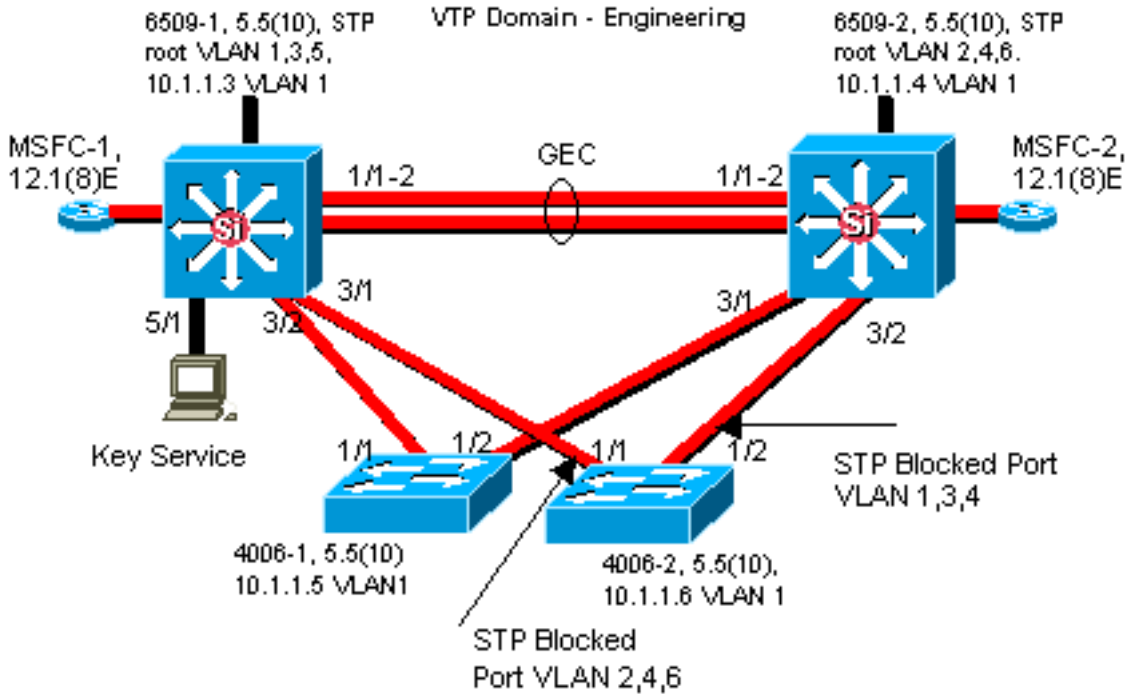
Netwerkdiagrammen

Duidelijke netwerkdiagrammen zijn een fundamenteel deel van netwerkoperaties. Ze zijn cruciaal tijdens de probleemoplossing en het belangrijkste medium voor de communicatie van informatie wanneer ze tijdens een stroomstoring naar verkopers en partners worden verschoven. Hun voorbereiding, gereedheid en toegankelijkheid moeten niet worden onderschat.

Aanbeveling

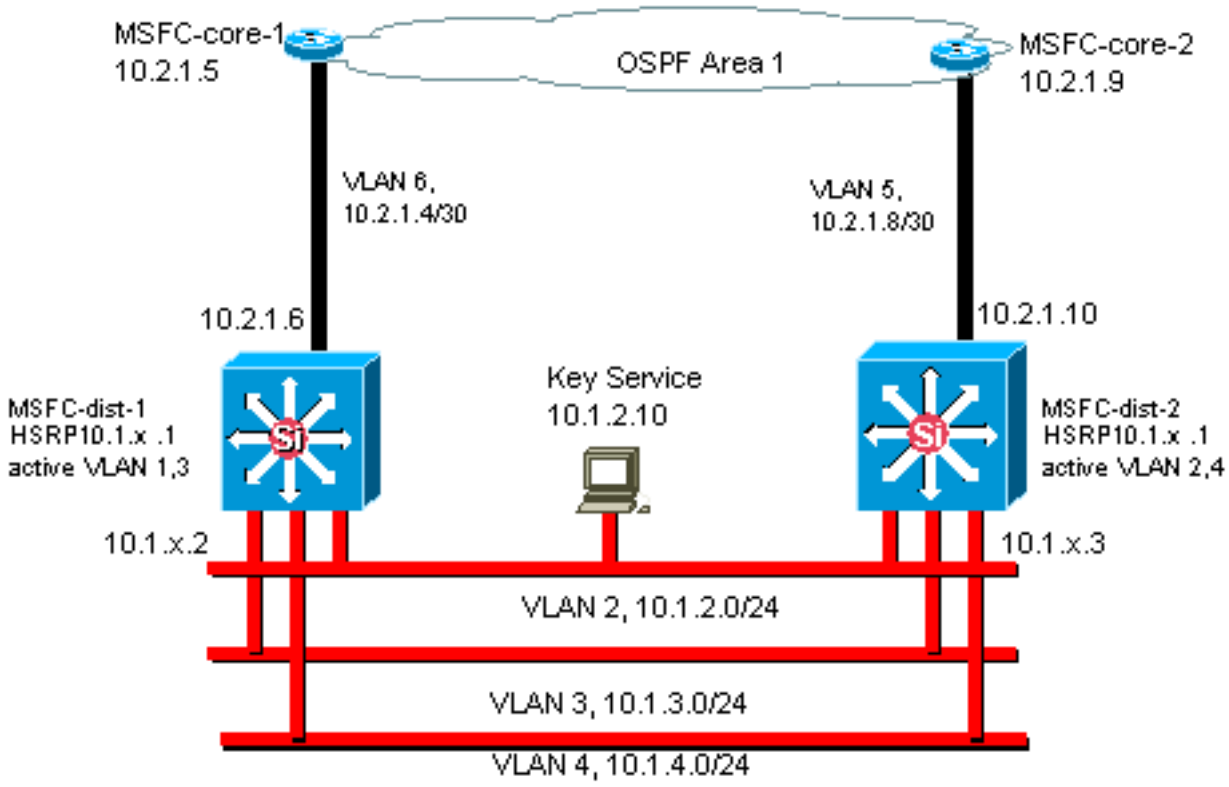
Cisco raadt u aan deze drie diagrammen te maken:

- **Algemeen Diagram**-zelfs voor de grootste netwerken, is een diagram dat de eind-aan-eind fysieke en logische connectiviteit toont belangrijk. Het kan gebruikelijk zijn voor ondernemingen die een hiërarchisch ontwerp hebben ingevoerd om elke laag afzonderlijk te documenteren. Tijdens het plannen en oplossen van problemen is het echter vaak een goede kennis van de manier waarop domeinen met elkaar verbinden die ertoe doet.
- **Fysiek Diagram**-toont alle switch en router hardware en bekabeling. Trunks, links, snelheden, kanaalgroepen, poortnummers, slots, chassis types, software, VTP domeinen, root-brug, prioriteit van de backup-root-brug, MAC-adres en geblokkeerde poorten per VLAN moeten worden geëtiketteerd. Het is vaak helderder om interne apparaten, zoals Catalyst 6500/6000 MSFC, als router op een stok af te beelden die door middel van een stam werd



aangesloten.

- **Logical Diagram**-shows only L3-functionaliteit (routers als objecten, VLAN's als Ethernet-segmenten). IP-adressen, subnetwerken, secundaire adressering, HSRP actieve en standby, access-core distributieslagen en routinginformatie moeten worden geëtiketteerd.



Inbraakbeheer

Afhankelijk van de configuratie zou de switch in-band (interne) beheerinterface (bekend als sc0) deze gegevens kunnen verwerken:

- Switch Management-protocollen zoals SNMP, telnet, Secure Shell Protocol (SSH) en SLUG
- Gebruikersgegevens zoals uitzendingen en multicast

- Switch controle protocollen zoals STP BPDU's, VTP, DTP, CDP, enzovoort

Het is algemeen gebruik in het ontwerp van de meerlaagse van Cisco om een beheer VLAN te vormen dat een geschakeld gebied overspant en alle sc0 interfaces bevat. Dit helpt om beheerverkeer te scheiden van gebruikersverkeer en verhoogt de beveiliging van de switch beheerinterfaces. In deze sectie worden de betekenis en mogelijke problemen beschreven bij het gebruik van de standaard VLAN 1 en het uitvoeren van beheerverkeer naar de switch in hetzelfde VLAN als gebruikersverkeer.

Overzicht

De primaire zorg over het gebruik van VLAN 1 voor gebruikersgegevens is dat het NMP van de Supervisor Engine in het algemeen niet hoeft te worden onderbroken door een groot deel van het multicast en uitgezonden verkeer dat door eindstations wordt gegenereerd. Oudere hardware van Catalyst 5500/5000, de Supervisor Engine I en Supervisor Engine II in het bijzonder, heeft beperkte middelen om met dit verkeer om te gaan, hoewel het beginsel op alle Supervisor Engine van toepassing is. Als de Supervisor Engine CPU, buffer of in-band kanaal naar de backplane volledig in gebruik is bij het luisteren naar onnodig verkeer, is het mogelijk dat de besturingsframes gemist kunnen worden. In het slechtst denkbare scenario zou dit kunnen leiden tot een Spanning Tree loop of EtherChannel-storing.

Als de opdrachten van de **show interface** en de **show ip stats** worden uitgegeven op de Catalyst, kunnen ze enige indicatie geven van het aandeel van uitzending aan het unicastverkeer en het gedeelte van IP aan niet IP verkeer (niet typisch gezien in beheer VLANs).

Een verdere controle van de gezondheid voor oudere hardware van Catalyst 5500/5000 moet de output van **show *inband*** onderzoeken / *biga* (verborgen opdracht) voor resource fouten (RSCRErOUters), vergelijkbaar met bufferdruppels in een router. Als deze resource fouten continu omhoog gaan, is het geheugen niet beschikbaar om systeempakketten te ontvangen, misschien vanwege een significante hoeveelheid uitzending verkeer in het beheer VLAN. Een enkele resource fout kan betekenen dat de Supervisor Engine geen pakket zoals BPDU's kan verwerken. Dit kan snel een probleem worden omdat protocollen zoals het overspannen van bomen gemiste BPDU's niet opnieuw verzenden.

Aanbeveling

Zoals gemarkeerd in het gedeelte Automation Control van dit document, is VLAN 1 een speciaal VLAN dat het grootste deel van het besturingsplane-verkeer markeert en verwerkt. VLAN 1 wordt standaard op alle stammen ingeschakeld. Met grotere campus netwerken moet aandacht worden besteed aan de diameter van het VLAN 1 **STP-domein**; instabiliteit in één deel van het netwerk zou VLAN 1 kunnen beïnvloeden, waarbij de stabiliteit van het controlevlak en daarom STP stabiliteit voor alle andere VLAN's zou kunnen beïnvloeden. In CatOS 5.4 en hoger is het mogelijk om VLAN 1 van het dragen van gebruikersgegevens en het uitvoeren van STP met deze opdracht te beperken:

```
clear trunk mod/port vlan 1
```

Dit houdt niet op dat er pakketten voor de controle van switch naar switch in VLAN 1 worden verzonden, zoals met een netwerkanalyzer wordt gezien. Er worden echter geen gegevens doorgestuurd en STP wordt niet via deze link uitgevoerd. Daarom kan deze techniek worden gebruikt om VLAN 1 tot kleinere mislukkingsdomeinen te splitsen.

Opmerking: Het is momenteel niet mogelijk om VLAN 1 trunks op 3500s en 2900XLs te wissen.

Zelfs als de zorg met het ontwerp van de campus is genomen om gebruiker VLANs aan relatief kleine switch domeinen en overeenkomstige kleine mislukking/L3 grenzen te beperken, zijn sommige klanten nog steeds in de verleiding gebracht om het beheer VLAN anders te behandelen en te proberen om het gehele netwerk met één enkel managementnet te bedekken. Er is geen technische reden waarom een centrale NMS-toepassing L2-naast de door haar beheerde apparatuur moet zijn, noch is dit een gekwalificeerd veiligheidsargument. Cisco raadt u aan de diameter van de beheerVLAN's te beperken tot dezelfde routestructuur als VLAN's van gebruikers en u kunt het out-of-band beheer en/of de ondersteuning CatOS 6.x SSH overwegen als manier om de beveiliging van het netwerkbeheer te verhogen.

Andere opties

Er zijn echter ontwerpoverwegingen voor deze Cisco-aanbevelingen in bepaalde topologieën. Bijvoorbeeld, is een gewenst en gemeenschappelijk ontwerp van Cisco meerlaagse die het gebruik van een actieve Spanning Tree voorkomt. Dit vereist dat u elk IP Subnet/VLAN aan één enkele switch van de toegangslaag, of cluster van switches beperkt. In deze ontwerpen kan er geen trunking worden ingesteld op de toegangslaag.

Er is geen gemakkelijk antwoord op de vraag of een afzonderlijk beheer VLAN gecreëerd en trunking toegelaten wordt om het tussen L2 toegang en L3 distributielagen te dragen. Dit zijn twee opties voor ontwerpbeoordeling met uw Cisco-engineer:

- **Optie 1:** stam twee of drie unieke VLAN's van de distributielaag tot elke switch van de toegangslaag. Dit staat voor een gegevens VLAN, een stem VLAN, en een beheer VLAN toe, bijvoorbeeld, en heeft nog het voordeel dat STP inactief is. (Merk op dat als VLAN 1 van de trunks wordt gewist, er een extra configuratiestap is.) In deze oplossing zijn er ook ontwerppunten die in overweging moeten worden genomen om het tijdelijk zwart-heiligen van routed Traffic Shaping te voorkomen tijdens het herstel van het defect: STP PortFast voor trunks (CatOS 7.x en hoger) of VLAN-automatische synchronisatie met STP-transport (later dan CatOS 5.5[9]).
- **Optie 2:** één VLAN voor gegevens en beheer kan aanvaardbaar zijn. Dankzij nieuwere hardware van de switch, zoals krachtigere CPU's en controle-vlakke snelheidsbeperkende controles, plus een ontwerp met relatief kleine uitzending domeinen zoals bepleit door het meerlaagse ontwerp, is de realiteit voor veel klanten dat het gescheiden houden van de sc0 interface van de gebruikersgegevens minder belangrijk is dan ooit geweest is. Een definitief besluit wordt waarschijnlijk het best genomen met het onderzoek van het uitzendverkeersprofiel voor dat VLAN en een discussie van de mogelijkheden van de hardware van de switch met uw Cisco-engineer. Als het beheerVLAN inderdaad alle gebruikers op die switch van de toegangslaag bevat, wordt het gebruik van IP-invoerfilters sterk aanbevolen om de switch van gebruikers te beveiligen, zoals besproken in het gedeelte Security Configuration van dit document.

out-of-band beheer

Met de argumenten van het vorige deel een stap verder, kan het netwerkbeheer beter beschikbaar worden gemaakt door de bouw van een afzonderlijke beheersinfrastructuur rond het productienet, zodat de voorzieningen altijd op afstand bereikbaar zijn, ongeacht welke verkeersgestuurde of bestuurlijk-vlakke gebeurtenissen zich voordoen. Deze twee benaderingen zijn typisch:

- End-of-band beheer met een exclusief LAN
- Out-of-Band Management met terminalservers

Overzicht

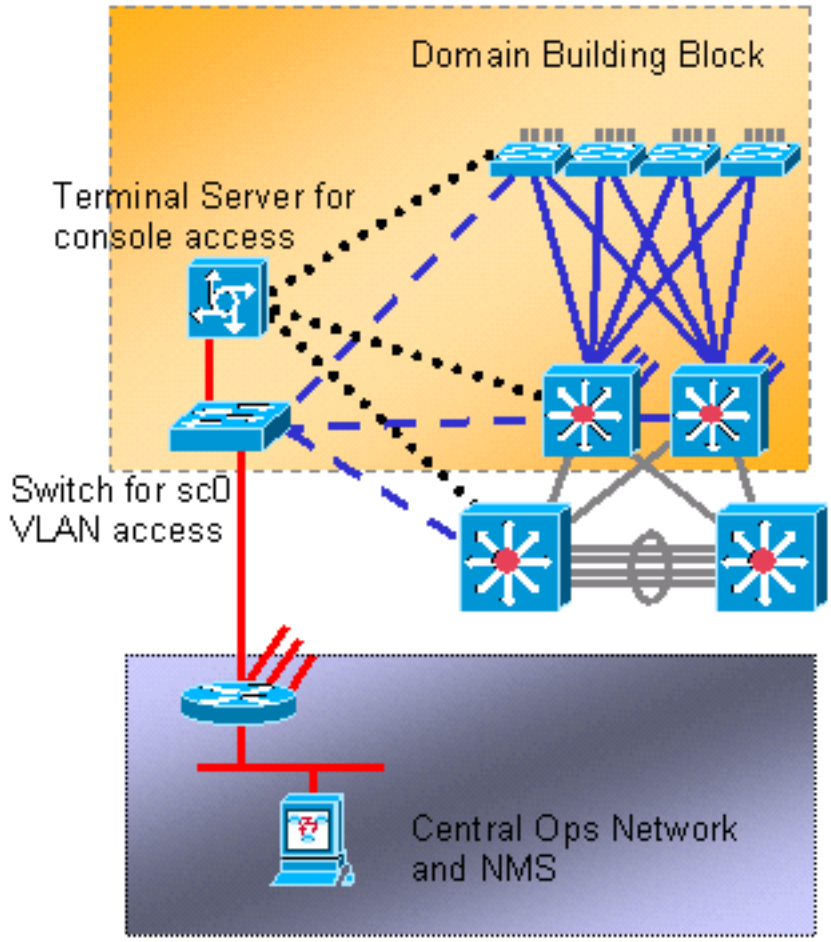
Elke router en switch in het netwerk kan met een out-of-band Ethernet beheersinterface op een beheer-VLAN worden voorzien. Eén Ethernet-poort op elk apparaat wordt ingesteld in het beheerVLAN en buiten het productienetwerk gecable naar een afzonderlijk geschakeld beheernetwerk via de sc0-interface. Merk op dat Catalyst 4500/4000 switches een speciale me1 interface op de Supervisor Engine hebben die alleen voor out-of-band beheer gebruikt moet worden, niet als switch poort.

Bovendien kan de connectiviteit van de eindserver door de configuratie van Cisco 2600 of 3600 met RJ-45-aan-seriekabels worden bereikt om tot de console poort van elke router en switch in de lay-out te toegang hebben. Een terminalserver vermijdt ook de noodzaak van het configureren van back-upscenario's, zoals modems op hulppoorten voor elk apparaat. Een enkele modem kan op de hulppoort van de eindserver worden ingesteld om inbelservice aan de andere apparaten te bieden tijdens een storing van de netwerkconnectiviteit.

Aanbeveling

Dankzij deze regeling zijn twee out-of-band paden voor elke switch en router mogelijk in aanvulling op talloze in-band paden, zodat u hoger beschikbaar netwerkbeheer kunt realiseren. Out-of-band is verantwoordelijk voor:

- Out-of-band scheidt beheerverkeer van gebruikersgegevens.
- Out-of-band heeft het beheer-IP-adres in een afzonderlijk netwerk, VLAN en switch voor hogere beveiliging.
- Out-of-band biedt een betere beveiliging voor het leveren van beheergegevens tijdens netwerkfouten.
- Out-of-band heeft geen actieve Spanning Tree in beheer VLAN. Redundantie is niet cruciaal.



Systeemtests

Opstarten diagnostiek

Tijdens het opstarten van een systeem worden een aantal processen uitgevoerd om ervoor te zorgen dat er een betrouwbaar en operationeel platform beschikbaar is, zodat defecte hardware het netwerk niet verstoort. Catalyst start diagnostiek is verdeeld tussen Power-On Self Test (POST) en online diagnostiek.

Overzicht

Afhankelijk van de platform- en hardwareconfiguratie worden verschillende diagnoses uitgevoerd bij het opstarten en wanneer een kaart wordt omgedraaid in het chassis. Een hoger niveau van diagnostiek leidt tot een breder aantal problemen die worden gedetecteerd, maar een langere herstartcyclus. Deze drie niveaus van POST-diagnostiek kunnen worden geselecteerd (alle testen controleren DRAM, RAM, en cache aanwezigheid en grootte en initialiseren ze):

Overzicht			
omzeilen	N.v.t.	3	Niet beschikbaar voor 4500/4000-series met CatOS 5.5 of eerder.
Minimaal	Patroonschrift test alleen op de eerste MB DRAM.	30	standaard voor de reeksen 5500/5000 en 6500/6000; niet beschikbaar voor 4500/4000-reeks.

Complet	Patroonschrijftests voor alle geheugen.	60	Standaard op 4500/4000-serie.

Online diagnostiek

Deze testen controleren pakketpaden intern in de switch. Het is belangrijk op te merken dat online diagnostiek daarom systeembreed testen zijn, en niet alleen haventesten. Op Catalyst 5500/5000 en 6500/6000 switches worden eerst tests uitgevoerd vanuit de standby Supervisor Engine en nog eens vanuit de primaire Supervisor Engine. De lengte van de diagnostiek hangt af van de systeemconfiguratie (aantal slots, modules, havens). Er zijn drie categorieën tests:

- Loopback test-pakketten van Supervisor Engine NMP worden naar elke poort verzonden, dan teruggestuurd naar NMP en onderzocht op fouten.
- Het bundelen van test—kanalen van maximaal acht poorten worden gecreëerd en loopback testen uitgevoerd naar de instantie om het hashing naar specifieke links te controleren (raadpleeg de sectie EtherChannel van dit document voor meer informatie).
- Enhanced Address Recognition Logic (EARL)-test — zowel de Central Supervisor Engine als de inline Ethernet module L3-herschrijfmotoren worden getest. Aanwijzingen voor het doorsturen van hardware en routepoorten worden gemaakt voordat steekproefpakketten worden verzonden (voor elk type protocol-insluiting) van het NMP via de overschakelhardware op elke module en terug naar het NMP. Dit is voor Catalyst 6500/6000 PFC-modules en nieuwer.

Complete online diagnostiek kan ongeveer twee minuten in beslag nemen. Minimale diagnostiek voert geen bundel- of herschrijftest uit op modules anders dan de Supervisor Engine, en kan ongeveer 90 seconden duren.

Tijdens een geheugentest, wanneer een verschil in het gelezen patroon wordt teruggevonden in vergelijking met het geschreven patroon, wordt de status van de poort veranderd in `fout`. De resultaten van deze tests kunnen worden gezien als de opdracht **test show** wordt gegeven, gevolgd door het te onderzoeken modulenummer:

```
>show test 9

Diagnostic mode: complete (mode at next reset: complete)
!--- Configuration setting. Module 9 : 4-port Multilayer Switch Line Card Status for Module 9 :
PASS Port Status : Ports 1 2 3 4 ----------------- . . . . Line Card Diag Status for Module 9 (.
= Pass, F = Fail, N = N/A) Loopback Status [Reported by Module 1] : Ports 1 2 3 4 ----------
--- . . F . !--- Faulty. Channel Status : Ports 1 2 3 4 ----------------- . . . .
```

Aanbeveling

Cisco raadt aan dat alle switches worden ingesteld voor het gebruik van volledige diagnostiek om maximale foutdetectie te bieden en storingen bij normaal gebruik te voorkomen.

Opmerking: Deze wijziging wordt pas van kracht wanneer het apparaat opnieuw wordt opgestart. Geef deze opdracht uit om de diagnose volledig te stellen:

```
set test diaglevel complete
```

Andere opties

In sommige situaties kan een snelle opstarttijd beter zijn dan wachten op een volledige diagnostiek. Er spelen nog andere factoren en timing bij de invoering van een systeem, maar over het geheel genomen nemen de diagnostiek en de online diagnostiek nog eens ongeveer een derde toe in de tijd. Bij het testen met een volledig bevolkt chassis met één Supervisor Engine met negen sleuven met Catalyst 6509 was de totale starttijd ongeveer 380 seconden met een volledige diagnostiek, ongeveer 300 seconden met een minimale diagnostiek en slechts 250 seconden met een gepasseerde diagnostiek. Geef deze opdracht uit om bypass te configureren:

```
set test diaglevel bypass
```

Opmerking: Catalyst 4500/4000 accepteert dat deze voor minimale diagnostiek wordt geconfigureerd, hoewel dit nog steeds resulteert in een volledige test die wordt uitgevoerd. De minimale modus kan in de toekomst op dit platform worden ondersteund.

Tijddiagnostiek uitvoeren

Zodra het systeem operationeel is, oefent de Supervisor Engine van de switch verschillende monitoring van de andere modules uit. Als een module niet bereikbaar is via de beheerberichten (Serial Control Protocol [SCP] dat over de out-of-band beheersbus loopt), probeert de Supervisor Engine de kaart opnieuw te starten of andere actie te ondernemen, al naar gelang van het geval.

Overzicht

De Supervisor Engine voert automatisch verschillende controles uit; hiervoor is geen configuratie nodig . Voor Catalyst 5500/5000 en Catalyst 6500/6000 worden deze onderdelen van de switch bewaakt:

- NMP via een waakhond
- Uitgebreide EARL-chips
- Inband kanaal van Supervisor Engine naar backplane
- Modules via keepalives over out-of-band kanaal (Catalyst 6500/6000)
- Active Supervisor Engine wordt gecontroleerd door de standby Supervisor Engine voor status (Catalyst 6500/6000)

Systeem- en hardwaredetectie

Overzicht

In CatOS 6.2 en later is verdere functionaliteit toegevoegd om kritische systemen en hardware-level-componenten te kunnen bewaken. Deze drie hardwareonderdelen worden ondersteund:

- Inband
- Poortteller
- Geheugen

Als deze functie is ingeschakeld en een foutmelding wordt gedetecteerd, genereert de switch een syslig-bericht. Het bericht stelt de beheerder ervan in kennis dat er een probleem bestaat voordat

er sprake is van een merkbare verslechtering van de prestaties. In CatOS-versies 6.4(16), 7.6(12), 8.4(2) en later wordt de standaardmodus voor alle drie onderdelen gewijzigd van uitgeschakeld naar ingeschakeld.

Inband

Als een inband fout wordt gedetecteerd, meldt een syslogbericht u dat een probleem bestaat voordat er een duidelijke verslechtering van de prestaties optreedt. De fout geeft het type inband error voorkomen weer. Een paar voorbeelden zijn:

- Inband zit vast
- resourcefouten
- Inband mislukt tijdens opstarten

Bij het detecteren van een inband ping-storing rapporteert de functie ook een extra syslg-bericht met een snapshot van de huidige Tx- en Rx-snelheid op de inband verbinding, CPU en de backplane kast van de switch. Met dit bericht kunt u naar behoren bepalen of de inband vast zit (geen Tx/Rx) of overbelast is (buitensporige Tx/Rx). Deze extra informatie kan u helpen de oorzaak van inband pingfouten te bepalen.

Poortteller

Wanneer u deze optie activeert, creëert en start het een proces om poorttellers te debug. De poortteller controleert periodiek de interne van de havenfout tellers. De architectuur van de lijnkaart, en meer in het bijzonder de ASIC's op de module, bepaalt welke de functievragen tellen. Cisco Technical Support or Development Engineering kan deze informatie dan gebruiken om problemen bij de oplossing te zoeken. Deze optie biedt geen fouttellers zoals FCS, CRC, uitlijning en runts die direct verbonden zijn met de connectiviteit van de verbindingspartner. Zie het gedeelte EtherChannel/Link-fouten voor het verwerken van dit document om deze functie te integreren.

De peiling wordt om de 30 minuten uitgevoerd en werkt op de achtergrond van geselecteerde fouttellers. Als het aantal oploopt tussen twee opvolgende opiniepeilingen in dezelfde poort, meldt een syslogbericht het incident en geeft de module/poort en foutmelding.

De optie van de poortteller wordt niet ondersteund op Catalyst 4500/4000 platform.

Geheugen

Het inschakelen van deze functie voert achtergrondcontrole uit en detecteert de corruptievoorwaarden van de DRAM. Dergelijke geheugencorruptievoorwaarden omvatten:

- Toewijzing
- Freeing
- Buiten bereik
- Slechte uitlijning

Aanbeveling

Schakel alle functies voor foutdetectie in, waaronder inband, poorttellers en geheugen, waar deze worden ondersteund. Met deze functies kan een beter proactief systeem- en

hardwarewaarschuwingsdiagnostiek voor de Catalyst switch worden bereikt. Geef deze opdrachten uit om alle drie de functies voor foutdetectie mogelijk te maken:

```
set errordetection inband enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection
portcounters enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later. set errordetection memory
enable
!--- This is the default in CatOS 6.4(16), 7.6(12), 8.4(2), and later.
```

Geef deze opdracht uit om te bevestigen dat foutdetectie is ingeschakeld:

```
>show errordetection

Inband error detection:                  enabled
Memory error detection:                  enabled
Packet buffer error detection:           errdisable
Port counter error detection:            enabled
Port link-errors detection:              disabled
Port link-errors action:                 port-failover
Port link-errors interval:               30 seconds
```

EtherChannel/Link-fouten - verwerking

Overzicht

In CatOS 8.4 en later is een nieuwe optie geïntroduceerd om een automatische failover van verkeer van één poort in een EtherChannel naar een andere poort in hetzelfde EtherChannel te bieden. De port failover komt voor wanneer één van de poorten in het kanaal een configureerbare foutdrempel binnen het gespecificeerde interval overschrijdt. De port failover komt alleen voor als er een operationele poort links in EtherChannel is. Als de mislukte poort de laatste poort in EtherChannel is, gaat de poort niet de `port-over-`status in. Deze poort blijft verkeer doorgeven, ongeacht het type fouten dat wordt ontvangen. Enkelvoudige, niet-kanaliseerde poorten gaan niet naar de `port-over-`status. Deze poorten gaan naar de status `foutmelding` als de foutdrempel binnen het opgegeven interval wordt overschreden.

Deze optie is alleen effectief als u **selectietekenmerken** kunt **instellen**. De te controleren link fouten zijn gebaseerd op drie tellers:

- fouten
- RXCRC's (CRCA-fouten)
- TxCRC's

Geef de opdracht **tellers van de show uit** op een switch om het aantal fouttellers te tonen. Dit is een voorbeeld:

```
>show counters 4/48

.......

32 bit counters

0  rxCRCAlignErrors           =          0
.......
```

```
6  ifInErrors                =          0
.......

12 txCRC                     =          0
```

Deze tabel is een lijst van mogelijke configuratieparameters en de respectieve standaardconfiguratie:

parameters	Standaard
Wereldwijd	Uitgeschakeld
Poortmonitor voor RXCRC	Uitgeschakeld
Poortmonitor voor inbelfouten	Uitgeschakeld
Poortmonitor voor TXCRC	Uitgeschakeld
Handeling	Poortfailover
Interval	30 seconden
Steekproef	3 achtereenvolgende
Lage drempel	1000
Hoge drempel	1001

Als de optie is ingeschakeld en de fouttelling van een poort de hoge waarde van de aanpasbare drempelwaarde bereikt binnen de opgegeven periode van de steekproeftelling, dan is de aanpasbare actie foutloos of poortfailover. De fout schakelt actie in om de poort in de `foutmelding` te plaatsen. Als u de port failover-actie instelt, wordt de status van het poortkanaal overwogen. De haven is slechts foutloos als de haven in een kanaal is maar die haven is niet de laatste operationele haven in het kanaal. Als de geconfigureerde actie bovendien een port-failover is en de poort één poort is of niet-gekanaliseerde, wordt de poort in de `foutmelding` geplaatst wanneer de port error teller de hoge waarde van de drempelwaarde bereikt.

Het interval is een timer constante voor het lezen van de port error tellers. De standaardwaarde van het link-fouten interval is 30 seconden. Het toegestane bereik ligt tussen 30 en 1800 seconden.

Er bestaat een risico op onvoorziene onjuistheden van een haven door een onverwachte eenmalige gebeurtenis. Om dit risico zo klein mogelijk te maken, worden alleen maatregelen naar een haven genomen wanneer de toestand zich blijft voordoen door middel van dit opeenvolgende bemonsteringsaantal keren. De standaardsteekproefwaarde is 3 en het toegestane bereik loopt van 1 tot 255.

De drempel is een absoluut aantal dat moet worden gecontroleerd op basis van het link-foutinterval. De standaard link-fout lage drempel is 1000 en het toegestane bereik is 1 tot 65.535. De standaard link-fout hoge drempel is 1001. Wanneer het opeenvolgende aantal bemonsteringstijden de lage drempel bereikt, wordt een syslog verstuurd. Als de achtereenvolgende bemonsteringstijden de hoge drempel bereiken, wordt een syslog verzonden en wordt een foutmelding of een port failover actie geactiveerd.

Opmerking: Gebruik dezelfde configuratie voor de detectie van poortfouten voor alle poorten in een kanaal. Raadpleeg deze secties van de Catalyst 6500 Series softwareconfiguratie handleiding voor meer informatie:

- De *configuratie van EtherChannel/Link-fout bij* de verwerking van de controlestatus en de connectiviteit
- Het *configureren van poortfoutdetectie* van Ethernet-, Fast Ethernet-, Gigabit Ethernet- en 10 Gigabit Ethernet-switching

Aanbevelingen

Omdat de functie SCP-berichten gebruikt om de gegevens te registreren en te vergelijken, kunnen grote aantallen actieve poorten CPU-intensief zijn. Dit scenario is zelfs nog meer CPU-intensief wanneer het drempelinterval is ingesteld op een zeer kleine waarde. Schakel deze optie in met vrijheid voor poorten die als belangrijke koppelingen zijn aangewezen en verkeers naar gevoelige toepassingen. Geef deze opdracht uit om wereldwijd de detectie van link-fouten mogelijk te maken:

```
set errordetection link-errors enable
```

Begin ook met de standaard drempel-, interval- en bemonsteringsparameters. En gebruik de standaard actie, port failover.

Geef deze opdrachten uit om de globale link-foutparameters op afzonderlijke poorten toe te passen:

```
set port errordetection mod/port inerrors enable

set port errordetection mod/port rxcrc enable

set port errordetection mod/port txcrc enable
```

U kunt deze opdrachten uitgeven om de configuratie van de link-fouten te controleren:

```
show errordetection

show port errordetection {mod | mod/port}
```

Catalyst 6500/6000 Packet Buffer-diagnostiek

In CatOS-versies 6.4(7), 7.6(5) en 8.2(1) is de diagnostiek van Catalyst 6500/6000 pakketbuffers geïntroduceerd. De pakketbufferdiagnostiek, die standaard ingeschakeld is, detecteert pakketbufferfouten die veroorzaakt worden door tijdelijke Static RAM (SRAM) defecten. Detectie is beschikbaar voor deze 48-poorts 10/100 Mbps lijnmodules:

- WS-X6248-RJ45
- WS-X6248-RJ21
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6148-RJ45

- WS-X6148-RJ21

Wanneer de mislukkingsconditie zich voordoet, blijven 12 van de 48 10/100 Mbps poorten aangesloten en kunnen willekeurige connectiviteitsproblemen ervaren. De enige manier om te herstellen van deze conditie is het aandrijven van de lijnmodule.

Overzicht

De diagnostiek van de pakketbuffer controleert de gegevens die in een specifiek gedeelte van de pakketbuffer zijn opgeslagen om te bepalen of deze door tijdelijke SRAM defecten beschadigd is. Als het proces iets anders leest dan wat het schreef, voert het dan twee mogelijke aanpasbare herstelopties uit:

1. De standaardinstelling is om de lijnkaartpoorten uit te schakelen die worden beïnvloed door de bufferstoring.
2. De tweede optie is om de lijnkaart van stroom te voorzien.

Er zijn twee syslog-berichten toegevoegd. De berichten geven een waarschuwing voor de foutmelding van de poorten of het stroomprogramma van de module vanwege fouten in de pakketbuffer:

```
%SYS-3-PKTBUFFERFAIL_ERRDIS:Packet buffer failure detected.
Err-disabling port 5/1.
%SYS-3-PKTBUFFERFAIL_PWRCYCLE: Packet buffer failure detected.
Power cycling module 5.
```

In CatOS-versies die eerder dan 8.3 en 8.4 zijn geweest, bedraagt de tijd voor het stroomprogramma van de lijnkaart tussen 30 en 40 seconden. Er is een voorziening voor snelle start-up geïntroduceerd in CatOS-versies 8.3 en 8.4. De functie downloads automatisch de firmware naar de geïnstalleerde lijnkaarten tijdens de eerste start-procedure om de opstarttijd te minimaliseren. De functie Rapid Boot (Rapid Boot) verkort de tijd voor het stroomprogramma tot ongeveer 10 seconden.

Aanbeveling

Cisco raadt de standaardoptie van *foutmelding aan*. Deze actie heeft het minste effect op de netwerkservice tijdens de productieuren. Verplaats indien mogelijk de verbinding die wordt beïnvloed door de foutgehandicapte poorten naar andere beschikbare switches om de service te herstellen. Stel tijdens het onderhoudsvenster een handmatige stroomcyclus van de lijnkaart in. Geef de opdracht **resetten van de module** uit om volledig te herstellen van de gecorrumpeerde toestand van de pakketbuffer.

Opmerking: Als de fouten doorgaan nadat de module is hersteld, probeer dan de module opnieuw te plaatsen.

Geef deze opdracht uit om de *foutoptie* in te schakelen:

```
set errordetection packet-buffer errdisable
!--- This is the default.
```

Andere opties

Omdat een stroomcyclus van de lijnkaart nodig is om alle poorten die een SRAM-storing hebben ondervonden volledig te kunnen herstellen, moet een andere herstelactie worden ondernomen om de energieprogrammaoptie te configureren. Deze optie is nuttig in omstandigheden waarin een stroomstoring in netwerkdiensten die tussen 30 en 40 seconden kan duren, aanvaardbaar is. Deze tijdsduur is de tijd die nodig is voor een lijnmodule om het programma volledig te aandrijven en zichzelf weer in bedrijf te stellen zonder de functie Rapid Boot. Met de optie Rapid Boot <Rapid Boot> kan de tijd van de stroomuitval in de netwerkservices met de optie stroomcyclus tot 10 seconden worden verkort. Geef deze opdracht uit om de optie voor het stroomprogramma mogelijk te maken:

```
set errordetection packet-buffer power-cycle
```

Packet Buffer-diagnostiek

Deze test is alleen voor Catalyst 5500/5000 switches. Deze test is ontworpen om mislukte hardware te vinden op Catalyst 5500/5000 switches die Ethernet modules met specifieke hardware gebruiken die 10/100 Mbps connectiviteit tussen gebruikerspoorten en de backplane van de switch voorzien. Aangezien zij geen CRC-controle op getrunkeerde frames kunnen uitvoeren, als een havenpakketbuffer tijdens run defect raakt, kunnen pakketten gecorrumpeerd raken en CRC-fouten veroorzaken. Helaas zou dit kunnen leiden tot de verspreiding van slechte beelden verder in het ISL-netwerk Catalyst 5500/5000, wat mogelijk leidt tot het verstoren van het vliegtuig en het uitzenden van stormen in ergste scenario's.

nieuwere Catalyst 5500/5000 modules en andere platforms hebben ingebouwde hardware error check bijgewerkt en hebben de pakketbuffertests niet nodig, dus er is geen optie om deze te configureren.

De lijnmodules die de diagnose pakketbuffer nodig hebben zijn WS-X5010, WS-X5011, WS-X5013, WS-X5020, WS-X5111, WS-X5113, WS-X5114, WS-X 5201, WS-X5203, WS-X5213/a, WS-X5223, WS-X5224, WS-X5506, WS-X5509, WS-U531, WS-U55 533 en WS-U5535.

Overzicht

Dit diagnostische onderzoek controleert of gegevens die opgeslagen zijn in een specifiek gedeelte van de pakketbuffer niet per ongeluk gecorrumpeerd worden door defecte hardware. Als het proces iets anders leest dan het geschreven is, sluit het de poort in de `mislukte` modus af, omdat die haven gegevens kan beschadigen. Er is geen drempel voor fouten nodig. Stapte poorten kunnen niet opnieuw worden ingeschakeld totdat de module is gereset (of vervangen).

Er zijn twee modi voor pakketbuffertests: gepland en op aanvraag. Wanneer een test begint, worden syslog-berichten gegenereerd om de verwachte lengte van de test aan te geven (afgerond tot op de dichtstbijzijnde minuut) en het feit dat de test is gestart. De exacte lengte van de test varieert per type poort, grootte van de buffer en het type testrun.

Aanwezigheidsproeven zijn agressief om binnen enkele minuten te kunnen eindigen. Aangezien deze testen zich actief met pakketgeheugen bemoeien, moeten poorten administratief vóór het testen worden afgesloten. Geef deze opdracht uit om de poorten te sluiten:

```
> (enable) test packetbuffer 4/1
```

```
Warning: only disabled ports may be tested on demand - 4/1 will be skipped.
> (enable) set port disable 4/1
> (enable) test packetbuffer 4/1
Packet buffer test started. Estimated test time: 1 minute.
%SYS-5-PKTTESTSTART:Packet buffer test started
%SYS-5-PKTTESTDONE:Packet buffer test done. Use 'show test' to see test results
```

Geplande testen zijn veel minder agressief dan de on-demand testen, en ze voeren op de achtergrond uit. De tests worden parallel uitgevoerd over meerdere modules maar op één poort per module tegelijk. De test behoudt, schrijft en leest kleine delen van het geheugen van de pakketbuffer voordat u de gegevens van de gebruikerspakketbuffer herstelt, en genereert dus geen fouten. Aangezien de test echter is geschreven om geheugen op te stellen, blokkeert deze binnenkomende pakketten voor een paar milliseconden en veroorzaakt het verlies op drukke links. Standaard is er een acht-seconden durende pauze tussen elke buffer-schrijf test om pakketverlies te minimaliseren, maar dit betekent dat een systeem vol modules die de pakketbuffertest nodig hebben, meer dan 24 uur kan duren voordat de test voltooid is. Deze geplande test is standaard ingeschakeld om wekelijks op zondag vanaf CatOS 5.4 of later om 3.30 uur te starten, en de teststatus kan met deze opdracht worden bevestigd:

```
>show test packetbuffer status

!--- When test is running, the command returns !--- this information: Current packet buffer test
details Test Type : scheduled Test Started : 03:30:08 Jul 20 2001 Test Status : 26% of ports
tested Ports under test : 10/5,11/2 Estimated time left : 11 minutes !--- When test is not
running, !--- the command returns this information: Last packet buffer test details Test Type :
scheduled Test Started : 03:30:08 Jul 20 2001 Test Finished : 06:48:57 Jul 21 2001
```

Aanbeveling

Cisco raadt u aan de geplande pakketbuffertestfunctie voor Catalyst 5500/5000 systemen te gebruiken, aangezien het voordeel van het ontdekken van problemen op modules zwaarder weegt dan het risico van laag pakketverlies.

Vervolgens moet er een gestandaardiseerde wekelijkse tijd over het netwerk worden gepland, zodat de klant, indien nodig, koppelingen van defecte poorten of RMA-modules kan wijzigen. Aangezien deze test wat pakketverlies kan veroorzaken, afhankelijk van netwerklading, moet het voor rustiger netwerktijden gepland zijn, zoals de standaard 3:30 AM op een zondagochtend. Geef deze opdracht uit om de testtijd in te stellen:

```
set test packetbuffer Sunday 3:30
!--- This is the default.
```

Als CatOS eenmaal is ingeschakeld (net als wanneer CatOS wordt bijgewerkt naar 5.4 en later voor het eerst), is er een kans dat een eerder verborgen geheugen-/hardwareprobleem wordt blootgesteld, en wordt een poort automatisch afgesloten. Dit bericht is te zien:

```
%SYS-3-PKTBUFBAD:Port 1/1 failed packet buffer test
```

Andere opties

Als het niet acceptabel is om een laag niveau van pakketverlies per poort op wekelijkse basis te riskeren, wordt het aanbevolen om de optie op aanvraag tijdens geplande uitgangen te gebruiken. Geef deze opdracht uit om deze optie handmatig op basis van bereik te starten (hoewel de poort eerst administratief moet worden uitgeschakeld):

```
test packetbuffer port range
```

Vastlegging systeem

Syrische berichten zijn Cisco-specifiek en een essentieel onderdeel van proactief foutbeheer. Een breder bereik van netwerk- en protocolvoorwaarden wordt gemeld met behulp van syslog dan mogelijk is via standaard SNMP. Management-platforms, zoals Cisco Resource Manager Essentials (RME's) en de Network Analysis Toolkit (NATkit) maken sterk gebruik van opslaginformatie omdat zij deze taken uitvoeren:

- Presence analyse naar ernst, bericht, apparaat, enz.
- Filteren van berichten die binnenkomen voor analyse inschakelen
- Waarschuwing van triggers, zoals piepers, of het op aanvraag verzamelen van inventaris- en configuratieveranderingen

Aanbeveling

Een belangrijk aandachtspunt is welk niveau van houtkapinformatie lokaal moet worden gegenereerd en in de switch buffer moet worden bewaard in plaats van het niveau dat naar een syslig server wordt verzonden (met behulp van de opdracht *voor de ingestelde* ernst van de logserver). Sommige organisaties registreren een hoog niveau van informatie centraal, terwijl anderen naar de switch zelf gaan om de gedetailleerdere logbestanden voor een gebeurtenis te bekijken of om een hoger niveau van systeemopname alleen tijdens de probleemoplossing te realiseren.

Debugging is anders op CatOS-platforms dan Cisco IOS-software, maar de gedetailleerde systeemvastlegging kan per sessie worden ingeschakeld waarbij de ingestelde logatessie wordt geactiveerd zonder te veranderen wat standaard wordt vastgelegd.

Cisco raadt over het algemeen u aan om de spantree- en systeemselectiefaciliteiten tot niveau 6 te brengen, aangezien dit belangrijke stabiliteitseigenschappen zijn om te volgen. Bovendien wordt voor multicast omgevingen het logniveau van de mcast-faciliteit tot 4 aanbevolen, zodat er syslogberichten worden geproduceerd als routerpoorten worden verwijderd. Helaas kan dit vóór CatOS 5.5(5) ertoe leiden dat er syslog-berichten worden opgenomen voor IGMP-verbindingen en -bladeren, wat te veel lawaai is om te controleren. Tenslotte wordt, als IP-invoerlijsten worden gebruikt, een minimaal logniveau van 4 aanbevolen om niet-geautoriseerde inlogpogingen op te nemen. Geef deze opdrachten uit om deze opties in te stellen:

```
set logging buffer 500
!--- This is the default. set logging server syslog server IP address set logging server enable
!--- This is the default. set logging timestamp enable
set logging level spantree 6 default
!--- Increase default STP syslog level. set logging level sys 6 default
!--- Increase default system syslog level. set logging server severity 4
!--- This is the default; !--- it limits messages exported to syslog server. set logging console
disable
```

Schakel de console-berichten uit om te beschermen tegen het risico van het ophangen van de switch wanneer deze wacht op een reactie van een trage of niet bestaande terminal wanneer het

berichtvolume hoog is. De loggen van de console is een hoge prioriteit onder CatOS en wordt hoofdzakelijk gebruikt om de laatste berichten lokaal te vangen wanneer de oplossing of in een switch crashscenario komt.

Deze tabel geeft de individuele houtkapfaciliteiten, de standaardinstellingen en de aanbevolen veranderingen voor Catalyst 6500/6000 weer. Elk platform heeft een beetje verschillende faciliteiten, afhankelijk van de ondersteunde functies.

faciliteit	Standaardniveau	Aanbevolen actie
bel	5	Laat met rust.
cdp	4	Laat met rust.
agenten	3	Laat met rust.
dpp	8	Laat met rust.
oorl	2	Laat met rust.
ethc[1]	5	Laat met rust.
vijvers	2	Laat met rust.
gvrp	2	Laat met rust.
ip	2	Verandert in 4 als IP-invoerlijsten worden gebruikt.
kern	2	Laat met rust.
1 quinquies	3	Laat met rust.
werpen	2	Verandering naar 4 indien multicast gebruikt (CatOS 5.5[5] en later).
steun	5	Laat met rust.
moussere n	5	Laat met rust.
pagineren	5	Laat met rust.
protagina	2	Laat met rust.
snoeien	2	Laat met rust.
Privatevla n	3	Laat met rust.
qos	3	Laat met rust.
straal	2	Laat met rust.
rsvp	3	Laat met rust.
beveiliging	2	Laat met rust.
verklikken	2	Laat met rust.
spanboom	2	Verander naar 6.
sys	5	Verander naar 6.
tac	2	Laat met rust.
tcp	2	Laat met rust.
telnet	2	Laat met rust.

Tftp	2	Laat met rust.
UDLD	4	Laat met rust.
VMPS	2	Laat met rust.
VTP	2	Laat met rust.

[1] In CatOS 7.x en later vervangt de code van de ethische faciliteit de code van de pagofaciliteit om de LACP-ondersteuning weer te geven.

Opmerking: Op dit moment registreren de Catalyst switches een melding op het niveau-6 van de configuratiewijziging voor elke **ingestelde** of **duidelijke** opdracht die wordt uitgevoerd, in tegenstelling tot Cisco IOS-software, die het bericht alleen activeert nadat u de configuratie-modus hebt afgesloten. Als u RME's nodig hebt om in real-time configuraties in back-ups te maken op basis van deze trigger, dan moeten deze berichten ook naar de RMEs syslogserver worden verzonden. Voor de meeste klanten zijn periodieke configuratieback-ups voor Catalyst switches genoeg en er is geen verandering nodig in de ernst van de vastlegging van de standaard server.

Als u de NMS-waarschuwingen aanpast, raadpleegt u de systeemberichtgids.

Eenvoudig netwerkbeheerprotocol

SNMP wordt gebruikt om statistieken, tellers, en tabellen op te halen die in de Bases van de Informatie van het netwerkapparaat (MIBs) worden opgeslagen. De verzamelde informatie kan door NMS's (zoals HP OpenView) worden gebruikt om real-time waarschuwingen te genereren, de beschikbaarheid te meten en informatie over capaciteitsplanning te produceren, evenals om configuratie- en probleemoplossing-controles uit te voeren.

Overzicht

Met sommige veiligheidsmechanismen, kan een netwerkbeheerstation informatie in de MIBs met SNMP protocol krijgen en volgende verzoeken krijgen, en parameters veranderen met de **set** opdracht. Bovendien kan een netwerkapparaat worden geconfigureerd om een valbericht voor de NMS te genereren voor realtime-signalering. SNMP-polling gebruikt IP UDP-poort 161 en SNMP-traps gebruiken poort 162.

Cisco ondersteunt deze versies van SNMP:

- SNMPv1: RFC 1157 Internet Standard, met gebruik van duidelijke sms-beveiliging van de tekstgemeenschap. Een IP-toegangscontrolelijst en wachtwoord definiëren de community van managers die toegang hebben tot de agent MIB.
- SNMPv2C: een combinatie van SNMPv2, een ontwerp-internetstandaard gedefinieerd in RFC's van 1902 tot en met 1907, en SNMPv2C, een op de gemeenschap gebaseerd administratief kader voor SNMPv2 dat een experimenteel ontwerp is dat in RFC van 1901 is gedefinieerd. Voordelen omvatten een bulkherkenningsmechanisme dat het ophalen van tabellen en grote hoeveelheden informatie ondersteunt, het aantal benodigde retourvluchten minimaliseert en de verwerking van fouten verbetert.
- SNMPv3: Het voorgestelde RFC 2570-ontwerp biedt veilige toegang tot apparaten door de combinatie van verificatie en encryptie van pakketten via het netwerk. De beveiligingsfuncties in SNMPv3 zijn:Berichtintegriteit: garandeert dat er niet met een pakje is geknoeidVerificatie: bepaalt dat het bericht uit een geldige bron afkomstig isEncryptie: roamt de inhoud van een

pakje om te voorkomen dat het makkelijk te zien is door een niet - geautoriseerde bron
Deze tabel identificeert de combinaties van beveiligingsmodellen:

Model niveau	Verificatie	Versleuteling	Resultaat
v1	NoAuthNoPriv, Community-string	Nee	Gebruikt een community string match voor authenticatie.
v2c	NoAuthNoPriv, Community-string	Nee	Gebruikt een community string match voor authenticatie.
v3	AuthNoPriv, Username	Nee	Gebruikt een gebruikersnaam voor authenticatie.
v3	AutoNoPriv, MD5 of SHA	Np	Hier vindt u verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen.
v3	authPriv, MD5 of SHA	DES	Hier vindt u verificatie op basis van de HMAC-MD5 of HMAC-SHA-algoritmen. Biedt DES 56-bits codering naast verificatie op basis van de CBC-DES (DES-56)-standaard.

Opmerking: Let op deze informatie over SNMPv3 objecten:

- Elke gebruiker behoort tot een groep.
- Een groep definieert het toegangsbeleid voor een reeks gebruikers.
- Een toegangsbeleid definieert welke SNMP-objecten benaderd kunnen worden om te lezen, schrijven en te maken.
- Een groep bepaalt de lijst van kennisgevingen die de gebruikers kunnen ontvangen.
- Een groep definieert ook het beveiligingsmodel en het beveiligingsniveau voor de gebruikers.

SNMP-trap - aanbeveling

SNMP is de stichting van al netwerkbeheer en wordt toegelaten en gebruikt op alle netwerken. De SNMP-agent op de switch moet worden ingesteld om de versie van SNMP te gebruiken die wordt ondersteund door het beheerstation. Aangezien een agent met meerdere managers kan communiceren, is het mogelijk om de software te configureren om communicatie met één beheerstation te ondersteunen met behulp van het SNMPv1 protocol en een ander met behulp van het SNMPv2 protocol, bijvoorbeeld.

De meeste NMS-stations gebruiken vandaag nog SNMPv2C onder deze configuratie:

```
set snmp community read-only string
!--- Allow viewing of variables only. set snmp community read-write string
!--- Allow setting of variables. set snmp community read-write-all string
!--- Include setting of SNMP strings.
```

Cisco raadt aan SNMP-trap in te schakelen voor alle functies in gebruik (functies die niet worden gebruikt, kunnen indien gewenst worden uitgeschakeld). Als een val is ingeschakeld, kan deze worden getest met de **opdracht** test snmp **en de** juiste hantering op de NMS voor de fout (zoals een paginanummer of pop-up).

Alle vallen worden standaard uitgeschakeld en moeten aan de configuratie worden toegevoegd, individueel of met de **all** parameter, zoals wordt getoond:

```
set snmp trap enable all
set snmp trap server address read-only community string
```

De beschikbare vallen in CatOS 5.5 omvatten:

Trap	Beschrijving
oen	Verificatie
brug	overbruggen
landingsgestel	Chassis
configuratie	Configuratie
entiteit	entiteit
parelen	IP-vergunning
module	Module
repeater	repeteerster
stpx	Spanning Tree-uitbreiding
sloven	Syslog-melding
vmps	VLAN-Membership Policy Server
vtp	VLAN Trunk-protocol

Opmerking: De syslog-val stuurt ook alle syslog-berichten die door de switch zijn gegenereerd naar de NMS als SNMP-val. Als syslogarting al door een analyzer zoals Cisco Works 2000 RME's wordt uitgevoerd, is het niet noodzakelijk nuttig om deze informatie tweemaal te ontvangen.

In tegenstelling tot Cisco IOS-software zijn de vallen van SNMP van het poortniveau door standaard uitgeschakeld omdat switches honderden actieve interfaces kunnen hebben. Cisco raadt daarom aan dat belangrijke poorten, zoals infrastructurele links naar routers, switches en hoofdservers, SNMP-trap op poortniveau zijn ingeschakeld. Andere poorten, zoals host-poorten, zijn niet vereist, waardoor het netwerkbeheer wordt vereenvoudigd.

```
set port trap port range enable
!--- Enable on key ports only.
```

SNMP-stemaanbeveling

Een herziening van het netwerkbeheer wordt aanbevolen om specifieke behoeften in detail te bespreken. Enkele fundamentele Cisco-filosofieën voor het beheer van grote netwerken worden echter opgesomd:

- Doe iets eenvoudigs en doe het goed.
- Vermindert de overbelasting van het personeel door excessieve gegevensverzameling, verzameling, gereedschappen en handmatige analyse.
- Netwerkbeheer is mogelijk met slechts een paar tools, zoals HP OpenView als NMS, Cisco RME's als configuratie, configuratie, inventaris en softwaremanager, Microsoft Excel als een NMS-gegevensanalyzer en CGI als manier om naar het web te publiceren.
- Met het publiceren van rapporten aan het web kunnen gebruikers, zoals directeuren en analisten, zich helpen om informatie te verstrekken zonder het operationele personeel te belasten met vele speciale verzoeken.
- Zoek uit wat goed werkt op het netwerk en laat het met rust. Richt je op wat niet werkt.

De eerste fase van NMS-implementatie moet zijn gericht op de uitgangssituatie van de netwerkhardware. Er kan veel worden gevraagd over de status van het apparaat en de protocolstatus van een eenvoudige CPU, het geheugen en het buffergebruik op routers, en NMP CPU, het geheugen en het backplane gebruik op switches. Slechts nadat een hardware basislijn L2 en L3 verkeersbelasting doet, pieken en gemiddelde basislijnen volledig betekenisvol worden. Baselines worden gewoonlijk in verschillende maanden gevestigd om de dagelijkse, wekelijkse en driemaandelijkse trends zichtbaar te maken, afhankelijk van de conjunctuurcyclus van de onderneming.

Veel netwerken hebben te kampen met problemen met de prestaties en de capaciteit van MMS als gevolg van overpeinzing. Daarom wordt aanbevolen om, zodra de basislijn is vastgesteld, op de apparaten zelf alarmdrempels en RMON-drempels in te stellen om de NMS op abnormale veranderingen te waarschuwen en zo de stemming te verwijderen. Dit stelt het netwerk in staat om de exploitanten te vertellen wanneer iets niet normaal is, in plaats van voortdurend te peilen om te zien of alles normaal is. Drempelwaarden kunnen worden vastgesteld op basis van verschillende regels, zoals maximumwaarde plus een percentage of standaardafwijking van een gemiddelde, en vallen buiten het toepassingsgebied van dit document.

De tweede fase van de NMS-implementatie is om met SNMP meer in detail te kijken naar bepaalde gebieden van het netwerk. Dit omvat gebieden van twijfel, gebieden vóór verandering, of gebieden die gekarakteriseerd worden als goed functionerend. Gebruik de NMS-systemen als een zoeklicht om het netwerk in detail te scannen en brandwonden aan te geven (probeer niet het hele netwerk op te lichten).

De Cisco Network Management Consulting-groep stelt voor deze belangrijke fout-MIB's te analyseren of te controleren op campusnetwerken. Raadpleeg de Cisco Network Monitoring and Event Correlatie Guidelines voor meer informatie (over MIBs van prestaties om te bellen, bijvoorbeeld).

Naam van object	Beschrijving object	OID	Poll Interval	Drempel
MIB-II				
sysUpTime	systeemuptime in 1/100 seconden	1.3.6.1.2.1.1.3	5 min.	< 30000

Naam van	Beschrij	OID	Poll	Drem

object	ving object		Inter val	pel
CISCO-PROCES-MIB				
CPUTotal 5min	Het globale CPU drukke percentage in de laatste 5 minuten	1.3.6.1.4.1.9.9.109.1.1.1.1.5	10 min.	Baseline

Naam van object	Beschrijving object	OID	Poll Interval	Drempel
CISCO-STACK-MIB				
sysEnableChassisTraps	Geeft aan of de vallen van chassisAlarmOn en chassisAlarmOff in deze MIB moeten worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.24	24 uur	1
sysEnableModuleTraps	Geeft aan of moduleUp en moduleDown vallen in deze MIB moeten worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.25	24 uur	1
sysEnableBridgeTraps	Duidt op het feit of de vallen NewRoot and topologieChange in de BRIDGE-MIB (RFC 1493) moeten worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.26	24 uur	1
sysEnableRepeaterTraps	Geeft aan of de vallen in REPEATER-MIB (RFC1516) moeten worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.29	24 uur	1
sysEnableIpPermitTraps	Geeft aan of de IP-bestandsvallen in deze MIB moeten worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.31	24 uur	1

sysEnableVmpsTraps	Geeft aan of de vmVmpsChange-val die in CISCO-VLAN-MBERSHIP-MIB is gedefinieerd, moet worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.33	24 uur	1
sysEnableConfig	Geeft aan of sysConfigChange-val in deze MIB moet worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.35	24 uur	1
sysEnableStxTrap	Geeft aan of de stapInconsistentieUpdate-val in de CISCO-STP-EXTENSIES-MIB moet worden gegenereerd.	1.3.6.1.4.1.9.5.1.1.40	24 uur	1
chassis/PS1status	Status van de stroomvoorziening 1.	1.3.6.1.4.1.9.5.1.2.4	10 min.	2
chassis/PS1Test-resultaat	Gedetailleerde informatie over de stand van de elektriciteitsvoorziening 1.	1.3.6.1.4.1.9.5.1.2.5	Waar nodig.	
chassis/PS2Status	Status van de stroomvoorziening 2.	1.3.6.1.4.1.9.5.1.2.7	10 min.	2
chassisPS2TestResultaat	Gedetailleerde informatie over de stand van de elektriciteitsvoorziening 2	1.3.6.1.4.1.9.5.1.2.8	Waar nodig.	
ChassisFanStatus	Status van chassis ventilator	1.3.6.1.4.1.9.5.1.2.9	10 min.	2
ChassisFanTestResultaat	Gedetailleerde informatie over de status van de chassisventilator.	1.3.6.1.4.1.9.5.1.2.10	Waar nodig.	
ChassisMinorAlarm	De status van kleine alarmfase Chassis.	1.3.6.1.4.1.9.5.1.2.11	10 min.	1
Chassis MajorAlarm	Hoofdalarmstatus chassis	1.3.6.1.4.1.9.5.1.2.12	10 min.	1

ChassisTempAlarm	Alarmstatus chassis temperatuur.	1.3.6.1.4.1.9.5.1.2.13	10 min.	1
moduleStatus	Operationele status van de module.	1.3.6.1.4.1.9.5.1.3.1.1.10	30 min.	2
moduleTestResultaat	Gedetailleerde informatie over de moduscondities.	1.3.6.1.4.1.9.5.7.3.1.1.11	Waar nodig.	
moduleStandbyStatus	Status van een redundante module	1.3.6.1.4.1.9.5.7.3.1.1.21	30 min.	=1 of =4

Naam van object	Beschrijving object	OID	Poll Interval	Drempel
CISCO-MEMORY-POOL-MIB				
dot1dStpTimeByTopologieWijzigen	De tijd (in 1/100 seconden) sinds de laatste keer dat een topologie verandering door de entiteit werd gedetecteerd.	1.3.6.1.2.1.17.2.3	5 min.	< 30000
dot1dStpTopChanges	Het totale aantal topologieveranderingen die door deze brug worden gedetecteerd sinds de beheerentiteit voor het laatst werd hersteld of geformatteerd.	1.3.6.1.2.1.17.2.4	Waar nodig.	
dot1dStpPortState [1]	De huidige status van de poort zoals gedefinieerd door toepassing van het Spanning Tree Protocol.	1.3.6.1.2.1.17.2.15.1.3	Waar nodig.	

	De return value kan er één zijn: `gehandicapt (1), blokkeren (2), luisteren (3), leren (4), doorsturen (5),` of `breken (6).`			

Naam van object	Beschrijving object	OID	Poll Interval	Drempel
CISCO-MEMORY-POOL-MIB				
CiscoMemoryPoolGebruikte	Geeft het aantal bytes uit de geheugenpool aan die momenteel wordt gebruikt door toepassingen op het beheerde apparaat.	1.3.6.1.4.1.9.9.48.1.1.1.5	30 min.	Baseline
CiscoMemoryPoolFree	Geeft het aantal bytes uit de geheugenpool aan die op het beheerde apparaat nog niet is gebruikt. **Opmerking:** de som van ciscoMemoryPoolGebruikt en ciscoMemoryPoolFree is de totale hoeveelheid geheugen in de pool.	1.3.6.1.4.1.9.9.48.1.1.1.6	30 min.	Baseline
CiscoMemoryPoolLargestFree	Geeft het grootste aantal aaneengesloten bytes uit de geheugenpool aan die op het beheerde apparaat nog niet is gebruikt.	1.3.6.1.4.1.9.9.48.1.1.1.7	30 min.	Baseline

Raadpleeg de Cisco Network Management Toolkit - MIB's voor meer informatie over Cisco MIB-ondersteuning.

Opmerking: Sommige standaard MIB's gaan ervan uit dat een bepaalde SNMP-entiteit slechts één exemplaar van de MIB bevat. De standaard MIB heeft derhalve geen index die gebruikers rechtstreeks toegang geeft tot een bepaald geval van de MIB. In deze gevallen wordt indexering van het communautaire string verstrekt om toegang te krijgen tot elk exemplaar van de standaard MIB. De syntax is [community string]@[instantie number], waarbij een voorbeeld doorgaans een VLAN-nummer is.

Andere opties

De veiligheidsaspecten van SNMPv3 betekenen dat verwacht wordt dat het gebruik ervan SNMPv2 in de tijd zal inhalen. Cisco raadt klanten aan dit nieuwe protocol voor te bereiden als deel van hun MNS-strategie. De voordelen zijn dat gegevens veilig van SNMP apparaten kunnen worden verzameld zonder angst voor knoeien of corruptie. Vertrouwelijke informatie, zoals SNMP **set** commandopakketten die een switch configuratie wijzigen, kan worden versleuteld om te voorkomen dat de inhoud ervan op het netwerk wordt blootgesteld. Daarnaast kunnen verschillende gebruikersgroepen verschillende privileges hebben.

Opmerking: de configuratie van SNMPv3 is aanzienlijk anders dan de SNMPv2-opdrachtregel en de verhoogde CPU-belasting op de Supervisor Engine is te verwachten.

Externe bewaking

RMON maakt het mogelijk dat MIB-gegevens vooraf door het netwerkapparaat zelf worden verwerkt, ter voorbereiding op gemeenschappelijke toepassingen of toepassing van die informatie door de netwerkbeheerder, zoals het uitvoeren van historische basisbepaling en drempelanalyse.

De resultaten van RMON - verwerking worden opgeslagen in RMON MIBs voor verdere verzameling door een NMS, zoals gedefinieerd in RFC 1757 .

Overzicht

Catalyst switches ondersteunen mini-RMON in hardware op elke poort die uit vier basisgroepen RMON-1 bestaat: Statistieken (groep 1), Geschiedenis (groep 2), alarmen (groep 3), en Evenementen (groep 9).

Het machtigste deel van RMON-1 is het **drempelmechanisme** dat door de **alarm- en** eventgroepen wordt geboden. Zoals besproken, staat de configuratie van RMON - drempels de switch toe om een SNMP val te verzenden wanneer een anomalische omstandigheid zich voordoet. Zodra belangrijke havens zijn geïdentificeerd kan SNMP worden gebruikt om tellers of de groepen van de geschiedenis van RMON te krijgen en basislijnen te creëren die normale verkeersactiviteit voor die havens registreren. Vervolgens kunnen RMON - stijgende en dalende drempels worden ingesteld en alarmen worden ingesteld voor wanneer er een bepaalde afwijking van de basislijn is.

De configuratie van drempels wordt het best uitgevoerd met een RMON - beheerpakket, aangezien de succesvolle creatie van de rijen van parameters in Alarm en Event tabellen lastig is. Commerciële RMON NMS pakketten, zoals de Cisco Traffic Director, deel van Cisco Works 2000, bevatten GUIs die de instelling van RMON - drempels veel eenvoudiger maken.

Voor basislijnen biedt de etherStats-groep een nuttige reeks L2 verkeersstatistieken. De objecten in deze tabel kunnen worden gebruikt om statistieken te krijgen over unicast, multicast, en uitgezonden verkeer evenals een verscheidenheid aan L2 fouten. De RMON - agent op de switch kan ook worden geconfigureerd om deze bemonsterde waarden in de geschiedenisgroep op te slaan. Dit mechanisme maakt het mogelijk het aantal stemmen te verminderen zonder het aantal steekproeven te verlagen. RMON - historiën kunnen accurate basislijnen geven zonder substantiële ondertiteling. Hoe meer historiën worden verzameld, des te meer switches worden gebruikt.

Terwijl switches slechts vier basisgroepen RMON-1 leveren, is het belangrijk om de rest van RMON-1 en RMON-2 niet te vergeten. Alle groepen worden gedefinieerd in RFC 2021, inclusief USR History (groep 18) en ProbeConfig (groep 19). L3 en de hogere informatie kan van switches met de haven van SPAN of van VLAN ACL worden teruggewonnen om eigenschappen opnieuw te richten die u in staat stellen om verkeer naar een externe RMON SwitchProbe of een interne Module van de Netwerkanalyse (NAM) te kopiëren.

NAM's ondersteunen alle RMON - groepen en kunnen zelfs **toepassingslaaggegevens** onderzoeken, inclusief NetFlow-gegevens die worden geëxporteerd uit Catalyst wanneer MLS is ingeschakeld. Lopen MLS betekent dat de router niet alle pakketten in een stroom switch, zodat alleen NetFlow data-export en niet de interfacetellers een betrouwbare VLAN-accounting geven.

U kunt een SPAN poort en een switch sonde gebruiken om een pakketstroom voor een bepaalde poort, stam of VLAN op te nemen en de pakketten te uploaden om met een RMON - beheerpakket te decoderen. De SPAN-poort kan door de SPAN-groep in de CISCO-STACK-MIB worden bestuurd, zodat dit proces eenvoudig te automatiseren is. De Traffic Director maakt gebruik van deze functies met de functie ROVER-agent.

Er zijn voorbehouden om een heel VLAN te overspannen. Zelfs als u een 1 Gbps sonde gebruikt, kan de volledige pakketstroom van één VLAN of zelfs één 1 Gbps volledig-duplexpoort de bandbreedte van de SPAN poort overschrijden. Als de SPAN poort ononderbroken met volledige bandbreedte loopt, zijn de kansen gegevens verloren. Raadpleeg de functie Catalyst Switched Port Analyzer (SPAN) voor meer informatie.

Aanbeveling

Cisco raadt aan om RMON - drempels en alarmerend te worden opgesteld om netwerkbeheer op een intelligentere manier dan SNMP - opiniepeiling alleen te helpen. Dit vermindert netwerkbeheerverkeer overhead en stelt het netwerk in staat om verstandig te waarschuwen wanneer iets van de basislijn is veranderd. RMON moet worden bestuurd door een externe agent zoals verkeersdirecteur; er is geen CLI-ondersteuning. Geef deze opdrachten uit om RMON in te schakelen:

```
set snmp rmon enable
set snmp extendedrmon netflow enable mod
!--- For use with NAM module only.
```

Het is belangrijk om te onthouden dat de primaire functie van een switch is om frames door te sturen, om niet als een grote multi-poorts RMONsonde te handelen. Daarom, als u historiën en drempels op meerdere havens voor meerdere voorwaarden opstelt, houd in gedachten dat de middelen worden verbruikt. Neem een NAM module in overweging als u RMON scant. Herinner ook de kritieke havenregel: alleen opiniepeilingen en drempelwaarden voor de havens die in de planningsfase als belangrijk zijn aangemerkt .

Geheugenvereisten

RMON - geheugengebruik is constant bij alle platforms van de switch met betrekking tot statistieken, geschiedenissen, alarmen en gebeurtenissen. RMON gebruikt een emmer om historiën en statistieken op de RMON - agent (de switch, in dit geval) op te slaan. De emmer grootte wordt gedefinieerd op de RMON - sonde (de sonde van de Switch) of RMON - toepassing (Traffic Director), en vervolgens naar de switch gestuurd om te worden ingesteld. Gewoonlijk zijn geheugenbeperkingen slechts een overweging op oudere Supervisor Engine met minder dan 32 MB DRAM. Raadpleeg deze richtsnoeren:

- Ongeveer 450K aan coderuimte wordt aan het NMP-beeld toegevoegd om mini-RMON te ondersteunen (dat vier groepen RMON is: statistieken, geschiedenis, alarmen en gebeurtenissen). De vereisten voor dynamisch geheugen voor RMON variëren omdat het van de configuratie van de tijd afhangt. De time RMON - informatie over het geheugengebruik voor elke mini-RMON - groep wordt hier uitgelegd:Ethernet Statistics group-neemt 800 bytes voor elke switched Ethernet/FE-interface.History group-Voor de Ethernet interface, neemt elke geconfigureerde geschiedenis control-ingang met 50 emmers ongeveer 3,6 KB geheugenruimte en 56 bytes voor elke extra emmer mee.Alarmgroepen en gebeurtenissen: neemt 2,6KB in beslag voor elk geconfigureerd alarm en de bijbehorende eventitems.
- Om de RMON-gerelateerde configuratie op te slaan duurt ongeveer 20K NVRAM van ruimte als de systeemtotale grootte NVRAM 256K of meer en 10K NVRAM van ruimte is als de totale grootte NVRAM 128K is.

Netwerktijdprotocol

De NTP, RFC 1305 , synchroniseert de timing tussen een reeks gedistribueerde tijdservers en klanten en laat gebeurtenissen met elkaar in verband staan wanneer systeemlogbestanden worden gecreëerd of wanneer andere tijdspecifieke gebeurtenissen zich voordoen.

NTP biedt nauwkeurigheden van de clienttijd, doorgaans binnen een milliseconde op LAN's en tot een paar tientallen milliseconden op WAN's, in verhouding tot een primaire server die is gesynchroniseerd met Integrated Universal Time (UTC). 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.

Overzicht

NTP werd eerst gedocumenteerd in RFC 958 , maar is geëvolueerd via RFC 1119 (NTP versie 2) en is nu opgenomen in de derde versie zoals gedefinieerd in RFC 1305 . Het loopt over UDP poort 123. Alle NTP-communicatie gebruikt UTC, wat hetzelfde is als Greenwich Mean Time.

Openbare tijdservers gebruiken

NTP-net omvat momenteel meer dan 50 openbare primaire servers die rechtstreeks aan UTC zijn gesynchroniseerd 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 gesynchroniseerd op de primaire servers die synchronisatie bieden aan meer dan 100.000 klanten en servers op het internet. De huidige lijsten worden onderhouden op de pagina Lijst van openbare NTP-servers, die regelmatig wordt bijgewerkt. Er zijn talrijke

particuliere primaire en secundaire servers die normaal niet ook voor het publiek beschikbaar zijn. Voor een lijst van openbare NTP servers en informatie over hoe ze te gebruiken, raadpleeg de website van de University of Delaware Time Synchronization Server .

Aangezien er geen garantie is dat deze openbare NTP-servers beschikbaar zullen zijn of dat zij de juiste tijd produceren, wordt er sterk op aangedrongen dat andere opties worden overwogen. Dit kan het gebruik van verschillende standalone Global Positioning Service (GPS)-apparaten omvatten die direct op een aantal routers zijn aangesloten.

Een andere mogelijke optie is het gebruik van verschillende routers geconfigureerd als Stratum 1-meesters, hoewel dit niet wordt aanbevolen.

Stratum

Elke NTP server adopteert een stratum dat aangeeft hoe ver weg van een externe bron van tijd de server is. Stratum 1-servers hebben toegang tot een externe tijdbron, zoals een radiokloktijd. Stratum 2-servers krijgen tijdgegevens van een reeks van Stratum 1-servers, terwijl Stratum 3-servers tijdgegevens van Stratum 2-servers krijgen, enzovoort.

Relatie tussen servers

- Een server is er een die reageert op clientverzoeken maar niet probeert datuminformatie uit een clientbron op te nemen.
- Een peer is er een die reageert op verzoeken van klanten, maar probeert de verzoeken van klanten te gebruiken als potentiële kandidaat voor een betere tijdbron en om te helpen bij de stabilisatie van de klokfrequentie.
- Om een echte peer te zijn, moeten beide kanten van de verbinding in een peer relatie binnengaan in plaats van een gebruiker een peer en de andere gebruiker een server te hebben. Het wordt ook aanbevolen dat peers sleutels uitwisselen zodat alleen vertrouwde hosts met elkaar praten als gelijken.
- In een client verzoek aan een server beantwoordt de server de client en vergeet dat de client ooit een vraag heeft gesteld. in een client verzoek aan een peer , beantwoordt de server de client en houdt de statinformatie over de client bij om te achterhalen hoe goed het op tijd doet en welke stratum server het runt .**Opmerking:** CatOS kan alleen optreden als NTP-client.

Het is geen probleem voor een NTP server om vele duizenden cliënten te behandelen. Honderden peers verwerken heeft echter een impact op het geheugen en het staatsonderhoud verbruikt zowel de CPU-middelen als de bandbreedte meer.

Verkiezingen

Het NTP protocol staat een client toe om een server te vragen wanneer het wil. In feite, wanneer NTP voor het eerst in een apparaat van Cisco wordt gevormd, stuurt het acht vragen in snelle opvolging bij NTP_MINPOLL (24 = 16 seconden) intervallen uit. NTP_MAXPOLL is 214 seconden (dat is 16.384 seconden of 4 uur, 33 minuten, 4 seconden), de maximale tijd die het nodig heeft voordat NTP opnieuw instelt voor een respons. Op dit moment heeft Cisco geen methode om de POLL-tijd handmatig te forceren die door de gebruiker moet worden ingesteld.

De NTP-stempelteller begint op 2^6 (64) seconden en wordt verhoogd door twee machten (als de twee servers sync met elkaar) naar 2^{10}. Dat wil zeggen, u kunt verwachten dat de sync-berichten tussen 64, 128, 256, 512 of 1024 worden verzonden seconden per geconfigureerde server of

peer. De tijd varieert tussen 64 seconden en 1024 seconden als een vermogen van twee gebaseerd op de fase-vergrendelde lus die pakketten verstuurt en ontvangt. Als er in die tijd veel kritiek is, komt dat vaker voor. Als de referentieklok nauwkeurig is en de netwerkconnectiviteit consistent is, ziet u de opinietijden samenvallen op 1024 seconden tussen elke opiniepeiling.

In de echte wereld betekent dit dat het NTP Poll Interval verandert aangezien de verbinding tussen de client en de server verandert. Hoe beter de verbinding, hoe langer het poll interval, wat betekent dat de NTP-client acht reacties heeft ontvangen voor zijn laatste acht verzoeken (het poll-interval is dan verdubbeld). Een enkele gemiste reactie zorgt ervoor dat het poll interval gehalveerd wordt. Het poll-interval begint bij 64 seconden en loopt tot maximaal 1024 seconden. In het beste geval duurt het iets meer dan twee uur voordat het poll-interval van 64 seconden naar 1024 seconden gaat.

Uitzending

NTP-uitzendingen worden nooit doorgestuurd. De opdracht **ntp-uitzending** veroorzaakt de router om NTP-uitzendingen te genereren op de interface waarop deze is geconfigureerd. De opdracht **ntp zendt** de router of switch toe om naar NTP-uitzendingen te luisteren op de interface waarop het wordt geconfigureerd.

NTP-verkeersniveaus

De bandbreedte die door NTP wordt gebruikt is minimaal, aangezien het interval tussen stemberichten die tussen peers worden uitgewisseld gewoonlijk terugratches naar niet meer dan één bericht elke 17 minuten (1024 seconden). Met zorgvuldige planning kan dit binnen routernetwerken via de WAN-koppelingen worden onderhouden. De NTP-klanten moeten zich richten op lokale NTP-servers, niet volledig over WAN naar de centrale server-kernrouters die de stratum 2-servers zullen zijn.

Een geconvergeerde NTP client gebruikt ongeveer 0,6 bits/seconde per server.

Aanbeveling

Veel klanten hebben NTP vandaag in clientmodus ingesteld op hun CatOS-platforms, gesynchroniseerd vanuit verschillende betrouwbare feeds van het internet of een radioklok. Echter, een eenvoudiger alternatief voor servermodus bij het gebruik van een groot aantal switches is NTP in uitzending clientmodus op het beheer VLAN in een geschakeld domein in te schakelen. Dit mechanisme staat een volledig domein van Catalysatoren toe om een klok van één enkel uitzending te ontvangen. De nauwkeurigheid van de tijdscontrole wordt echter marginaal beperkt, omdat de informatiestroom eenrichtingsverkeer is.

Het gebruik van loopback adressen als bron van updates kan ook met consistentie helpen. De veiligheidsproblemen kunnen op deze twee manieren worden aangepakt:

- Filmserverupdates
- Verificatie

De tijdcorrelatie van de gebeurtenissen is in twee gevallen uiterst waardevol: problemen oplossen en veiligheidscontroles . Voorzichtigheid is geboden om de tijdbronnen en gegevens te beschermen en encryptie wordt aanbevolen om te voorkomen dat belangrijke gebeurtenissen opzettelijk of onbedoeld worden gewist.

Cisco raadt deze configuraties aan:

Catalyst-configuratie

```
set ntp broadcastclient enable
set ntp authentication enable
set ntp key key
!--- This is a Message Digest 5 (MD5) hash. set ntp
timezone
```

Alternatieve Catalyst-configuratie

```
!--- This more traditional configuration creates !---
more configuration work and NTP peerings. set ntp client
enable
set ntp server IP address of time server set timezone
zone name set summertime date change details
```

Routerconfiguratie

```
!--- This is a sample router configuration to distribute
!--- NTP broadcast information to the Catalyst broadcast
clients. ntp source loopback0
ntp server IP address of time server ntp update-calendar
clock timezone zone name clock summer-time date change
details ntp authentication key key ntp access-group
access-list
!--- To filter updates to allow only trusted sources of
NTP information. Interface to campus/management VLAN
containing switch sc0 ntp broadcast
```

Cisco-detectieprotocol

CDP wisselt informatie uit tussen aangrenzende apparaten over de datalink-laag en is zeer behulpzaam bij de bepaling van de netwerktopologie en de fysieke configuratie buiten de logische of IP-laag. Ondersteunde apparaten zijn vooral switches, routers en IP-telefoons. Deze sectie belicht een aantal verbeteringen van CDP versie 2 boven versie 1.

Overzicht

CDP gebruikt SNAP-insluiting met type code 2000. Op Ethernet, ATM en FDDI, wordt het bestemming multicast adres **01-00-0c-cc-cc, HDLC protocol type 0x2000** gebruikt. Op Token Rings wordt het functionele adres c000.0800.000 gebruikt. CDP-frames worden standaard elke minuut verzonden.

CDP-berichten bevatten een of meer subberichten waarmee de doelapparaten informatie over elk buurapparaat kunnen verzamelen en opslaan.

CDP versie 1 ondersteunt deze parameters:

Parameter	Type	Beschrijving
1	ApparaatID	Hostnaam van het apparaat of hardwareserienummer in ASCII.
2	Adres	Het L3 adres van de interface die de update heeft verzonden.
3	Port-ID	De haven waarop de CDP-update is verstuurd.
4	Capaciteit	Beschrijft de functionele functies van het apparaat: router: 0x01 TB-brug: 0x02 SR-brug: 0x04 Switch: 0x08 (biedt L2- en/of L3-switching) host: 0x10 IGMP voorwaardelijk filteren: 0x20 De brug of de Switch zendt IGMP geen rapport pakketten op niet routers door. Repeater: 0x40
5	Versie	Een tekenstring met daarin de softwareversie (dezelfde als in de **show-versie**).
6	platform	Hardware platform, zoals WS-C5000, WS-C6009 of Cisco RSP.

In CDP versie 2 zijn extra protocolvelden geïntroduceerd. CDP versie 2 ondersteunt elk veld maar de in de lijst opgenomen velden kunnen in bepaalde omgevingen bijzonder nuttig zijn en worden gebruikt in CatOS.

Opmerking: Als een switch CDPv1 draait, worden v2-frames verlaagd. Wanneer een switch die CDPv2 draait een CDPv1 frame op een interface ontvangt, zal hij naast CDPv2-frames ook CDPv1-frames naar buiten sturen.

Parameter	Type	Beschrijving
9	VTP-domein	Het VTP-domein, indien geconfigureerd op het apparaat.
10	Native VLAN	In punt1q, is dit het niet gelabelde VLAN.
11	Full/Half-Duplex	Dit veld bevat de tweezijdige instelling van de verzendende poort.

Aanbeveling

CDP wordt standaard ingeschakeld en is essentieel om zichtbaarheid van aangrenzende apparaten te verkrijgen en problemen op te lossen. Het wordt ook gebruikt door netwerkbeheertoepassingen om L2 topologieën kaarten te bouwen. Geef deze opdrachten uit om CDP op te zetten:

```
set cdp enable
!--- This is the default. set cdp version v2
!--- This is the default.
```

In delen van het netwerk waar een hoog beveiligingsniveau vereist is (zoals DMZ's op het internet), moet CDP als dusdanig zijn uitgeschakeld:

```
set cdp disable port range
```

De opdracht Cdp-buren toont de lokale CDP-tabel. Vermeldingen die zijn gemarkeerd met een ster (*) geven een VLAN-mismatch aan. items die zijn gemarkeerd met een # geven een dubbele mismatch aan. Dit kan een waardevolle hulp zijn bij het oplossen van problemen.

```
>show cdp neighbors

* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port  Device-ID          Port-ID Platform
----- ------------------ ------- ------------
 3/1  TBA04060103(swi-2) 3/1     WS-C6506
 3/8  TBA03300081(swi-3) 1/1     WS-C6506
15/1  rtr-1-msfc         VLAN 1  cisco    Cat6k-MSFC
16/1  MSFC1b             Vlan2   cisco    Cat6k-MSFC
```

Andere opties

Sommige switches, zoals Catalyst 6500/6000, hebben de mogelijkheid om stroom door middel van kabels van het UTP aan IP telefoons te leveren. Informatie die wordt ontvangen door middel van CDP helpt het energiebeheer op de switch.

Aangezien IP telefoons een PC kunnen hebben die op hen wordt aangesloten, en beide apparaten verbinden aan de zelfde poort op de Catalyst, heeft de switch de mogelijkheid om de VoIP telefoon in een afzonderlijk VLAN, de hulpstof, te plaatsen. Hierdoor kan de switch eenvoudig een andere QoS-kwaliteit (Quality of Service) voor het VoIP-verkeer toepassen.

Als bovendien het hulpVLAN wordt aangepast (bijvoorbeeld om de telefoon te dwingen om een specifiek VLAN of een specifieke tagging methode te gebruiken), wordt deze informatie naar de telefoon door middel van CDP verzonden.

Parameter	Type	Beschrijving
14	Applicatie-id	Hiermee kan het VoIP-verkeer worden gedifferentieerd van ander verkeer, zoals door afzonderlijke VLAN-id (extra VLAN).
16	Stroomverbruik	De hoeveelheid energie die een VoIP-telefoon verbruikt, in milliwatt.

Opmerking: Catalyst 2900 en 3500XL switches ondersteunen momenteel geen CDPv2.

Beveiligingsconfiguratie

Idealiter heeft de klant al een beveiligingsbeleid ingesteld om te helpen definiëren welke tools en technologieën van Cisco gekwalificeerd zijn.

Opmerking: Cisco IOS-softwarerelease, in tegenstelling tot CatOS, wordt in veel documenten behandeld, zoals Cisco ISP wezenlijk.

Functies voor basisbeveiliging

Wachtwoorden

Het wachtwoord op gebruikersniveau configureren (inloggen). Wachtwoorden zijn hoofdlettergevoelig in CatOS 5.x en hoger en kunnen van 0 tot 30 tekens lang zijn, inclusief spaties. Wachtwoord instellen:

```
set password password set enablepass password
```

Alle wachtwoorden moeten aan minimum lengte normen voldoen (bijvoorbeeld zes tekens minimaal, een combinatie van letters en getallen, bovenste en onderste letters) voor inlognaam en indien gebruikt wachtwoorden inschakelen. Deze wachtwoorden worden versleuteld met het algoritme MD5.

Om voor meer flexibiliteit in het beheer van wachtwoordbeveiliging en toegang tot het apparaat te staan, adviseert Cisco het gebruik van een TACACS+ server. Raadpleeg het gedeelte TACACS+ van dit document voor meer informatie.

Secure Shell

Gebruik SSH-encryptie om beveiliging te bieden voor Telnet-sessies en andere externe verbindingen naar de switch. SSH-encryptie wordt alleen ondersteund voor afstandsbediening naar de switch. U kunt Telnet-sessies niet versleutelen die vanaf de switch worden geïnitieerd. SSH versie 1 wordt ondersteund in CatOS 6.1 en versie 2 ondersteuning werd toegevoegd in CatOS 8.3. SSH versie 1 ondersteunt de gegevensencryptie Standard (DES) en Triple-DES (3-DES) encryptiemethoden en SSH versie 2 ondersteunt de 3-DES en Advanced Encryption Standard (AES)-encryptiemethoden. U kunt SSH-encryptie gebruiken met RADIUS- en TACACS+-verificatie. Deze optie wordt ondersteund door SSH (k9)-afbeeldingen. Raadpleeg hoe u SSH kunt configureren op Catalyst Switches die CatOS uitvoeren voor meer informatie.

```
set crypto key rsa 1024
```

Om versie 1-back uit te schakelen en versie 2-verbindingen te aanvaarden, geeft u deze opdracht uit:

```
set ssh mode v2
```

IP-toegangsfilters

Dit zijn filters om toegang tot de sc0 interface van het beheer door telnet en andere protocollen te waarborgen. Deze zijn vooral belangrijk wanneer het VLAN dat voor beheer wordt gebruikt ook gebruikers bevat. Geef deze opdrachten uit om IP-adres en poortfiltering in te schakelen:

```
set ip permit enable
set ip permit IP address mask Telnet|ssh|snmp|all
```

Als de toegang tot telnet echter met deze opdracht is beperkt, kan de toegang tot CatOS-apparaten alleen worden bereikt via een paar vertrouwde end-stations. Deze installatie kan een belemmering vormen voor het oplossen van problemen. Houd in gedachten dat het mogelijk is om IP-adressen te bederven en gefilterde toegang voor gek te houden, dus dit is slechts de eerste beschermingslaag.

Poortbeveiliging

Overweeg het gebruik van havenveiligheid om slechts één of meerdere bekende adressen van MAC toe te staan om gegevens op een bepaalde haven door te geven (om de statische eindstations tegen te houden voor nieuwe stations zonder veranderingscontrole, bijvoorbeeld). Dit is mogelijk door statische MAC adressen.

```
set port security mod/port enable MAC address
```

Dit is ook mogelijk door de beperkte MAC adressen dynamisch te leren.

```
set port security port range enable
```

Deze opties kunnen worden ingesteld:

- de *tijdwaarde* van de *poort op* security instellen, specificeert de duur waarvoor de adressen op de poort zijn beveiligd voordat een nieuw adres kan worden geleerd. Geldige tijd in minuten is 10-1440. Standaard is geen veroudering.
- stel port *security mod/port* maximum *waarde* - sleutelwoord in dat het maximum aantal MAC adressen om op de poort te beveiligen specificeert. Geldige waarden zijn 1 (standaard) - 1025.
- Stel de *mod/*de shutdown van de havenveiligheid in*/poort*—sluit de haven (standaard) af als de schending ook overschrijdt en verstuurt syslogbericht (standaard) en vergooit het verkeer.
- Stel *de waarde van de* sluitingstijd van de haven*/*de *tijd* —duur in waarvoor een haven gehandicapt blijft. Geldige waarden zijn 10-1440 minuten. Standaard wordt de projector permanent afgesloten

Met CatOS 6.x en later, heeft Cisco 802.1x authenticatie geïntroduceerd die cliënten om aan een centrale server voor te schrijven toestaat voor poorten voor gegevens kunnen worden ingeschakeld. Deze optie bevindt zich in de vroege stadia van ondersteuning op platforms zoals Windows XP, maar kan door veel bedrijven als een strategische richting worden beschouwd. Raadpleeg Port Security configureren voor informatie over het configureren van poortbeveiliging op switches die Cisco IOS-software uitvoeren.

Login Banners

Maak geschikte apparaatbanners om specifiek de acties te vermelden die worden ondernomen voor toegang door onbevoegden. Deel geen naam van de site of netwerkgegevens die informatie kunnen verstrekken aan niet-geautoriseerde gebruikers. Deze spandoeken bieden hun toevlucht in het geval dat een toestel wordt aangetast en de dader wordt betrapt:

```
# set banner motd ^C
*** Unauthorized Access Prohibited ***
***  All transactions are logged   ***
------------- Notice Board -------------
----Contact Joe Cisco at 1 800 go cisco for access problems----
^C
```

Fysieke beveiliging

Apparaten mogen niet fysiek toegankelijk zijn zonder de juiste toestemming, zodat de apparatuur zich in een gecontroleerde (vergrendelde) ruimte bevindt. Om ervoor te zorgen dat het netwerk operationeel blijft en niet wordt beïnvloed door kwaadaardige manipulatie van milieufactoren, moet alle apparatuur over een geschikte UPS (met indien mogelijk redundante bronnen) en temperatuurregeling (airconditioning) beschikken. Onthoud, als fysieke toegang door een persoon met kwaadwillige bedoeling wordt geschonden, is verstoring door wachtwoordherstel of andere methoden veel waarschijnlijker.

Terminal Access Control-systeem

Standaard zijn de niet-geprivilegieerde en geprivilegieerde wachtwoorden mondiaal en zijn ze van toepassing op elke gebruiker die de switch of router benadert, vanuit de console poort of via een Telnet-sessie over het netwerk. Hun implementatie op netwerkapparaten is tijdrovend en niet-gecentraliseerd. Het is ook lastig om toegangsbeperkingen uit te voeren met behulp van toegangslijsten die kunnen worden blootgesteld aan configuratiefouten.

Er zijn drie beveiligingssystemen beschikbaar om de controle en de toegang van de politie tot netwerkapparaten te vergemakkelijken. Deze gebruiken client/server architecturen om alle veiligheidsinformatie in één centrale database te plaatsen. Deze drie beveiligingssystemen zijn:

- TACACS+
- RADIUS
- Kerberos

TACACS+ is een gemeenschappelijke toepassing in Cisco-netwerken en vormt de focus van dit hoofdstuk. Dit biedt de volgende functies:

- Verificatie-het identificatie- en verificatieproces voor een gebruiker. Er kunnen verschillende methoden worden gebruikt om een gebruiker te authentiseren, maar de meest voorkomende methode is een combinatie van naam en wachtwoord.
- Verificatie-van verschillende opdrachten kunnen worden toegestaan zodra een gebruiker voor de authenticatie is gewaarmerkt.
- Boekhouding-de opname wat een gebruiker op het apparaat doet of heeft gedaan.

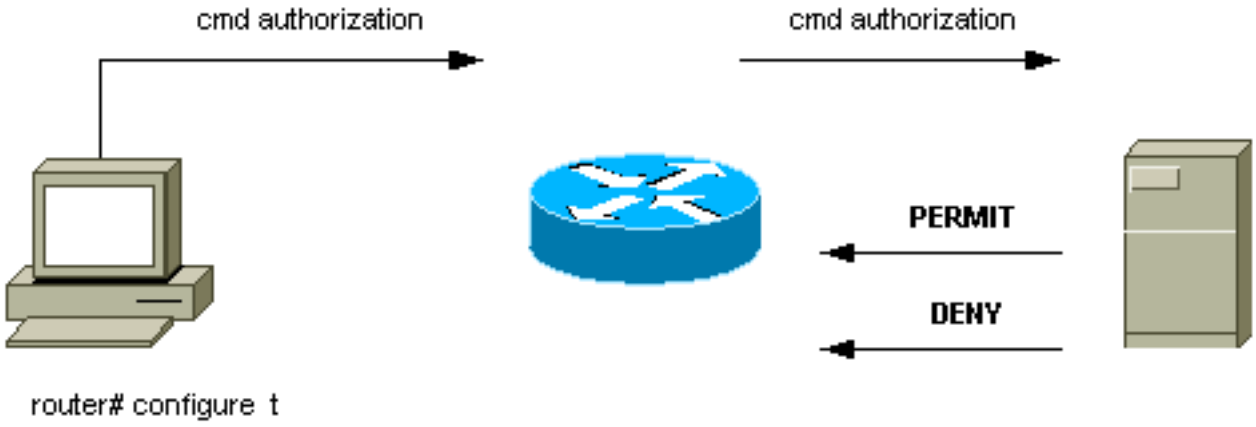
Raadpleeg TACACS+, RADIUS en Kerberos configureren op Cisco Catalyst Switches voor meer informatie.

Overzicht

Het TACACS+ protocol doorstuurt gebruikersnamen en wachtwoorden naar de gecentraliseerde server, versleuteld via het netwerk met één manier om **MD5** te hashing (RFC 1321). Het gebruikt TCP poort 49 als zijn transportprotocol; Dit biedt deze voordelen ten opzichte van UDP (gebruikt door RADIUS):

- Op aansluiting gericht vervoer
- Aparte erkenning dat een verzoek is ontvangen (TCP ACK), ongeacht hoe geladen het backend-authenticatiemechanisme momenteel is
- Onmiddellijke indicatie van een serverongeluk (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. Dit zorgt voor meer controle over de opdrachten die op de switch kunnen worden uitgevoerd terwijl de koppeling van het verificatiemechanisme wordt losgekoppeld. Met behulp van opdrachtaccounting kan de opdracht worden gecontroleerd die een bepaalde gebruiker heeft afgegeven terwijl hij aan een bepaald netwerkapparaat is gekoppeld.



Wanneer een gebruiker een eenvoudige ASCII-inlognaam probeert te controleren door verificatie van een netwerkapparaat met TACACS+, gebeurt dit proces doorgaans:

- Wanneer de verbinding wordt gelegd, contacteert de switch de TACACS+-daemon om een gebruikersnaam te verkrijgen die dan aan de gebruiker wordt weergegeven. 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 wachtwoordmelding weer aan de gebruiker, die dan een wachtwoord invoert dat ook naar de TACACS+-naam wordt verzonden.
- Het netwerkapparaat ontvangt uiteindelijk een van deze reacties van de TACACS+-datum:ACCEPT-e gebruiker is echt en de service 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 kan verdere toegang worden ontzegd of wordt gevraagd de loginsequentie opnieuw in te stellen, afhankelijk van de TACACS+-datum.FOUT-een fout is op een bepaald moment tijdens verificatie opgetreden. Dit kan zijn bij de daemon of in de netwerkverbinding tussen de daemon en de switch. Als een FOUTrespons wordt ontvangen, probeert het netwerkapparaat gewoonlijk een alternatieve methode te gebruiken om de gebruiker voor de gek te houden.GA DOOR—de gebruiker wordt opgeroepen voor extra verificatieinformatie.
- 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 en wordt een ACCEPT- of AFWIJZINGSAANVRAAG ingediend. 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, en bepaalt hij de opdrachten waar de gebruiker toegang toe heeft.

Aanbeveling

Cisco raadt het gebruik van TACACS+ aan, omdat het makkelijk kan worden geïmplementeerd met behulp van Cisco Secure ACS voor NT, Unix of andere software van derden. TACACS+-functies omvatten een gedetailleerde boekhouding om statistieken te verschaffen over het gebruik van commando's en systemen, MD5-encryptie-algoritme en administratieve controle van de echtheids- en autorisatieprocessen.

In dit voorbeeld, inloggen en inschakelen de modi de TACACS+ server voor verificatie gebruiken en kunnen deze terugvallen op lokale verificatie als de server niet beschikbaar is. Dit is een belangrijke achterdeur om in de meeste netwerken te verlaten. Geef deze opdrachten uit om TACACS+ in te stellen:

```
set tacacs server server IP primary set tacacs server server IP
!--- Redundant servers are possible. set tacacs attempts 3
!--- This is the default. set tacacs key key
!--- MD5 encryption key. set tacacs timeout 15
!--- Longer server timeout (5 is default). set authentication login tacacs enable
set authentication enable tacacs enable
set authentication login local enable
set authentication enable local enable
!--- The last two commands are the default; they allow fallback !--- to local if no TACACS+
server available.
```

Andere opties

Het is mogelijk om een TACACS+ vergunning te gebruiken om de opdrachten te besturen die elke gebruiker of gebruikersgroep op de switch kan uitvoeren, maar het is moeilijk om een aanbeveling te doen omdat alle klanten op dit gebied individuele eisen hebben. Raadpleeg Toegang tot de Switch controleren met behulp van verificatie, autorisatie en accounting voor meer informatie.

Ten slotte bieden boekhoudkundige opdrachten een controletraject van wat elke gebruiker typt en geconfigureerd heeft. Dit is een voorbeeld dat gebruikmaakt van de gebruikelijke praktijk om de auditinformatie aan het eind van de opdracht te ontvangen:

```
set accounting connect enable start-stop tacacs+
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
set accounting update periodic 1
```

Deze configuratie heeft deze functies:

- De opdracht **verbinden** maakt accounting van uitgaande verbindingsgebeurtenissen op de switch zoals telnet mogelijk.

- De exec-opdracht maakt het mogelijk om inlogsessies op de switch, zoals het bewerkingspersoneel, te accounting.
- De systeemopdracht maakt het mogelijk om systeemgebeurtenissen op de switch te verwerken, zoals opnieuw laden of resetten.
- De opdracht maakt rekenschap van wat op de switch was ingevoerd mogelijk, zowel voor tonen **als** voor het configureren.
- Periodieke *updates* per minuut aan de server zijn behulpzaam om op te nemen of de gebruikers nog inlogd zijn.

Configuratiecontrolelijst

In dit deel wordt een samenvatting gegeven van de aanbevolen configuraties, met uitzondering van de veiligheidsgegevens.

Het is zeer nuttig om alle havens te etiketteren. Geef deze opdracht uit om de poorten te etiketteren:

```
set port description descriptive name
```

Gebruik deze toets in combinatie met de tabellen voor opdracht die zijn opgenomen:

Sleutel:
Vage tekst - aanbevolen wijziging
Normale tekst - standaard, aanbevolen instelling

Opdrachten voor wereldwijde configuratie

Opdracht	Opmerking
vtp - *domeinnaam passWord instellen*	Beveiliging tegen onbevoegde VTP-updates tegen nieuwe switches.
vtp-modus transparant	Selecteer VTP-modus die in dit document wordt bevorderd. Raadpleeg de sectie VLAN Trunking Protocol van dit document voor meer informatie.
spanboom instellen als alle mogelijkheden aanwezig zijn	Zorg ervoor dat STP op alle VLAN's is ingeschakeld.
stel spantree root *VLAN* in	Aanbevolen om root (en secundaire root) bruggen per VLAN te plaatsen.
instellen van de spantree backbonefast	Snellere STP-convergentie van indirecte fouten inschakelen (alleen als alle switches in het domein de functie ondersteunen).
zet spantree uplinkfast	Kunt u snelle STP-conversie van

aan	directe fouten inschakelen (alleen voor switches op de toegangslaag).
spanboomstam geschikt voor bpdu	Schakel de poort in om automatisch te worden afgesloten als er een niet-geautoriseerde Spanning Tree-extensie is.
instellen	Schakel de detectie van een unidirectionele link in (ook configuratie op poortniveau).
testdiagonaal compleet	volledige diagnostiek inschakelen bij het opstarten (standaard Catalyst 4500/4000).
set test packetbuffer sun 3:30	Schakel controle van fouten door poortbuffer in (alleen van toepassing op Catalyst 5500/5000).
zetten houtkapbuffer 500	Zorg voor maximale interne syslogbuffer.
IP-adres ***van logserver***	Configureer de doelserver voor het registreren van externe systeemmeldingen.
setlogserver	Toestaan de externe logserver.
tijdstempel voor vastzetten	Laat tijden van berichten in het logbestand toe.
instelniveau spanboom 6 standaard	Verhoog standaard STP syslg niveau.
niveau voor bloggen instellen syber 6 standaard	Standaardsysteemniveau verhogen
ernst van logserver instellen 4	Toestaan dat de zwaardere strook alleen wordt uitgevoerd.
vastlogconsole uitschakelen	Schakel de console uit, tenzij u problemen oplossen.
set snmp community read-only *string*	Configureer het wachtwoord zodat gegevens op afstand kunnen worden verzameld.
vaste *snmp community read*-**schrijf** *string*	Configureer het wachtwoord om de configuratie op afstand toe te staan.
vaste *snmp* **community read-writers-all** *string*	Configureer het wachtwoord zodat het op afstand kan worden ingesteld, inclusief wachtwoorden.
zet snmp trap in	SNMP-trap naar de NMS-server inschakelen voor signaleringen met fouten en gebeurtenissen.

set snmp trap ***server address string***	Het adres van de NMS-vanger configureren.
forceren	RMON - inschakelen voor lokale statistische verzameling. Raadpleeg het gedeelte Afstandsbewaking van dit document voor meer informatie.
set ntp omroep client zet	Kunt u nauwkeurige systeemklokontvangst vanaf een upstream router inschakelen.
naam **van de ntp -** *tijdzone*	Stel de lokale tijdzone voor het apparaat in.
details **van ntp summertime** *date change*	Stel zonodig de zomertijd in voor de tijdzone.
set ntp authenticatie mogelijk	Gecodeerde tijdinformatie voor veiligheidsdoeleinden configureren.
ntp-*toets* **instellen**	Configuratie van de encryptiesleutel.
cdp instellen	Zorg ervoor dat de buurontdekking is ingeschakeld (ook ingeschakeld op poorten).
primaire *IP-***adressaat van tacacs server**	Configureer het adres van de AAA-server.
IP-adres **van tacs-server**	Redundant AAA-servers indien mogelijk.
tac ' s instellen 3	3 wachtwoordpogingen voor de AAA-gebruikersaccount toestaan
tacacs - *toets* **instellen**	Stel de AAA MD5 encryptie-toets in.
reeks tactieken - out 15	Toestaan van een langere servertijd (vijf seconden is standaard).
set authenticatie loginlogtacacs inschakelen	Gebruik AAA voor verificatie voor inloggen.
set authenticatie mogelijk	Gebruik AAA voor verificatie om modus mogelijk te maken.
lokale toetsenbord voor verificatie instellen	Standaard; maakt een back-up naar een lokale computer mogelijk als er geen AAA-server beschikbaar is.
locale verificatie mogelijk maken	Standaard; maakt een back-up naar een lokale computer mogelijk als er geen AAA-server beschikbaar is.

Configuratieopdrachten voor hostpoorten

Opdracht	Opmerking
poortbereik **instellen**	Verwijder overbodige poortverwerking. Deze macro stelt spantree PortFast in, kanaliseer uit, stam uit.
instelbaar *bereik* instelbaar	Verwijder overbodige poortverwerking (standaard uitgeschakeld op koperpoort).
auto met *poortbereik* instellen	Gebruik automatische onderhandeling met up-to-date host NIC-stuurprogramma's.
instellen *poortbereik* uitschakelen	Geen SNMP-vallen nodig voor algemene gebruikers; alleen belangrijke poorten.

Configuratieopdrachten voor servers

Opdracht	Opmerking
poortbereik **instellen**	Verwijder overbodige poortverwerking. Deze macro stelt spantree PortFast in, kanaliseer uit, stam uit.
instelbaar *bereik* instelbaar	Verwijder overbodige poortverwerking (standaard uitgeschakeld op koperpoort).
ingesteld *poortbereik 10 | 100*	Configureer normaal statische/serverpoorten; anders wordt gebruik gemaakt van autonome onderhandelingen .
ingesteld port duplex *poortbereik volledig | helft*	Doorgaans statische/serverpoorten; anders wordt gebruik gemaakt van autonome onderhandelingen .
poortbereik **instellen** *voor* **poortval**	Belangrijkste dienstenhavens moeten de NMS een val geven.

Configuratieopdrachten voor ongebruikte poorten

Opdracht	Opmerking
stel spantree *port range* , *in*	Schakel de benodigde poortverwerking en beveiliging voor STP in.
stel poortbereik *in*	Ongebruikte poorten uitschakelen.
set vlan *ongebruikt dummy vlan poortbereik*	Direct onbevoegd verkeer naar ongebruikt VLAN als de poort is ingeschakeld.
zet *poortbereik* **uit**	Uitschakelen van de "trunking" tot toediening.

stel wijze van *poortbereik* in	Uitschakelen van kantelpoort tot toediening.

Infrastructuurpoorten (switch-switch, switch-router)

Opdracht	Opmerking
ingesteld udld, *poortbereik instellen*	Schakel de detectie van een unidirectionele link in (geen standaard op koperpoorten).
stel onbestendig-mode *poortbereik in*	Schakel agressieve modus in (voor apparaten die deze ondersteunen).
poortadapter voor *poortonderhandelin g* instellen	Laat standaard GE autonomie van link parameters toe.
poortbereik ***instellen*** *voor* ***poortval***	Laat SNMP vallen voor deze zeer belangrijke havens toe.
zet *poortbereik* uit	Schakel deze optie uit als u geen trunks gebruikt.
Stel *romp-mod/poort in met ISL | punt 1q | onderhandelingen*	Bij gebruik van stammen heeft dot1q de voorkeur.
Vlan *bereik* van *de* stam/*poort*	Limiet STP diameter door VLAN's uit stammen te snoeien waar ze niet nodig zijn.
stel wijze van *poortbereik* in	Schakel deze optie uit als u geen kanalen gebruikt.
stel gewenste poortkanaalbereik in	Als u kanalen gebruikt, stelt dit PAgP in.
zet het kanaal van de haven alle distributie ip beide	Laat L3 bron/bestemming taakverdeling toe indien gebruik van kanalen (standaard op Catalyst 6500/6000).
zetten *mod/poort op ISL voor* niet-onderhandeling *| punt 1q*	Uitschakelen DTP bij trunking naar router, Catalyst 2900XL, 3500 of een andere verkoper.
Mod */poort* voor *poortonderhandelin g instellen*	De onderhandelingen kunnen niet compatibel zijn voor een aantal oude GE-apparaten.

Gerelateerde informatie

- Common CatOS-foutmeldingen op Catalyst 4500/4000 Series Switches
- Common CatOS-foutmeldingen op Catalyst 5000/5500 Series Switches
- Common CatOS-foutmeldingen op Catalyst 6500/6000 Series Switches
- Productondersteuning voor switches

- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning en documentatie – Cisco Systems