Herstel de uitgeschakelde poortstatus op Cisco IOS-platforms

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Platforms die gebruikmaken van erreless
Uitschakelen
Functie van Erreless
Oorzaken van storingen
Bepaal of poorten ongeschikt zijn
Bepaal de reden voor de foutloze staat (consoleberichten, syslog en de show erreless herstel commando)
Een poort herstellen van een foutieve staat
Het hoofdprobleem corrigeren
De uitgeschakelde poorten opnieuw inschakelen
Verifiëren
Problemen oplossen
Gerelateerde informatie

Inleiding

Dit document beschrijft de toestand van uitgeschakelde bestanden, hoe u ervan kunt herstellen en geeft voorbeelden van uitgeschakelde herstel. In dit document worden de termen erreless en error deblokkeerbaar door elkaar gebruikt. Klanten nemen vaak contact op met Cisco Technical Support wanneer ze merken dat een of meer van hun switch poorten foutloos zijn geworden, wat betekent dat de poorten een status van heruitgeschakeld hebben. Deze klanten willen weten waarom de fout disablement gebeurd is en hoe ze de poorten weer normaal kunnen maken.

> **Opmerking:** De poortstatus van `per ongeluk uitgeschakeld` displays in de uitvoer van de **opdracht status interface_number van de show**.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Om de voorbeelden in dit document te maken, hebt u twee Cisco Catalyst 4500/6500 Series Switches (of het equivalent) nodig in een laboratoriumomgeving met duidelijke configuraties. De switches moeten Cisco IOS®-software uitvoeren en elke switch moet twee Fast Ethernet-poorten hebben die geschikt zijn voor EtherChannel en PortFast.

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

Achtergrondinformatie

Platforms die gebruikmaken van erreless

De erreless eigenschap wordt ondersteund op deze Catalyst switches:

- Catalyst switches waarop Cisco IOS-software wordt uitgevoerd:2900XL / 3500XL2940/2950/2960/29703550/3560/3560-E/3750/3750-E3650/38504500 / 4503 / 4506 / 4507 / 4510 / 4500-X6500/6503/6504/6506/65099200/9300/9400/9500

De manier waarop err< (Fantasie) wordt geïmplementeerd varieert per softwareplatform. Dit document richt zich specifiek op errunk voor switches die Cisco IOS-software uitvoeren.

Uitschakelen

Functie van Erreless

Als de configuratie laat zien dat een poort is ingeschakeld, maar dat de software op de switch een foutsituatie op de poort detecteert, sluit de software die poort af. Met andere woorden, de poort wordt automatisch uitgeschakeld door de software van het besturingssysteem van de switch vanwege een fout die wordt aangetroffen op de poort.

Wanneer een poort fout is uitgeschakeld, is deze effectief uitgeschakeld en wordt er geen verkeer verzonden of ontvangen op die poort. De poort LED is ingesteld op de kleur oranje en wanneer u de opdracht **show interfaces** uitgeeft, wordt de poortstatus `foutloos weergegeven`. Hier is een voorbeeld van hoe een door een fout uitgeschakeld poort eruitziet vanuit de opdrachtregelinterface (CLI) van de switch:

```
cat6knative#show interfaces gigabitethernet 4/1 status

Port    Name       Status       Vlan       Duplex  Speed Type
Gi4/1              err-disabled 100          full   1000 1000BaseSX
```

Of, als de interface wegens een foutenvoorwaarde onbruikbaar is gemaakt, kunt u berichten zien die aan deze in zowel de console als syslog gelijkaardig zijn:

```
%SPANTREE-SP-2-BLOCK_BPDUGUARD:
   Received BPDU on port GigabitEthernet4/1 with BPDU Guard enabled. Disabling port.
%PM-SP-4-ERR_DISABLE:
   bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state
```

Dit voorbeeldbericht toont wanneer een hostpoort de Bridge Protocol Data Unit (BPDU) ontvangt.

Het eigenlijke bericht hangt af van de reden voor de foutvoorwaarde.

De fout schakelt functie dient twee doeleinden:

- Het laat de beheerder weten wanneer en waar er een poortprobleem is.
- Het elimineert de mogelijkheid dat deze poort andere poorten op de module (of de gehele module) kan doen falen.Een dergelijke storing kan optreden wanneer een slechte haven buffers of poortfoutmeldingen monopoliseert met interprocess-communicatie op de kaart, wat uiteindelijk kan leiden tot ernstige netwerkproblemen. De fout schakelt functie uit helpt deze situaties te voorkomen.

Oorzaken van storingen

Deze optie is eerst geïmplementeerd om speciale botsingssituaties aan te kunnen waarin de switch te veel of te laat botsingen op een poort heeft gedetecteerd. Er treden buitensporige botsingen op wanneer een frame wordt gedropt omdat de switch 16 botsingen na elkaar tegenkomt. De late botsingen komen voor omdat elk apparaat op de draad niet herkende dat de draad in gebruik was. Mogelijke oorzaken van dit soort fouten zijn onder meer:

- Een kabel die niet aan de specificatie voldoet (te lang, het verkeerde type of defect)
- Een slechte netwerkinterfacekaart (NIC) (met fysieke problemen of driver-problemen)
- Een poortduplexfoutEen poortduplexfout is een veel voorkomende oorzaak van fouten vanwege fouten bij het onderhandelen over de snelheid en duplexfout tussen twee rechtstreeks verbonden apparaten (bijvoorbeeld een NIC die verbinding maakt met een switch). Slechts kunnen de half-duplex verbindingen botsingen in LAN ooit hebben. Wegens de meervoudige toegang van de dragerbetekenis (CSMA) is de aard van Ethernet, zijn de botsingen normaal voor de helft - duplex, zolang de botsingen geen klein percentage van verkeer overschrijden.

Er zijn verschillende redenen waarom de interface erreless moet worden. De reden kan zijn:

- Duplex-mismatch
- Misconfiguratie van poortkanaal
- BPDU-wachtwoordschending
- UniDirectional Link Detection (UDLD)-voorwaarde
- Detectie van late botsingen
- Link-flap detectie
- Beveiligingsschending
- Poortaggregatieprotocol (PAgP)-flap
- Layer 2 Tunneling Protocol (L2TP)-beveiliging
- DHCP-snoopingstarief limiet
- Onjuiste GBIC / Small Form-Factor Pluggable (SFP) module of kabel
- Adres Resolution Protocol (ARP)-inspectie
- Inline voeding

  Opmerking: Fout-uitschakelen detectie is standaard ingeschakeld om al deze redenen. Gebruik de opdracht **Geen** fout-uitschakelen **oorzaak** opsporen om de detectie door fouten uit te schakelen. De opdracht **Detectie** van **show** erreless toont de fout-uitschakelen detectiestatus.

Bepaal of poorten ongeschikt zijn

U kunt bepalen of uw poort is uitgeschakeld als u de opdracht **showinterfaces** uitgeeft.

Hier is een voorbeeld van een actieve poort:

```
cat6knative#show interfaces gigabitethernet 4/1 status
!--- Refer to show interfaces status for more information on the command. Port Name Status Vlan
Duplex Speed Type Gi4/1 Connected 100 full 1000 1000BaseSX
```

Hier is een voorbeeld van dezelfde poort in de fout uitgeschakeld staat:

```
cat6knative#show interfaces gigabitethernet 4/1 status
!--- Refer to show interfaces status for more information on the command. Port Name Status Vlan
Duplex Speed Type Gi4/1 err-disabled 100 full 1000 1000BaseSX
```

> **Opmerking:** Wanneer een poort door een fout is uitgeschakeld, wordt de LED op het voorpaneel dat aan de poort is gekoppeld, ingesteld op de kleur oranje.

Bepaal de reden voor de foutloze staat (consoleberichten, syslog en de show erreless herstel commando)

Wanneer de switch een poort in de met een fout uitgeschakeld toestand zet, verstuurt de switch een bericht naar de console waarin wordt beschreven waarom de poort is uitgeschakeld. Het voorbeeld in deze sectie verschaft twee voorbeeldberichten die de reden voor de uitschakeling van de poort weergeven:

- Eén van de problemen is vanwege de PortFast BPDU-bewaker.
- De andere onmogelijkheid is vanwege een EtherChannel-configuratieprobleem.

> **Opmerking:** U kunt deze berichten in syslog ook zien als u het bevel van het **showlogboek** uitgeeft.

Hier volgen een paar voorbeelden:

```
%SPANTREE-SP-2-BLOCK_BPDUGUARD:
   Received BPDU on port GigabitEthernet4/1 with BPDU Guard enabled. Disabling port.

%PM-SP-4-ERR_DISABLE:
   bpduguard error detected on Gi4/1, putting Gi4/1 in err-disable state

 %SPANTREE-2-CHNMISCFG: STP loop - channel 11/1-2 is disabled in vlan 1
```

Als u **erreless herstel** hebt ingeschakeld, kunt u de reden voor de erreless status bepalen als u de opdracht erreless herstel uitvaardigt. Hierna volgt een voorbeeld:

```
cat6knative#show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Enabled
bpduguard            Enabled
security-violatio    Enabled
```

```
channel-misconfig    Enabled
pagp-flap            Enabled
dtp-flap             Enabled
link-flap            Enabled
l2ptguard            Enabled
psecure-violation    Enabled
gbic-invalid         Enabled
dhcp-rate-limit      Enabled
mac-limit            Enabled
unicast-flood        Enabled
arp-inspection       Enabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
---------    ---------------------    --------------
  Fa2/4                bpduguard          273
```

Een poort herstellen van een foutieve staat

Deze sectie geeft voorbeelden van hoe u een fout-gehandicapte haven kunt ontmoeten en hoe te om het te bevestigen, evenals een korte bespreking van een paar extra redenen dat een haven fout gehandicapt kan worden. Om een poort te herstellen van de erreless status, identificeer en corrigeer eerst het wortelprobleem en schakel vervolgens de poort opnieuw in. Als u de poort opnieuw inschakelt voordat u het wortelprobleem oplost, worden de poorten gewoon weer uitgeschakeld.

Het hoofdprobleem corrigeren

Nadat u ontdekt waarom de poorten uitgeschakeld waren, los het wortelprobleem op. De oplossing hangt af van wat het probleem veroorzaakt heeft. Er zijn een heleboel dingen die de shutdown kunnen activeren. In dit gedeelte worden enkele van de meest opvallende en veel voorkomende oorzaken besproken:

- EtherChannel-misconfiguratieOm EtherChannel te laten werken, moeten de betrokken poorten consistente configuraties hebben. De poorten moeten hetzelfde VLAN, dezelfde trunkmodus, dezelfde snelheid, dezelfde duplex enzovoort hebben. De meeste configuratieverschillen binnen een switch worden opgespoord en gerapporteerd wanneer u het kanaal maakt. Als één switch voor EtherChannel is geconfigureerd en de andere switch niet voor EtherChannel is geconfigureerd, kan het overspannen-boomproces de gekanaliseerde poorten aan de kant die voor EtherChannel is geconfigureerd uitschakelen. De on-mode van EtherChannel verstuurt geen PAgP-pakketten om met de andere kant te onderhandelen voor het kanaliseren; het gaat ervan uit dat de andere kant van de zaak kanaliseert. Bovendien schakelt dit voorbeeld EtherChannel niet in voor de andere switch, maar laat deze poorten als individuele, niet gekanaliseerde poorten. Als u de andere switch ongeveer een minuut in deze staat laat, denkt Spanning Tree Protocol (STP) op de switch waar EtherChannel is ingeschakeld dat er een lus is. Dit zet de kanaliserende poorten in de uitgeschakelde toestand.In dit voorbeeld werd een lus gedetecteerd en werden de poorten uitgeschakeld. De output van de **show etherchannel** opdracht toont aan dat het `aantal kanaalgroepen in gebruik 0` is. Wanneer u naar een van de poorten kijkt die betrokken zijn, kunt u zien dat de status is `foutloos`:
  ```
  %SPANTREE-2-CHNL_MISCFG: Detected loop due to etherchannel misconfiguration of Gi4/1
  ```

```
cat6knative#show etherchannel summary
!--- Refer to show etherchannel for more information on the command. Flags: D - down P - in
port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator u - unsuitable for bundling Number of channel-
groups in use: 0 Number of aggregators: 0 Group Port-channel Protocol Ports ------+---------
----+-----------+-----------------------------------------------
```

De EtherChannel werd afgebroken omdat de poorten op deze switch onbruikbaar werden gemaakt.

```
cat6knative#show interfaces gigabitethernet 4/1 status

Port     Name               Status       Vlan       Duplex  Speed Type
Gi4/1                       err-disabled 100          full   1000 1000BaseSX
```

Bekijk de foutmelding om te kunnen bepalen wat het probleem is. Het bericht geeft aan dat EtherChannel een overspannende boomloop tegenkwam. Zoals in dit gedeelte wordt uitgelegd, kan dit probleem zich voordoen wanneer EtherChannel op één apparaat (in dit geval de switch) handmatig is ingeschakeld met behulp van de aan-modus (in tegenstelling tot de gewenste modus) en op het andere aangesloten apparaat (in dit geval de andere switch) EtherChannel helemaal niet is ingeschakeld. Eén manier om de situatie te verhelpen is door de kanaalmodus in te stellen op gewenst aan beide zijden van de verbinding en vervolgens de poorten weer in te schakelen. Elke zijde vormt een kanaal als beide partijen akkoord gaan met het kanaliseren. Als ze niet akkoord gaan met het kanaliseren, blijven beide kanten functioneren als normale havens.

```
cat6knative(config-terminal)#interface gigabitethernet 4/1
cat6knative(config-if)#channel-group 3 mode desirable non-silent
```

- Duplex-mismatchDuplex mismatches komen vaak voor omdat u niet op de juiste manier over snelheid en duplex kunt onderhandelen. In tegenstelling tot een half duplex apparaat, dat moet wachten tot er geen andere apparaten zijn die op hetzelfde LAN segment verzenden, verzendt een full-duplex apparaat wanneer het apparaat iets te verzenden heeft, ongeacht andere apparaten. Als deze transmissie optreedt terwijl het half-duplex apparaat overbrengt, beschouwt het half-duplex apparaat dit als een botsing (tijdens de slottijd) of een late botsing (na de slottijd). Omdat de full-duplex kant nooit botsingen verwacht, realiseert deze kant zich nooit dat het dat gelaten vallen pakket moet opnieuw overbrengen. Een laag percentage botsingen is normaal met de helft van duplex, maar is niet normaal met volledig duplex. Een switch poort die veel recente botsingen ontvangt, geeft meestal een duplex mismatch probleem aan. Zorg ervoor dat de poorten aan beide zijden van de kabel op dezelfde snelheid en duplex zijn ingesteld. De **show interfaces interface_number** opdracht vertelt u de snelheid en duplex voor Catalyst switch poorten. Latere versies van Cisco Discovery Protocol (CDP) kunnen u waarschuwen voor een duplexfout voordat de poort in de met een fout uitgeschakeld toestand wordt gezet.Daarnaast zijn er instellingen op een NIC, zoals autopolariteit functies, die het probleem kunnen veroorzaken. Als u niet zeker weet, schakelt u deze instellingen uit. Als u meerdere NIC's van een leverancier hebt en de NIC's allemaal hetzelfde probleem lijken te hebben, controleer dan de website van de fabrikant voor de release notities en zorg ervoor dat u de nieuwste drivers hebt.Andere oorzaken van recente botsingen omvatten:Een slechte NIC (met fysieke problemen, niet alleen configuratieproblemen)Een slechte kabelEen kabelsegment dat te lang is
- BPDU-poortwachtEen poort die gebruik maakt van PortFast moet alleen verbinding maken met een eindstation (zoals een werkstation of server) en niet met apparaten die overspannende BPDU's genereren, zoals switches of bruggen en routers die overbruggen. Als de switch een overspannende boom BPDU op een poort ontvangt die het overspannen -

boom PortFast en het overspannen - BPDU bewaker toegelaten heeft, zet de switch de poort op erabled wijze om tegen potentiële lijnen te beschermen. PortFast veronderstelt dat een poort op een switch geen fysieke lus kan genereren. Daarom slaat PortFast de eerste overspanningscontrole voor die poort over, waardoor de time-out van eindstations bij bootup wordt vermeden. De netwerkbeheerder moet PortFast zorgvuldig implementeren. Op poorten waarop PortFast is ingeschakeld, helpt de BPDU-bewaker ervoor te zorgen dat het LAN zonder lijnen blijft.Dit voorbeeld laat zien hoe u deze functie kunt inschakelen. Dit voorbeeld is gekozen omdat het maken van een fout-uitschakelsituatie in dit geval eenvoudig is:

```
cat6knative(config-if)#spanning-tree bpduguard enable
!--- Refer to spanning-tree bpduguard for more information on the command.
```

In dit voorbeeld is een Catalyst 6509-switch aangesloten op een andere switch (een 6509). De 6500 verstuurt elke 2 seconden BPDU's (bij gebruik van de standaard overspannen - drie instellingen). Wanneer u PortFast inschakelt op de 6509 switch poort, de BPDU bewaker kijkt naar BPDU's die op deze poort binnenkomen. Wanneer een BPDU in de poort komt, wat betekent dat een apparaat dat geen eindapparaat is op die poort wordt gedetecteerd, schakelt de BPDU-beveiligingsfunctiefout de poort uit om de mogelijkheid van een overspannende boomlus te voorkomen.

```
cat6knative(config-if)#spanning-tree portfast enable
!--- Refer to spanning-tree portfast (interface configuration mode) !--- for more
information on the command. Warning: Spantree port fast start can only be enabled on ports
connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a
fast start port can cause temporary spanning tree loops. %PM-SP-4-ERR_DISABLE: bpduguard
error detected on Gi4/1, putting Gi4/1 in err-disable state.
```

In dit bericht geeft de switch aan dat hij een BPDU heeft ontvangen op een PortFast-enabled poort en dat de switch dus poort Gi4/1 uitschakelt.

```
cat6knative#show interfaces gigabitethernet 4/1 status

Port     Name               Status       Vlan       Duplex  Speed Type
Gi4/1                       err-disabled 100          full   1000 1000BaseSX
```

U moet de PortFast-functie uitschakelen omdat deze poort een poort is met een onjuiste verbinding. De verbinding is niet correct omdat PortFast is ingeschakeld en de switch verbinding maakt met een andere switch. Vergeet niet dat PortFast alleen bedoeld is voor gebruik op poorten die verbinding maken met eindstations.

```
cat6knative(config-if)#spanning-tree portfast disable
```

- UDLDHet UDLD-protocol maakt het mogelijk dat apparaten die zijn aangesloten via glasvezel- of koper-Ethernet-kabels (bijvoorbeeld categorie 5-bekabeling) de fysieke configuratie van de kabels bewaken en detecteren wanneer er een unidirectionele link bestaat. Wanneer een unidirectionele link wordt gedetecteerd, sluit UDLD de betreffende poort af en waarschuwt de gebruiker. Unidirectionele verbindingen kunnen een verscheidenheid van problemen veroorzaken, die over - boomtopologielijnen omvatten.**Opmerking:** UDLD ruilt protocolpakketten tussen de naburige apparaten. Beide apparaten op de link moeten UDLD ondersteunen en UDLD ingeschakeld hebben op de betreffende poorten. Als u UDLD hebt ingeschakeld op slechts één poort van een link, kan het ook het einde dat met UDLD is geconfigureerd verlaten om naar erreless status te gaan.Elke poortpoort die is geconfigureerd voor UDLD verstuurt UDLD-protocolpakketten die het poortapparaat (of poortid) en het buurapparaat (of poortid's) bevatten die door UDLD op die switch worden gezien. De aangrenzende poorten moeten hun eigen apparaat of poort-ID (echo) zien in de pakketten die van de andere kant worden ontvangen. Als de poort zijn eigen apparaat of poort-ID voor een bepaalde tijdsduur niet in de inkomende UDLD-pakketten ziet, wordt de koppeling als unidirectioneel beschouwd. Daarom is de respectieve poort uitgeschakeld en wordt een

bericht dat hierop lijkt op de console afgedrukt:
`PM-SP-4-ERR_DISABLE: udld error detected on Gi4/1, putting Gi4/1 in err-disable state.`
Raadpleeg het document UniDirectional Link Detection (UDLD) configureren voor meer informatie over de bediening, configuratie en opdrachten van UDLD.

- Link-flap foutLink flap betekent dat de interface voortdurend op en neer gaat. De interface wordt in de uitgeschakelde toestand gezet als deze meer dan vijf keer wordt gespiegeld in 10 seconden. De veel voorkomende oorzaak van linkflap is een Layer 1-kwestie zoals een slechte kabel, duplexfout of slechte Gigabit Interface Converter (GBIC)-kaart. Bekijk de consoleberichten of de berichten die naar de syslogserver werden verzonden die de reden voor de havensluiting verklaren.
  `%PM-4-ERR_DISABLE: link-flap error detected on Gi4/1, putting Gi4/1 in err-disable state`
  Geef deze opdracht uit om de flap-waarden weer te geven:
  ```
  cat6knative#show errdisable flap-values
  !--- Refer to show errdisable flap-values for more information on the command. ErrDisable
  Reason Flaps Time (sec) ----------------- ------ ---------- pagp-flap 3 30 dtp-flap 3 30
  link-flap 5 10
  ```
- TerugloopfoutEen loopback fout komt voor wanneer het keepalive pakket terug naar de haven wordt van een lus voorzien die keepalive verzond. De switch verstuurt standaard keepalives alle interfaces. Een apparaat kan de pakketten terug naar de broninterface van een lus voorzien, die gewoonlijk voorkomt omdat er een logische lijn in het netwerk is dat het overspannen - boom niet heeft geblokkeerd. De broninterface ontvangt het keepalive pakket dat het uitzond, en de switch schakelt de interface (errenable) onbruikbaar. Dit bericht wordt weergegeven omdat het keepalive-pakket is teruggekoppeld naar de poort die het keepalive-pakket heeft verzonden:
  `%PM-4-ERR_DISABLE: loopback error detected on Gi4/1, putting Gi4/1 in err-disable state`
  Keepalives worden standaard op alle interfaces verzonden in op Cisco IOS-softwarerelease 12.1EA gebaseerde software. In op Cisco IOS-softwarerelease 12.2SE gebaseerde software en hoger worden keepalives niet standaard verzonden op glasvezel- en uplinkinterfaces. Raadpleeg voor meer informatie Cisco bug-id CSC46385 (alleen geregistreerde klanten).De voorgestelde tijdelijke oplossing is om keepalives uit te schakelen en te upgraden naar Cisco IOS-softwarerelease 12.2SE of hoger.
- Schending van poortbeveiligingU kunt poortbeveiliging gebruiken met dynamisch aangeleerde en statische MAC-adressen om het toegangsverkeer van een poort te beperken. Om het verkeer te beperken, kunt u de MAC-adressen beperken die verkeer naar de poort mogen verzenden. Om de switch poort te configureren om de fout uit te schakelen als er een beveiligingsovertreding is, geeft u deze opdracht uit:
  ```
  cat6knative(config-if)#switchport port-security violation shutdown
  ```

  Een veiligheidsschending komt in één van beiden van deze twee situaties voor:Wanneer het maximale aantal beveiligde MAC-adressen op een beveiligde poort wordt bereikt en het MAC-adres van de bron van het toegangsverkeer verschilt van de geïdentificeerde beveiligde MAC-adressenIn dit geval past poortbeveiliging de geconfigureerde overschrijdingsmodus toe.Als verkeer met een beveiligd MAC-adres dat is geconfigureerd of geleerd op één beveiligde poort probeert toegang te krijgen tot een andere beveiligde poort in hetzelfde VLANIn dit geval past de poortbeveiliging de sluitingsschendingsmodus toe.
- L2PT-beveiligingWanneer Layer 2 PDU's de switch of toegangspoort op de inkomende edge-adapter ingaan, overschrijft de switch het MAC-adres van de PDU-bestemming van de klant met een bekend Cisco-bedrijfseigen multicast-adres (10-00-0c-cd-cd-d0). Als 802.1Q-tunneling is ingeschakeld, worden pakketten ook dubbelgelabeld. De buitenste tag is de klant metrotag en de binnentag is de klant VLAN tag. De core switches negeren de innerlijke tags

en sturen het pakket door naar alle trunkpoorten in dezelfde metro VLAN. De switches aan de uitgaande kant herstellen de juiste Layer 2-protocol en MAC-adresinformatie en sturen de pakketten door naar alle tunnelpoorten of toegangspoorten in dezelfde metro VLAN. Daarom wordt Layer 2 PDU's intact gehouden en over de service-provider-infrastructuur aan de andere kant van het klantnetwerk geleverd.

```
Switch(config)#interface gigabitethernet 0/7
l2protocol-tunnel {cdp | vtp | stp}
```

De interface gaat naar een uitgeschakelde toestand. Als een ingekapselde PDU (met het bedrijfseigen MAC-adres van de bestemming) wordt ontvangen van een tunnelpoort of toegangspoort met Layer 2-tunneling ingeschakeld, wordt de tunnelpoort afgesloten om lijnen te voorkomen. De poort wordt ook uitgeschakeld wanneer een geconfigureerde afsluitdrempel voor het protocol wordt bereikt. U kunt de poort handmatig opnieuw inschakelen (geef een **afsluiten uit**, **geen shutdown** commando sequentie) of als erreless herstel is ingeschakeld, wordt de operatie opnieuw geprobeerd na een gespecificeerd tijdsinterval.Om de interface van erreless staat terug te krijgen, schakel de poort opnieuw in met de opdracht **erreless herstel oorzaak l2ptguard**. Deze opdracht wordt gebruikt om het herstelmechanisme te configureren van een Layer 2-fout in maximumsnelheden, zodat de interface uit de uitgeschakelde toestand kan worden gehaald en opnieuw kan proberen. U kunt ook het tijdsinterval instellen. Schakel herstel standaard uit. als deze optie is ingeschakeld, is het standaardtijdsinterval 300 seconden.

- Onjuiste SFP-kabelPoorten gaan naar erreless status met de foutmelding `%PHY-4-SFP_NOT_SUPPORT` als u Catalyst 3560 en Catalyst 3750 Switches aansluit en een SFP Interconnect-kabel gebruikt.De Cisco Catalyst 3560 SFP interconnect-kabel (CAB-SFP-50CM=) biedt een goedkope point-to-point Gigabit Ethernet-verbinding tussen Catalyst 3560 Series Switches. De 50 centimeter (cm) kabel is een alternatief voor de SFP-transceivers om Catalyst 3560 Series Switches via hun SFP-poorten op korte afstand onderling te verbinden. Alle Cisco Catalyst 3560 Series Switches ondersteunen de SFP Interconnect-kabel.Wanneer een Catalyst 3560-Switch is aangesloten op een Catalyst 3750 of een ander type Catalyst-kabelmodel, kunt u de CAB-SFP-50CM= switch **niet** gebruiken. U kunt beide switches op beide apparaten aansluiten met een koperkabel met SFP (GLC-T) in plaats van een CAB-SFP-50CM=.
- 802.1X security overtreding

```
DOT1X-SP-5-SECURITY_VIOLATION: Security violation on interface GigabitEthernet4/8,
New MAC address 0080.ad00.c2e4 is seen on the interface in Single host mode
%PM-SP-4-ERR_DISABLE: security-violation error detected on Gi4/8, putting Gi4/8 in err-
disable state
```

Dit bericht geeft aan dat de poort op de gespecificeerde interface in de single-host modus is geconfigureerd. Om het even welke nieuwe gastheer die op de interface wordt ontdekt wordt behandeld als veiligheidsschending. De poort is door een fout uitgeschakeld.Zorg ervoor dat slechts één host is aangesloten op de poort. Als u verbinding moet maken met een IP-telefoon en een host erachter, configureer dan de Multidomain Authenticatiemodus op die switchpoort.In de MDA-modus (Multidomain Authentication) kunnen een IP-telefoon en één host achter de IP-telefoon onafhankelijk verifiëren, met 802.1X, MAC-verificatie-omzeiling (MAB) of (alleen voor de host) webgebaseerde verificatie. In deze toepassing verwijst Multidomain naar twee domeinen — gegevens en spraak — en slechts twee MAC-adressen zijn toegestaan per poort. De switch kan de host in de gegevens VLAN en de IP-telefoon in de spraak VLAN plaatsen, hoewel ze op dezelfde switch poort lijken te staan. De gegevens VLAN-toewijzing kan worden verkregen uit de leverancierspecifieke kenmerken (VSA's) die

van de AAA-server binnen de verificatie worden ontvangen.Raadpleeg voor meer informatie het gedeelte Multidomain Verification Mode van het gedeelte 802.1X-poortgebaseerde verificatie.

De uitgeschakelde poorten opnieuw inschakelen

Nadat u het wortelprobleem hebt opgelost, worden de poorten nog steeds uitgeschakeld als u niet hebt ingesteld voor herstel van de switch. In dat geval moet u de poorten handmatig opnieuw inschakelen. Geef het **shutdown** commando en vervolgens de **no shutdown** interface mode commando uit op de gekoppelde interface om de poorten handmatig opnieuw in te schakelen.

Met de opdracht **Herstel uitschakelen** kunt u het type fouten kiezen dat de poorten na een bepaalde tijd automatisch opnieuw inschakelt. De opdracht **Herstel uitschakelen** toont de standaard fout-uitschakelen herstelstatus voor alle mogelijke omstandigheden.

```
cat6knative#show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
mac-limit            Disabled
unicast-flood        Disabled
arp-inspection       Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
```

> **Opmerking:** Het standaard timeout interval is 300 seconden en standaard wordt de timeout feature uitgeschakeld.

Om **erreless herstel** in te schakelen en de erreless voorwaarden te kiezen, geef deze opdracht:

```
cat6knative#errdisable recovery cause ?
  all                 Enable timer to recover from all causes
  arp-inspection      Enable timer to recover from arp inspection error disable
                      state
  bpduguard           Enable timer to recover from BPDU Guard error disable
                      state
  channel-misconfig   Enable timer to recover from channel misconfig disable
                      state
  dhcp-rate-limit     Enable timer to recover from dhcp-rate-limit error
                      disable state
  dtp-flap            Enable timer to recover from dtp-flap error disable state
  gbic-invalid        Enable timer to recover from invalid GBIC error disable
                      state
  l2ptguard           Enable timer to recover from l2protocol-tunnel error
```

```
                    disable state
  link-flap         Enable timer to recover from link-flap error disable
                    state
  mac-limit         Enable timer to recover from mac limit disable state
  pagp-flap         Enable timer to recover from pagp-flap error disable
                    state
  psecure-violation Enable timer to recover from psecure violation disable
                    state
  security-violation Enable timer to recover from 802.1x violation disable
                    state
  udld              Enable timer to recover from udld error disable state
  unicast-flood     Enable timer to recover from unicast flood disable state
```

Dit voorbeeld laat zien hoe de BPDU-bewaker de herstelvoorwaarde uitschakelt:

```
cat6knative(Config)#errdisable recovery cause bpduguard
```

Een mooie eigenschap van deze opdracht is dat, als u erreless herstel inschakelt, de opdracht algemene redenen opsomt dat de poorten in de fout-uitschakelen status zijn gezet. In dit voorbeeld, merk op dat de BPDU bewaker functie de reden voor de sluiting van haven 2/4 was:

```
cat6knative#show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Enabled
security-violatio    Disabled
channel-misconfig    Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
mac-limit            Disabled
unicast-flood        Disabled
arp-inspection       Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

Interface      Errdisable reason      Time left(sec)
---------    ---------------------    --------------
  Fa2/4               bpduguard          290
```

Als een van de erreless herstelvoorwaarden is ingeschakeld, worden de poorten met deze voorwaarde na 300 seconden opnieuw ingeschakeld. U kunt deze standaardinstelling van 300 seconden ook wijzigen als u deze opdracht geeft:

```
cat6knative(Config)#errdisable recovery interval timer_interval_in_seconds
```

In dit voorbeeld wordt het herstelinterval voor erreless gewijzigd van 300 tot 400 seconden:

```
cat6knative(Config)#errdisable recovery interval 400
```

Verifiëren

- **toon versie**-Toont de versie van de software die op de switch wordt gebruikt.
- **toon interfaces interface_number status**-toont de huidige status van de switch poort.
- **toon erreless ontdekken**-Toont de huidige instellingen van de erreless onderbrekingseigenschap en, als om het even welke havens momenteel gehandicapt fout zijn, de reden dat zij gehandicapt fout zijn.

Problemen oplossen

- **toon interfacestatus err-gehandicapt**-toont welke lokale havens bij de errdeabled staat betrokken zijn.
- **toon etherchannel samenvatting**-toont de huidige status van EtherChannel.
- **toon erreless herstel**-toont de tijdspanne waarna de interfaces voor erreless voorwaarden worden toegelaten.
- **toon erreless ontdekken**-toont de reden voor erreless status.

Zie Switch- en interfaceproblemen met probleemoplossing voor meer informatie over het oplossen van switchpoortproblemen.

Gerelateerde informatie

- *De interface bevindt zich in de uitgeschakelde status* Hardware voor probleemoplossing en gebruikelijke problemen met Catalyst 6500/6000 Series Switches waarop Cisco IOS-systeemsoftware wordt uitgevoerd
- Verbetering van Spanning Tree PortFast BPDU Guard
- Inzicht in EtherChannel-inconsistentiedetectie
- Problemen met switchpoorten en interfaces troubleshooten
- LAN-productondersteuning
- Ondersteuning voor LAN-switching technologie
- Technische ondersteuning – Cisco Systems

Over deze vertaling

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