STP voor probleemoplossing bij Catalyst-Switches die Cisco IOS-systeemsoftware uitvoeren

Inhoud

Inleiding

Dit document bevat richtlijnen om Cisco IOS®-software te gebruiken om problemen met uw probleemoplossing op te lossen met Spanning-Tree Protocol (STP). Er zijn specifieke opdrachten die alleen van toepassing zijn op Catalyst 6500/6000; U kunt echter de meeste beginselen op elke Cisco Catalyst-switch toepassen die Cisco IOS-software draait.

De meeste problemen bij STP-probleemoplossing draaien rond drie problemen:

- uitgangen
- buitensporige overstromingen door een hoog percentage STP-topologische veranderingen (TC)
- kwesties in verband met de convergentietijd

Omdat het overbruggen geen mechanisme heeft om te volgen of een bepaald pakket meerdere malen wordt doorgestuurd (bijvoorbeeld, wordt een IP Tijd om te leven [TTL] gebruikt om verkeer weg te wijzen dat te lang in het netwerk circuleert) kan slechts één pad tussen twee apparaten in hetzelfde Layer 2 (L2) domein bestaan.

Het doel van STP is overtollige havens op basis van een STP algoritme te blokkeren, om overtollige fysieke topologie in een boom-achtige topologie op te lossen. Een het verzenden loop (zoals een STP lijn) komt voor wanneer geen haven in een overtollige topologie wordt geblokkeerd, en het verkeer in cirkels voor onbepaalde tijd wordt doorgestuurd.

Zodra de expediteits lijn begint, zal het waarschijnlijk de laagst-bandbreedte links langs zijn pad samenvatten—als alle links van dezelfde bandbreedte zijn, zullen alle links waarschijnlijk verstopt zijn. Deze congestie veroorzaakt pakketverlies en leidt tot een netwerk down situatie in het getroffen L2-domein.

Bij een overmatige overstroming zijn de symptomen mogelijk niet zo duidelijk. Sommige trage links kunnen door overstroomd verkeer overspoeld raken, en apparaten of gebruikers achter deze verstopte links kunnen een traagheid of een volledig verlies van connectiviteit ervaren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Diverse Spanning Tree types en hoe u deze kunt configureren. Zie STP- en IEEE 802.1s MST configureren voor meer informatie.
- Diverse Spanning Tree eigenschappen en de manier waarop u deze kunt configureren. Zie STP-functies configureren voor meer informatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 6500 met supervisor 2-motor
- Cisco IOS-softwarerelease 12.1(13)E

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 de potentiële impact van elke opdracht begrijpen.

Conventies

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

Waarom STP-fouten

STP maakt bepaalde aannames over zijn operationele omgeving. Dit zijn de aannames die het meest relevant zijn voor dit document:

- Elke koppeling tussen de twee bruggen is tweerichtings. Dit betekent dat, als A rechtstreeks verbinding maakt met B, A zal ontvangen wat B heeft verzonden en B zal ontvangen wat A heeft verstuurd, zolang de verbinding tussen hen is.
- Elke brug die STP in werking stelt kan de Eenheden van de Gegevens van het Protocol van STP van de Bridge (BPDU's), ook bekend als pakketten, regelmatig ontvangen, verwerken en verzenden.

Hoewel deze aannames logisch en duidelijk lijken, zijn er situaties waarin niet aan deze aannames

wordt voldaan. De meeste van deze situaties hebben betrekking op een of ander soort hardwareprobleem; softwaredefecten kunnen echter ook tot STP-storingen leiden. Verschillende hardwarefouten, foutieve configuraties of foutieve insluiting veroorzaken de meerderheid van STP-fouten, terwijl softwarefouten verantwoordelijk zijn voor de minderheid. STP-storingen kunnen ook optreden door onnodige extra verbindingen tussen de switches. VLAN's gaan door deze extra verbindingen naar een lagere status. Om dit probleem op te lossen, verwijdert u alle ongewenste verbindingen tussen de switches.

Wanneer niet aan een van deze aannames wordt voldaan, kunnen één of meer bruggen de BPDU's niet langer ontvangen of verwerken. Dit betekent dat de brug (of de bruggen) niet de netwerktopologie zal kunnen ontdekken. Zonder kennis van de juiste topologie kan de switch de lussen niet blokkeren. Om deze reden zal het overstroomde verkeer over de gecodeerde topologie circuleren, alle bandbreedte consumeren en het netwerk omlaag brengen.

Voorbeelden van waarom de switches geen BPDU's kunnen ontvangen zijn slechte transceivers of Gigabit-interfaceconverters (GBIC's), bekabelde problemen of hardwarefouten op de poort, de linecard of de Supervisor Engine. Een regelmatige reden voor STP-mislukkingen is een unidirectionele koppeling tussen de bruggen. In zo'n situatie stuurt één brug BPDU's, maar de stroomafwaartse brug ontvangt ze nooit. De STP-verwerking kan ook worden verstoord door een overbelaste CPU (99% of meer), omdat de switch geen BPDU's kan verwerken. BPDU's kunnen langs het pad van de ene brug naar de andere gecorrumpeerd worden, wat ook geschikt STP gedrag voorkomt.

Afgezien van de overslaglijnen, wanneer geen havens worden geblokkeerd, zijn er situaties wanneer slechts bepaalde pakketten onjuist door de blokkerende havens worden doorgestuurd. In de meeste gevallen wordt dit veroorzaakt door problemen met de software. Zulk gedrag kan 'langzaam lopen' veroorzaken. Dit betekent dat sommige pakketten van een netwerk zijn voorzien, maar het grootste gedeelte van het verkeer stroomt nog door het netwerk, omdat de links waarschijnlijk niet verstopt zijn.

De resterende secties in dit document bieden richtlijnen om problemen met de meest gebruikelijke STP-gerelateerde problemen op te lossen.

Doorvoerlijnen voor probleemoplossing

Het doorsturen van netwerken varieert enorm zowel in hun oorsprong (oorzaak) als in hun effect. Vanwege de grote verscheidenheid aan problemen die STP kunnen beïnvloeden, kan dit document alleen algemene richtlijnen bieden over hoe u problemen kunt oplossen bij het doorsturen van netwerken.

Voordat u een probleemoplossing start, moet u deze informatie verkrijgen:

- Een werkelijk topologisch diagram dat alle switches en bruggen gedetailleerd aangeeft
- Hun corresponderende (koppelende) poortnummers
- Configuratie-details STP, zoals welke switch de wortel en de reservewortel is, die de verbindingen een niet standaardkosten of prioriteit hebben, en de plaats van het blokkeren van havens

Over het algemeen houdt het oplossen van problemen deze stappen in (afhankelijk van de situatie zijn bepaalde stappen mogelijk niet nodig):

1. Identificeer de lus.Wanneer een geleidingslus in het netwerk ontwikkeld is, zijn dit de

gebruikelijke symptomen:Verlies van connectiviteit naar, van, en door getroffen netwerkgebiedenGebruik van hoge CPU's op routers die zijn aangesloten op getroffen segmenten of VLAN's die kunnen leiden tot verschillende symptomen, zoals routing protocol buurflapper of Hot Standby Router Protocol (HSRP) die actief kunnen flappenHoog link gebruik (vaak 100%)Hoge switch backplane gebruik (vergeleken met uitgangsgebruik)Syslogberichten die pakketlijnen in het netwerk aangeven (bijvoorbeeld HSRP dubbele IP-adresberichten)Syslogberichten die wijzen op constant adres dat relevant is of MAC-adres dat flapping-berichten aangeeftEen steeds groter aantal uitvoerdruppels op veel interfacesOpmerking: Een van deze redenen alleen kan verschillende problemen aangeven (of helemaal geen probleem). Wanneer veel van deze tegelijk worden waargenomen, is het echter zeer waarschijnlijk dat een doorvoerlijn in het netwerk is ontwikkeld.Opmerking: De snelste manier om dit te verifiëren is door gebruik van de switch backplane te controleren:

```
cat# show catalyst6000 traffic-meter

  traffic meter =   13%  Never cleared
          peak =   14%  reached at 12:08:57 CET Fri Oct 4 2002
```

Opmerking: Catalyst 4000 met Cisco IOS-software ondersteunt deze opdracht momenteel niet.Indien het huidige verkeersniveau ver boven het normale niveau ligt of indien het basisniveau niet bekend is, controleert u of het piekniveau recentelijk is bereikt en of het dicht bij het huidige verkeersniveau ligt. Bijvoorbeeld, als het piekverkeersniveau 15% is en het slechts twee minuten geleden werd bereikt en het huidige verkeersniveau 14% is, dan zou dat betekenen dat de switch werkt onder een ongewoon hoge belasting.Als de verkeersbelasting op een normaal niveau ligt, betekent dat waarschijnlijk dat er geen lus is of dat dit apparaat niet betrokken is bij de lus. Het kan echter nog steeds in een traag netwerk worden betrokken.

2. Ontdek de topologie (werkingssfeer) van de lus.Zodra is vastgesteld dat de reden voor de netwerkuitval een door-loop is, is de hoogste prioriteit de lijn te stoppen en de netwerkwerking te herstellen. Om de loop te stoppen moet u weten welke poorten bij de loop betrokken zijn: Bekijk de poorten met het hoogste verbindingsgebruik (pakketten per seconde). De opdracht interface Cisco IOS-software toont het gebruik voor elke interface.U kunt Cisco IOS-software gebruiken voor reguliere expressie en filtering van de uitvoer om alleen de gebruikersinformatie en de interfacenaam weer te geven (voor een snelle analyse). De show-interface uitgeven | Lijn|Vsec opdracht opnemen om alleen het pakket per seconde statistieken en de interfacenaam weer te geven:

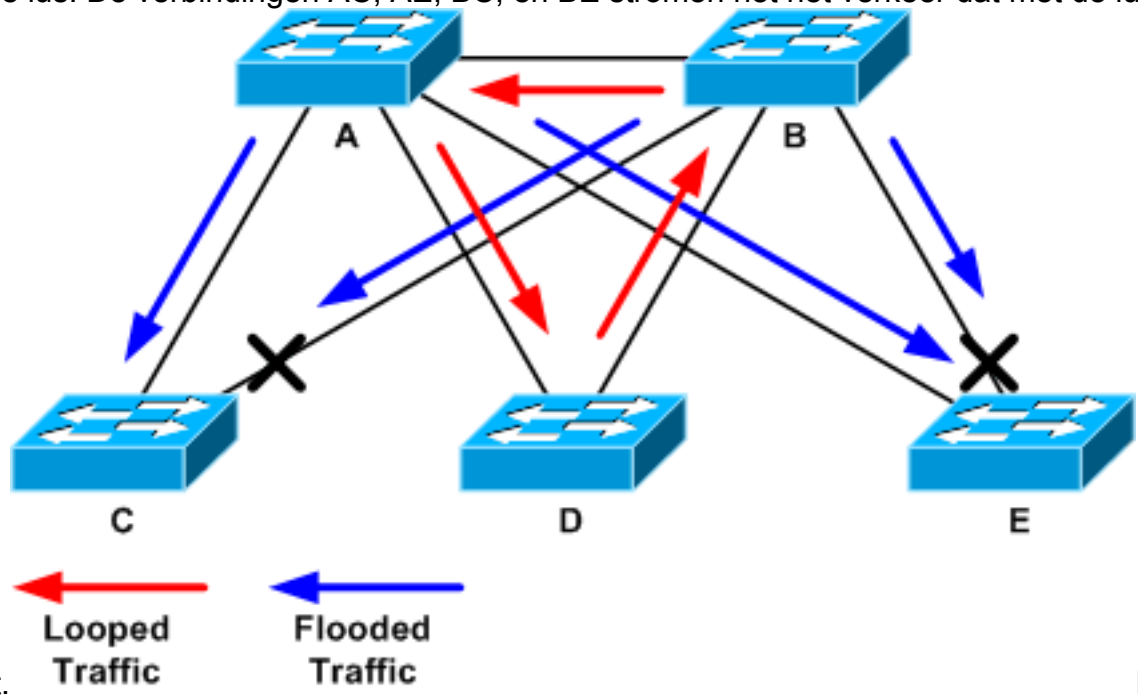
```
cat# show interface | include line|\/sec

GigabitEthernet2/1 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/2 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/3 is up, line protocol is up
  5 minute input rate 99765230 bits/sec, 24912 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/4 is up, line protocol is up
  5 minute input rate 1000 bits/sec, 27 packets/sec
  5 minute output rate 101002134 bits/sec, 25043 packets/sec
GigabitEthernet2/5 is administratively down, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/6 is administratively down, line protocol is down
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/7 is up, line protocol is down
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
GigabitEthernet2/8 is up, line protocol is up
  5 minute input rate 2000 bits/sec, 41 packets/sec
  5 minute output rate 99552940 bits/sec, 24892 packets/sec
```

Let vooral op de interfaces met het hoogste gebruik van de link. In dit voorbeeld zijn dit interfaces g2/3, g2/4 en g2/8; het zijn waarschijnlijk de havens die bij de lus betrokken zijn .

3. Breek de lus.Om de lus te breken, moet u de betrokken poorten afsluiten of afsluiten. Het is heel belangrijk om niet alleen de loop te stoppen maar ook de diepere oorzaak van de lus te vinden en te repareren. Het is relatief makkelijker om de lus te breken.**Opmerking:** om de volgende oorzaak analyse te vergemakkelijken, hoeft u niet alle poorten tegelijk te sluiten of los te koppelen van de elektriciteit; maar één voor één afgesloten . Het is over het algemeen beter om havens op het aggregatiepunt dat door de lus wordt getroffen, zoals een distributie of een switch van de kern, af te sluiten. Als u alle poorten tegelijk sluit en ze een voor een opnieuw aansluiten, werkt dit misschien niet; de lus wordt gestopt en kan niet onmiddellijk na het opnieuw aansluiten van de aangetaste haven starten . Het zou dan ook moeilijk zijn om het uitvallen van een bepaalde haven te correleren.**Opmerking:** aanbevolen wordt om informatie te verzamelen voordat u de switches opnieuw start om de lus te breken. Anders zal de daaropvolgende analyse van de grondoorzaak zeer moeilijk zijn.Nadat u elke poort uitschakelt of koppelt, moet u controleren of het backplane van de switch weer op een normaal niveau staat.**Opmerking:** Houd in gedachten dat, meestal, sommige poorten de lus niet onderhouden maar, eerder, het verkeer overspoelen dat aankomt met de loop. Wanneer u dergelijke overstroompoorten sluit, beperkt u slechts een kleine hoeveelheid backplane gebruik, maar u stopt de lus niet.In de volgende voorbeeldtopologie, is de lus tussen switches A, B, en D. Daarom linkt AB, AD, en BD aan. Als u een van deze koppelingen sluit, stopt u de lus. De verbindingen AC, AE, BC, en BE stromen net het verkeer dat met de lus



aankomt. Nad at de duurzame poort is afgesloten, zal de backplane kloksnelheid dalen naar een normale waarde. Het is van groot belang op te merken welke door de sluiting van de haven het gebruik van de backplane (en het gebruik van andere havens) op een normaal niveau werd

gebracht.Op dit punt wordt de lus gestopt en moet de netwerkwerking verbeteren; omdat de oorspronkelijke oorzaak van de loop waarschijnlijk niet was vastgesteld , zouden er echter nog enkele onopgeloste kwesties zijn .

4. Vind en bevestig de oorzaak van de lus.Zodra de loop is gestopt, moet je bepalen waarom de loop begon. Dit is vaak het moeilijkste onderdeel van het proces, omdat de redenen kunnen variëren. Het is ook moeilijk een exacte procedure te formaliseren die in elk geval werkt. Dit zijn echter enkele algemene richtsnoeren:Onderzoek het topologieschema, om een overtollig pad te vinden. Dit omvat de ondersteunende poort die in de vorige stap is gevonden en die naar dezelfde switch terugkomt (de padpakketten werden tijdens de loop uitgevoerd). In de vorige voorbeeldtopologie is dit pad AD-DB-BA.Controleer voor elke switch op het redundante pad op deze problemen:Weet de switch de juiste STP wortel?Alle switches in een L2 netwerk zouden het eens moeten worden over een gemeenschappelijke STP wortel. Het is een duidelijk symptoom van problemen wanneer bruggen constant een verschillende ID voor de STP wortel in een bepaald VLAN of STP instantie tonen. Geef de **opdracht** van de **show in** het **vlan VLAN *vlan-id uit* om de root-brug-ID voor een bepaald VLAN weer te geven:**

```
cat# show spanning-tree vlan 333

MST03
  Spanning tree enabled protocol mstp
  Root ID     Priority    32771
              Address     0050.14bb.6000
              Cost        20000
              Port        136 (GigabitEthernet3/8)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32771  (priority 32768 sys-id-ext 3)
              Address     00d0.003f.8800
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- ------------------------
Gi3/8            Root FWD 20000     128.136  P2p
Po1              Desg FWD 20000     128.833  P2p
```

Het VLAN-nummer kan vanuit de poort worden gevonden, omdat poorten die bij de lus betrokken zijn, in eerdere stappen zijn gezet. Als de havens in kwestie stammen zijn, vaak zijn alle VLANs op de boomstam betrokken. Als dit niet het geval is (bijvoorbeeld, als het lijkt dat de loop op één VLAN heeft plaatsgevonden) kunt u proberen om de **showinterfaces** uit te geven **| omvat L2|line|broadcast**-opdracht (alleen op supervisor 2 en latere motoren op Catalyst 6500/6000 Series switches, omdat supervisor 1 geen switching-statistieken per VLAN biedt). Bekijk alleen VLAN-interfaces. Het VLAN met de hoogste hoeveelheid geschakelde pakketten zal meestal degene zijn waar de lus voorkwam:

```
cat# show int | include L2|line|broadcast

Vlan1 is up, line protocol is up
  L2 Switched: ucast: 653704527 pkt, 124614363025 bytes - mcast:
        23036247 pkt, 1748707536 bytes
     Received 23201637 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan10 is up, line protocol is up
  L2 Switched: ucast: 2510912 pkt, 137067402 bytes - mcast:
        41608705 pkt, 1931758378 bytes
     Received 1321246 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan11 is up, line protocol is up
  L2 Switched: ucast: 73125 pkt, 2242976 bytes - mcast:
        3191097 pkt, 173652249 bytes
     Received 1440503 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
Vlan100 is up, line protocol is up
  L2 Switched: ucast: 458110 pkt, 21858256 bytes - mcast:
        64534391 pkt, 2977052824 bytes
     Received 1176671 broadcasts, 0 runts, 0 giants, 0 throttles
Vlan101 is up, line protocol is up
  L2 Switched: ucast: 70649 pkt, 2124024 bytes - mcast:
        2175964 pkt, 108413700 bytes
     Received 1104890 broadcasts, 0 runts, 0 giants, 0 throttles
```

In dit voorbeeld, VLAN 1 rekent voor het hoogste aantal uitzendingen en L2-geschakeld verkeer.Is de wortelhaven correct geïdentificeerd?De basishaven moet de laagste kosten voor de root-brug hebben (soms is één traject korter in termen van hoop maar langer in termen van kosten, aangezien hogesnelheidshavens hogere kosten hebben).Om te bepalen welke haven als de wortel voor een bepaald VLAN wordt beschouwd, geef de **show in - boom VLAN *vlan* opdracht uit**:

```
cat# show spanning-tree vlan 333

MST03
  Spanning tree enabled protocol mstp
  Root ID    Priority    32771
             Address     0050.14bb.6000
             Cost        20000
             Port        136 (GigabitEthernet3/8)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32771  (priority 32768 sys-id-ext 3)
             Address     00d0.003f.8800
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Status
---------------- ---- --- --------- -------- ------------------------
Gi3/8            Root FWD 20000     128.136  P2p
Po1              Desg FWD 20000     128.833  P2p
```

Worden BPDU's regelmatig ontvangen op de basishaven en op havens die zouden moeten worden geblokkeerd?BPDU's worden door de root-brug verstuurd met elk `hallo-`interval (twee seconden standaard). Niet-root-bruggen ontvangen, verwerken, wijzigen en propageren de BPDU's die van de wortel worden ontvangen.Geef de **opdracht *interface-*** interface **van de show uit** om te zien of de BPDU's worden ontvangen:

```
cat# show spanning-tree interface g3/2 detail

Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
   Port path cost 20000, Port priority 128, Port Identifier 128.130.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 4, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 3, received 53

cat# show spanning-tree interface g3/2 detail

Port 130 (GigabitEthernet3/2) of MST00 is backup blocking
   Port path cost 20000, Port priority 128, Port Identifier 128.130.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 5, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
```

```
   Loop guard is enabled by default on the port
   BPDU: sent 3, received 54
```

Opmerking: er is één BPDU ontvangen tussen de twee uitgangen van de opdracht (de teller ging van 53 naar 54).De getoonde tellers zijn eigenlijk tellers die door het STP proces zelf worden onderhouden. Dit betekent dat, als het aantal ontvangen tellers toenam, niet alleen BPDU door een fysieke haven werd ontvangen maar ook door het STP-proces werd ontvangen.Als de `ontvangen` BPDU-teller niet hoger is op de poort die verondersteld wordt de root-alternatieve of back-uppoort te zijn, controleer dan of de poort alle multicast ontvangt (BPDU's worden verzonden als multicast). Geef de opdracht **showinterface *interface* tellers** uit:

```
cat# show interface g3/2 counters

Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi3/2           14873036             2         89387             0

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi3/2          114365997         83776        732086            19

cat# show interface g3/2 counters

Port            InOctets   InUcastPkts   InMcastPkts   InBcastPkts
Gi3/2           14873677             2         89391             0

Port           OutOctets  OutUcastPkts  OutMcastPkts  OutBcastPkts
Gi3/2          114366106         83776        732087            19
```

(Een korte beschrijving voor STP poortrollen kan in het korte Samenvatting van STP van poortrollen worden gevonden van Verbeteringen in Spanning-Tree Protocol met Loop Guard en BPDU Scheefdetectie-functies.)Als er geen BPDU's worden ontvangen, controleert u of de poort geen fouten telt. Geef de opdracht *interface interface interface **tellers** tonen uit*:

```
cat# show interface g4/3 counters errors

Port     Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize OutDiscards
Gi4/3        0          0          0          0         0           0

Port  Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen   Runts    Giants
Gi4/3       0         0         0          0         0        0         0
```

Het is mogelijk dat de BPDU's door de fysieke poort worden ontvangen maar nog steeds niet het STP-proces bereiken. Als de opdrachten in de twee vorige voorbeelden tonen dat sommige multicast zijn ontvangen en fouten niet toenemen, dan controleer dan of de BPDU's op het STP-procesniveau worden gedropt. Geef de **afstandsbediening van de switch uit die in-boom processtats** opdracht **overslaat** op Catalyst 6500:

```
cat# remote command switch test spanning-tree process-stats

------------------TX STATS------------------
 transmission rate/sec     = 2
 paks transmitted          = 5011226
 paks transmitted (opt)    = 0
 opt chunk alloc failures  = 0
 max opt chunk allocated   = 0
------------------RX STATS------------------
 receive rate/sec          = 1
 paks received at stp isr  = 3947627
 paks queued at stp isr    = 3947627
 paks dropped at stp isr   = 0
 drop rate/sec             = 0
 paks dequeued at stp proc = 3947627
 paks waiting in queue     = 0
```

```
 queue depth               = 7(max) 12288(total)
--------------PROCESSING STATS---------------
 queue wait time (in ms)   = 0(avg) 540(max)
 processing time (in ms)   = 0(avg) 4(max)
 proc switch count         = 100
 add vlan ports            = 20
 time since last clearing  = 2087269 sec
```

De opdracht die in dit voorbeeld wordt gebruikt, geeft STP-processtatistieken weer. Het is belangrijk te controleren dat de druppelteller niet toeneemt en dat de ontvangen pakketten toenemen.Als ontvangen pakketten niet toenemen maar de fysieke poort wordt ontvangen multicast, controleer of de pakketten door de switch in-band interface (de interface van de CPU) worden ontvangen. Geef de **afstandsbediening switch weer, ibc | i rx_input** opdracht op Catalyst 6500/6000:

```
cat# remote command switch show ibc | i rx_input

rx_inputs=5626468, rx_cumbytes=859971138

cat# remote command switch show ibc | i rx_input

rx_inputs=5626471, rx_cumbytes=859971539
```

Dit voorbeeld toont aan dat, tussen de output, de in-band haven 23 pakketten heeft ontvangen.**N.B.:** Deze 23 pakketten zijn niet alleen BPDU-pakketten; Dit is een globale teller voor alle pakketten die door de in-band poort worden ontvangen.Als er geen aanwijzing is dat BPDU's op de lokale switch of poort worden gedropt, moet u naar de switch aan de andere kant van de link verhuizen en controleren of die switch BPDU's verstuurt.Worden BPDU's regelmatig verstuurd in niet-wortelhavens?Als, volgens de havenrol, de haven BPDU's - maar de buurman ontvangt niet - controleer of BPDU's eigenlijk worden verzonden. Geef de opdracht **voor *interface*-details van de show uit**:

```
cat# show spanning-tree interface g3/1 detail

Port 129 (GigabitEthernet3/1) of MST00 is designated forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.129.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 1774, received 1

cat# show spanning-tree interface g3/1 detail

Port 129 (GigabitEthernet3/1) of MST00 is designated forwarding
   Port path cost 20000, Port priority 128, Port Identifier 128.129.
   Designated root has priority 0, address 0007.4f1c.e847
   Designated bridge has priority 32768, address 00d0.003f.8800
   Designated port id is 128.129, designated path cost 2000019
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 0
   Link type is point-to-point by default, Internal
   Loop guard is enabled by default on the port
   BPDU: sent 1776, received 1
```

In dit voorbeeld zijn twee BPDU's tussen de uitgangen verstuurd.**Opmerking:** het STP-proces onderhoudt de `BPDU: Teller gestuurd`. Dit betekent dat de teller aangeeft dat de BPDU naar de fysieke poort is gestuurd, om uiteindelijk te worden uitgezonden. Controleer of de poorttellers voor overgebrachte multicast pakketten toenemen. Geef de opdracht **tonen**

interface *interface* tellers uit. Dit kan helpen bepalen of er BPDU's uitgaan of niet:

```
cat# show interface g3/1 counters

Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi3/1          127985312          83776         812319             19

Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Gi3/1          131825915          3442          872342            386

cat# show interface g3/1 counters

Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi3/1          127985312          83776         812319             19

Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Gi3/1          131826447          3442          872346            386
```

Met al deze stappen is het idee om de switch of link te vinden waar BPDU's niet ontvangen, verzonden of verwerkt worden.Het is mogelijk, hoe onwaarschijnlijk ook, dat de STP de juiste status voor de haven heeft berekend, maar door een probleem met betrekking tot het controlevliegtuig, kon zij deze staat niet op de verzendende hardware instellen. Er kan een lus worden gemaakt als de vermeende blokkerende poort niet op hardwareniveau is geblokkeerd. Als u een probleem op uw netwerk vermoedt, neemt u contact op met Cisco Technical Support voor verdere assistentie.

5. Herstelt de redundantie.Zodra het apparaat of de verbinding die de lus veroorzaakt is gevonden moet dit apparaat van het netwerk worden geïsoleerd, of moet er actie worden ondernomen om het probleem op te lossen (zoals de vezel of GBIC vervangen). De redundante links, die in Stap 3 zijn losgekoppeld, moeten worden hersteld.Het is belangrijk om zo weinig mogelijk manipulatie te doen aan het apparaat of de link die de loop veroorzaakt, omdat veel omstandigheden die tot een lus leiden zeer voorbijgaand, intermitterend en onstabiel kunnen zijn. Dit betekent dat, als de voorwaarde tijdens of na de probleemoplossing wordt gewist, het even kan duren voordat een dergelijke voorwaarde opnieuw optreedt. Het is mogelijk dat de aandoening helemaal niet meer voorkomt. Alle inspanningen moeten worden geleverd om de voorwaarde te bewaren, zodat het verder kan worden onderzocht door Cisco Technical Support. Het is belangrijk dat u informatie over de toestand verzamelt voordat u de switches opnieuw stelt. Als een conditie is verdwenen is het vaak onmogelijk om de diepere oorzaak van de loop te bepalen. Het vinden van het apparaat of de verbinding die de lus triggt is een belangrijk resultaat, maar u moet ervoor zorgen dat een andere mislukking van dezelfde soort niet de lus opnieuw veroorzaakt. Raadpleeg voor meer informatie het gedeelte Netwerk tegen doorsturen van lijnen van dit document.

Problemen oplossen Excessieve topologische veranderingen die overstromingen veroorzaken

De rol van het TC mechanisme is om L2-verzendtabellen te corrigeren nadat de verzendtopologie is gewijzigd. Dit is nodig om een aansluitingsbreuk te vermijden omdat, na een TC, sommige MAC-adressen die eerder toegankelijk waren door bepaalde poorten toegankelijk zouden kunnen worden via verschillende poorten. TC verkort de uitzendtijd van de tabel op alle switches in het VLAN waar de TC plaatsvindt; als het adres niet wordt vrijgegeven, zal het ouderdom hebben en zullen overstromingen voorkomen om ervoor te zorgen dat pakketten het MAC-adres van het bestemming bereiken.

TC wordt geactiveerd door de verandering van de STP-status van een haven in of van de STP-`verzendstaat`. Na afloop van een TC, zelfs als het specifieke MAC-adres van de bestemming is verouderd, hoeft de overstroming niet lang te worden voortgezet. Het adres wordt vrijgegeven door het eerste pakket dat van de host komt wiens MAC-adres is verouderd. Deze kwestie kan zich voordoen wanneer TC's herhaaldelijk en met korte tussenpozen plaatsvinden. De switches zullen hun expeditietafels voortdurend verouderen dus zullen de overstromingen vrijwel constant blijven.

Opmerking: met Rapid STP of Multiple STP (IEEE 802.1w en IEEE 802.1s) wordt TC geactiveerd door een verandering van de status van de poort om `door` te `sturen`, evenals de rolverandering van `aangewezen` naar `wortel`. Met Rapid STP wordt de L2-verzendtabel onmiddellijk gespoeld, in tegenstelling tot 802.1d, wat de verouderingstijd verkort. Het onmiddellijke spoelen van de het verzenden tafel herstelt connectiviteit sneller, maar zal meer overstroming veroorzaken.

TC zou een zeldzame gebeurtenis moeten zijn in een goed gevormd netwerk. Wanneer een verbinding op een haven van de switch omhoog of omlaag gaat is er uiteindelijk een TC, wanneer de STP staat van de haven in of van `het door` te `sturen` verandert. Wanneer de haven flappelt, zou dit repetitieve TC's en overstromingen veroorzaken.

Poorten met de STP portfast optie zullen geen TCs veroorzaken wanneer het gaan naar of van de `expediteur` staat. De configuratie van portfast op alle eindapparaatpoorten (zoals printers, PC's en servers) moet de TC's tot een laag niveau beperken en wordt ten zeerste aanbevolen. Raadpleeg voor meer informatie over TC's het begrip Spanning-Tree Protocol-wijzigingen.

Als er meerdere TC's op het netwerk staan, moet u de bron van deze TC's identificeren en actie ondernemen om ze te verminderen, om de overstroming tot een minimum te beperken.

Met 802.1d wordt STP-informatie over een TC-event verspreid onder de bruggen door een TC-melding (TCN), een speciaal type BPDU. Als u de poorten volgt die TCN BPDU's ontvangen, kunt u het apparaat vinden dat van oorsprong TC's is.

Instellen of overstromingen veroorzaakt worden door STP-bedrijven

Normaal gesproken kunt u bepalen dat er sprake is van overstroming door een trage prestatie, dat pakketdruppels op koppelingen die niet verondersteld worden te worden gestreept en dat de pakketanalyzer met meerdere pakketten op dezelfde bestemming is die niet op het lokale segment staat.

Raadpleeg voor meer informatie over overstroming op internet Unicast-overstromingen in Switched Campus Networks.

Op een Catalyst 6500/6000 die Cisco IOS-software draait, kunt u de expediteur 2-motor controleren om de hoeveelheid overstroming in te schatten. Geef de **afstandsbediening switch vroege statistieken op | i MISS_DA|ST_FR** opdracht:

```
cat# remote command switch show earl statistics | i MISS_DA|ST_FR

         ST_MISS_DA      =       18                      530308834
         ST_FRMS         =       97                      969084354

cat# remote command switch show earl statistics | i MISS_DA|ST_FR

         ST_MISS_DA      =       4                       530308838
```

```
        ST_FRMS        =       23                      969084377
```

In dit voorbeeld, toont de eerste kolom de verandering sinds de laatste keer deze opdracht werd uitgevoerd, en de tweede kolom toont de cumulatieve waarde sinds de laatste herstart. De eerste regel toont de hoeveelheid overstroomde frames en de tweede regel toont de hoeveelheid verwerkte frames. Als de twee waarden dicht bij elkaar liggen, of de eerste waarde in hoog tempo toeneemt, kan het zijn dat de switch het verkeer overspoelt. Dit kan echter alleen worden gebruikt in combinatie met andere manieren om overstromingen te controleren, aangezien de tellers niet granulair zijn. Er is één teller per switch, niet per poort of VLAN. Het is normaal om sommige overstroompakketten te zien, aangezien de switch altijd overstroomt als het bestemmingsMAC-adres niet in de verzendingstabel is. Dit zal het geval zijn wanneer de switch een pakje met een bestemmingsadres ontvangt dat nog niet geleerd is.

Onderzoeken van de bron van de TC's

Als het VLAN-nummer bekend is voor het VLAN waar buitensporige overstromingen plaatsvinden, controleert u de STP-tellers om te zien of het aantal TC's hoog is of regelmatig toeneemt. Geef de **opdracht** van de **show in** het **vlan-*VLAN-id* detail** uit (in dit voorbeeld wordt VLAN 1 gebruikt):

```
cat# show spanning-tree vlan 1 detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 32768, sysid 1, address 0007.0e8f.04c0
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 0, address 0007.4f1c.e847
  Root port is 65 (GigabitEthernet2/1), cost of root path is 119
  Topology change flag not set, detected flag not set
  Number of topology changes 1 last change occurred 00:00:35 ago
          from GigabitEthernet1/1
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
```

Als het VLAN-nummer niet bekend is, kunt u de pakketanalyzer gebruiken of de TC-tellers voor alle VLAN's controleren.

Maatregelen ter voorkoming van overmatige bedrijfsverplaatsingen

U kunt het `aantal topologieveranderingen` controleren om te zien of het regelmatig groeit. Verplaats vervolgens naar de brug die aangesloten is op de poort die wordt getoond, om de laatste TC te ontvangen (in het vorige voorbeeld, haven Gigabit Ethernet1/1) en zie van waar de TC voor die brug kwam. Dit proces moet worden herhaald tot de end-station poort zonder STP portfast wordt gevonden, of tot de flappinglink wordt gevonden die moet worden gerepareerd. De hele procedure moet worden herhaald als TC's nog steeds uit andere bronnen komen. Als de link tot een end-host behoort, dient u de Portfast-functie te configureren om de generatie van TC's te voorkomen.

Opmerking: In de Cisco IOS software STP-implementatie zal de teller voor TCs alleen toenemen als een GN BPDU door een poort in een VLAN wordt ontvangen. Als een normale configuratie BPDU met een ingestelde TC-vlag wordt ontvangen, wordt de TC-teller niet verhoogd. Dit betekent dat, als u vermoedt dat een TC de reden voor overstromingen is, het best is om de bronnen voor de TC vanaf de STP root-brug in dat VLAN op te sporen. Zij zal over de meest accurate informatie beschikken over het bedrag en de bron van de TC's.

Problemen oplossen en conversietijd

Er zijn situaties waarin de eigenlijke werking van STP niet overeenkomt met het verwachte gedrag. Dit zijn de twee meest voorkomende problemen:

- convergentie of herconvergentie van STP verloopt langer dan verwacht.
- De resulterende topologie is anders dan verwacht.

Meestal zijn dit de redenen voor dit gedrag:

- Een mismatch tussen de echte en gedocumenteerde topologie
- Misconfiguratie, zoals een inconsistente configuratie van STP-timers, die de STP-diameter overschrijden of een snelle verkeerde configuratie
- Overbelaste switch CPU's bij convergentie of herconvergentie
- Softwaredefect

Zoals eerder vermeld kan dit document alleen algemene richtlijnen bieden voor het oplossen van problemen, vanwege de grote verscheidenheid aan problemen die STP kunnen beïnvloeden.

Om te begrijpen waarom de convergentie langer duurt dan verwacht, bekijk dan de opeenvolging van STV - gebeurtenissen om te weten te komen wat er gebeurde en in welke volgorde. Omdat de STP-implementatie in Cisco IOS-software geen speciale vastlegging heeft (behalve voor specifieke gebeurtenissen, zoals poortinconsistenties), kunt u Cisco IOS software STP-zuiveringsfuncties gebruiken om te begrijpen wat er gebeurt.

Voor STP met een Catalyst 6500/6000 die Cisco IOS-software draait, wordt de verwerking uitgevoerd op de Switch Processor (SP) (of supervisor), dus moeten de databases op de SP-basis ingeschakeld zijn. Voor Cisco IOS-softwarebruggroepen wordt de verwerking uitgevoerd op de Routeprocessor (RP), zodat de debugs moeten worden ingeschakeld op de RP (MSFC).

STP-foutoplossingen

Vele STP **debug** opdrachten zijn bedoeld voor gebruik in ontwikkelingstechniek. Ze bieden geen output die betekenisvol is voor iemand zonder gedetailleerde kennis van de STP implementatie in Cisco IOS-software. Sommige debugs kunnen output leveren die onmiddellijk leesbaar is, zoals veranderingen in de havenstaat, rolveranderingen, gebeurtenissen zoals TC's, en een stortplaats van ontvangen en overgedragen BPDU's. Deze paragraaf geeft geen volledige beschrijving van alle deposito's, maar introduceert kort de meest gebruikte.

N.B.: Wanneer u **debug-**opdrachten gebruikt, schakelt u de minimaal benodigde apparaten in. Als real-time versies niet nodig zijn, neem de uitvoer naar het logbestand op in plaats van het op de console af te drukken. Extreme defecten kunnen de CPU overladen en de werking van de switch verstoren. Om uitvoer naar het logbestand in plaats van naar de console of naar de Telnet-sessies te sturen geeft u de **houtkapconsole-informatie** uit en **geen** opdrachten van de **houtkapmonitor** in de mondiale configuratie-modus.

Om het logbestand van algemene gebeurtenissen te zien, geeft u het opdracht **om een** overspannende **boom**-gebeurtenis af te **draaien** voor Per VLAN Spanning-Tree (PVST) en Rapid-PVST. Dit is het eerste debug dat een algemeen idee geeft van wat er met STP gebeurt.

In de Meervoudige Spanning-Tree (MST) modus werkt het niet om de opdracht **debug** van **overspannende bomen** uit te geven. Geef daarom de **debug van het overspannen van een boom mstp rollen uit** om de veranderingen van de havenrol te zien.

Om de de staat van de haven STP te zien verandert, geef het **debug van de staat van de switch**

van de overspanning uit samen met het debug pm vp bevel:

```
cat-sp# debug spanning-tree switch state

Spanning Tree Port state changes debugging is on

cat-sp# debug pm vp

Virtual port events debugging is on
Nov 19 14:03:37: SP:     pm_vp 3/1(333): during state forwarding, got event 4(remove)
Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333):
  forwarding -> notforwarding

port 3/1 (was forwarding) goes down in vlan 333

Nov 19 14:03:37: SP: *** vp_fwdchange: single: notfwd: 3/1(333)
Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): notforwarding -> present
Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/1(333)
Nov 19 14:03:37: SP: @@@ pm_vp 3/1(333): present -> not_present
Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/1(333)
Nov 19 14:03:37: SP:     pm_vp 3/2(333): during state notforwarding,
  got event 4(remove)
Nov 19 14:03:37: SP: @@@ pm_vp 3/2(333): notforwarding -> present
Nov 19 14:03:37: SP: *** vp_linkchange: single: down: 3/2(333)

Port 3/2 (was not forwarding) in vlan 333 goes down

Nov 19 14:03:37: SP: @@@ pm_vp 3/2(333): present -> not_present
Nov 19 14:03:37: SP: *** vp_statechange: single: remove: 3/2(333)

Nov 19 14:03:53: SP:     pm_vp 3/1(333): during state not_present,
  got event 0(add)
Nov 19 14:03:53: SP: @@@ pm_vp 3/1(333): not_present -> present
Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/1(333)
Nov 19 14:03:53: SP:     pm_vp 3/1(333): during state present,
  got event 8(linkup)
Nov 19 14:03:53: SP: @@@ pm_vp 3/1(333): present ->
  notforwarding
Nov 19 14:03:53: SP: STP SW: Gi3/1 new blocking req for 0 vlans
Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/1(333)

Port 3/1 link goes up and blocking in vlan 333

Nov 19 14:03:53: SP:     pm_vp 3/2(333): during state not_present,
  got event 0(add)
Nov 19 14:03:53: SP: @@@ pm_vp 3/2(333): not_present -> present
Nov 19 14:03:53: SP: *** vp_statechange: single: added: 3/2(333)
Nov 19 14:03:53: SP:     pm_vp 3/2(333): during state present,
  got event 8(linkup)
Nov 19 14:03:53: SP: @@@ pm_vp 3/2(333): present ->
  notforwarding
Nov 19 14:03:53: SP: STP SW: Gi3/2 new blocking req for 0 vlans
Nov 19 14:03:53: SP: *** vp_linkchange: single: up: 3/2(333)

Port 3/2 goes up and blocking in vlan 333

Nov 19 14:04:08: SP: STP SW: Gi3/1 new learning req for 1 vlans
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 0 vlans
Nov 19 14:04:23: SP: STP SW: Gi3/1 new forwarding req for 1 vlans
Nov 19 14:04:23: SP:     pm_vp 3/1(333): during state notforwarding,
  got event 14(forward_notnotify)
Nov 19 14:04:23: SP: @@@ pm_vp 3/1(333): notforwarding ->
```

```
  forwarding
Nov 19 14:04:23: SP: *** vp_list_fwdchange: forward: 3/1(333)

Port 3/1 goes via learning to forwarding in vlan 333
```

Om te begrijpen waarom STP zich op een bepaalde manier gedraagt, is het vaak nuttig om de BPDU's te zien die door de switch worden ontvangen en verzonden:

```
cat-sp# debug spanning-tree bpdu receive

Spanning Tree BPDU Received debugging is on
Nov  6 11:44:27: SP: STP: VLAN1 rx BPDU: config protocol = ieee,
  packet from GigabitEthernet2/1  , linktype IEEE_SPANNING ,
  enctype 2, encsize 17
Nov  6 11:44:27: SP: STP: enc 01 80 C2 00 00 00 00 06 52 5F 0E 50 00 26 42 42 03
Nov  6 11:44:27: SP: STP: Data 00000000000000000074F1CE847000000013804800006525F0E4
  080100100140002000F00
Nov  6 11:44:27: SP: STP: VLAN1 Gi2/1:0000 00 00 00 000000074F1CE847 00000013
  80480006525F0E40 8010 0100 1400 0200 0F00
```

Dit debug werkt voor PVST-, Rapid-PVST- en MST-modi; maar de inhoud van de BPDU's wordt niet gedecodeerd. U kunt deze echter gebruiken om er zeker van te zijn dat BPDU's worden ontvangen.

Om de inhoud van de BPDU te zien, geef het **debug van de switch Rx decode** opdracht samen met het **debug in-boom switch rx procesopdracht** voor PVST en Rapid-PVST uit. Geef de opdracht **debug-in-boom** mstp **bpdu-rx uit** om de inhoud van de BPDU voor MST te zien:

```
cat-sp# debug spanning-tree switch rx decode

Spanning Tree Switch Shim decode received packets debugging is on

cat-sp# debug spanning-tree switch rx process

Spanning Tree Switch Shim process receive bpdu debugging is on

Nov  6 12:23:20: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov  6 12:23:20: SP:     encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov  6 12:23:20: SP:     42 42 03 SPAN
Nov  6 12:23:20: SP:     CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov  6 12:23:20: SP:     B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00

Nov  6 12:23:22: SP: STP SW: PROC RX: 0180.c200.0000<-0006.525f.0e50 type/len 0026
Nov  6 12:23:22: SP:     encap SAP linktype ieee-st vlan 1 len 52 on v1 Gi2/1
Nov  6 12:23:22: SP:     42 42 03 SPAN
Nov  6 12:23:22: SP:     CFG P:0000 V:00 T:00 F:00 R:0000 0007.4f1c.e847 00000013
Nov  6 12:23:22: SP:     B:8048 0006.525f.0e40 80.10 A:0100 M:1400 H:0200 F:0F00
```

In de MST-modus kunt u een gedetailleerde BPDU-decode inschakelen met deze opdracht **debug**:

```
cat-sp# debug spanning-tree mstp bpdu-rx

Multiple Spanning Tree Received BPDUs debugging is on
Nov 19 14:37:43: SP: MST:BPDU DUMP [rcvd_bpdu Gi3/2 Repeated]
Nov 19 14:37:43: SP: MST:   Proto:0 Version:3 Type:2 Role: DesgFlags[   F    ]
Nov 19 14:37:43: SP: MST:   Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST:   root_id  :0007.4f1c.e847 Prio:0
Nov 19 14:37:43: SP: MST:   br_id    :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST:   age:2 max_age:20 hello:2 fwdelay:15
```

```
Nov 19 14:37:43: SP: MST:   V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST:   ist_m_id :0005.74
Nov 19 14:37:43: SP: MST:BPDU DUMP [rcvd_bpdu Gi3/2 Repeated]
Nov 19 14:37:43: SP: MST:   Proto:0 Version:3 Type:2 Role: DesgFlags[   F    ]
Nov 19 14:37:43: SP: MST:   Port_id:32897 cost:2000019
Nov 19 14:37:43: SP: MST:   root_id  :0007.4f1c.e847 Prio:0
Nov 19 14:37:43: SP: MST:   br_id    :00d0.003f.8800 Prio:32768
Nov 19 14:37:43: SP: MST:   age:2 max_age:20 hello:2 fwdelay:15
Nov 19 14:37:43: SP: MST:   V3_len:90 PathCost:30000 region:STATIC rev:1
Nov 19 14:37:43: SP: MST:   ist_m_id :0005.7428.1440 Prio:32768  Hops:18
  Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3  Flags[ F    ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST:         br_id:00d0.003f.8800 Prio:32771 Port_id:32897
  Cost:2000028.1440 Prio:32768  Hops:18  Num Mrec: 1
Nov 19 14:37:43: SP: MST: stci=3  Flags[ F    ] Hop:19 Role:Desg [Repeated]
Nov 19 14:37:43: SP: MST:         br_id:00d0.003f.8800 Prio:32771 Port_id:32897
  Cost:20000
```

Opmerking: voor Cisco IOS-softwarerelease 12.1.13E en later worden voorwaardelijke oplossingen voor STP ondersteund. Dit betekent dat u BPDU's kunt zuiveren die op een per-poorts of per-VLAN basis worden ontvangen of verzonden.

Geef de **opdrachten debug-conditie vlan** *vlan_num* of **debug-interface interface af** om het bereik van de debug-uitvoer te beperken tot per-interface of per-VLAN.

Het netwerk beveiligen tegen het doorsturen van lijnen

Om STP's onvermogen om bepaalde fouten correct om te gaan heeft Cisco een aantal eigenschappen en verbeteringen ontwikkeld om de netwerken tegen het verzenden van loops te beschermen.

STP van de oplossing van problemen helpt om de oorzaak van een bepaalde mislukking te isoleren en misschien te vinden, terwijl de implementatie van deze verbeteringen de enige manier is om het netwerk tegen het verzenden loops te beveiligen.

Dit zijn methodes om uw netwerk tegen het verzenden loops te beschermen:

1. Schakel Unidirectional Link Detection (UDLD) in op alle switch-to-switch links. Raadpleeg voor meer informatie over UDLD het begrip en de configuratie van de functies voor Unidirectional Link Detection Protocol.
2. Loop Guard inschakelen op alle switches. Raadpleeg voor meer informatie over Loop Guard de verbeteringen van Spanning-Tree Protocol met Loop Guard en BPDU Skew Detectie-functies.Indien ingeschakeld, elimineren UDLD en Loop Guard de meerderheid van de mogelijke oorzaken voor het verzenden van loops. In plaats van een expediteur loop te maken, wordt de offending link (of alle links die afhankelijk zijn van de falende hardware) afgesloten of geblokkeerd.**Opmerking:** Hoewel deze twee functies ietwat overbodig lijken, heeft elk zijn unieke functies. Gebruik daarom beide functies tegelijkertijd om het hoogste beschermingsniveau te bieden. Voor een gedetailleerde vergelijking van UDLD en Loop Guard kunt u Loop Guard vs. Unidirectional Link Detection raadplegen.Er zijn verschillende meningen over of je agressieve of normale UDLD moet gebruiken. Er zij op gewezen dat agressieve UDLD niet meer bescherming biedt tegen loops in vergelijking met normale mode UDLD. Aggressieve UDLD detecteert poortgebonden scenario's (wanneer de link omhoog is, maar er zijn geen gekoppelde verkeerstekorten). De negatieve kant van deze toegevoegde functionaliteit is dat agressieve UDLD verbindingen potentieel kan verhinderen wanneer

geen consistente mislukking aanwezig is. Vaak verwarren mensen de verandering van de UDLD `hallo` interval met de agressieve UDLD optie. Dit klopt niet. Timers kunnen in beide UDLD-modi worden gewijzigd.**Opmerking:** In zeldzame gevallen kan een agressieve UDLD alle bergtoppen sluiten, wat de switch in wezen isoleert van de rest van het netwerk. Dit zou bijvoorbeeld kunnen gebeuren wanneer beide upstream switches een zeer hoog CPU-gebruik ervaren en wanneer de agressieve UDLD wordt gebruikt. Om deze reden wordt aangeraden om tijdelijke instellingen te configureren als de switch geen out-of-band beheer heeft.

3. Doe portfast op alle eindstationpoorten.U moet portfast in staat stellen om de hoeveelheid TC's en daaropvolgende overstromingen te beperken, die de prestaties van het netwerk kunnen beïnvloeden. Gebruik deze opdracht alleen met poorten die verbinding maken met eindstations. Anders kan een accidentele topologie-lus een datapakket opleveren en de switch en de netwerkhandeling ontwrichten.**Waarschuwing:** oefen voorzichtigheid wanneer u de **geen over-boom** opdracht gebruikt. Deze opdracht verwijdert alleen alle poortspecifieke opdrachten. Deze opdracht maakt portfast impliciet mogelijk als u de **over-boom** poort **standaard** opdracht definieert in mondiale configuratiemodus en als de poort geen boompoort is. Als u niet wereldwijd dynamisch instelt, is de **geen over-boom** portfast opdracht gelijk aan de **over-boom** opdracht **om te verhinderen**.
4. Stel EtherChannel in op `gewenste` modus aan beide zijden (indien ondersteund) en `niet-stille` optie.`Bewerkbare` modus maakt Port Aggregation Protocol (PAgP) mogelijk om een run op de consistentie tussen de kantelende peers te waarborgen. Dit geeft een extra mate van bescherming tegen loops, vooral tijdens kanaalherconfiguraties (zoals wanneer de verbindingen zich bij het kanaal aansluiten of verlaten, en de detectie van verbindingsmislukkingen). Er is een ingebouwde kanaalconfiguratie Garde, die standaard ingeschakeld is en die het doorsturen van lijnen door verkeerde configuratie of andere voorwaarden verhindert. Raadpleeg voor meer informatie over deze functie het begrip EtherChannel inconsistentie voor de detectie van inconsistenties.
5. Schakel automatische onderhandeling (indien ondersteund) niet uit op switch-naar-switch koppelingen.Automatische onderhandelingsmechanismen kunnen informatie over fouten op afstand overbrengen, wat de snelste manier is om fouten aan de verre kant te detecteren. Mocht er een storing worden gedetecteerd aan de afgelegen kant, dan drukt de lokale kant de link omlaag, zelfs als de link nog steeds pulsen ontvangt. Vergeleken met detectie op hoog niveau, zoals UDLD, is de automatische onderhandeling zeer snel (binnen microseconden) maar heeft de end-to-end dekking van UDLD (zoals de gehele datapath: CPU—door:sturen van logica—port1—door:sturen van logica—CPU versus port1—port2). Aggressieve UDLD-modus biedt een soortgelijke functionaliteit als de automatische onderhandeling wat betreft de detectie van storingen. Wanneer onderhandelingen aan beide zijden van de verbinding worden ondersteund, hoeft geen agressieve modus UDLD mogelijk te maken.
6. Gebruik voorzichtigheid als u de STP-timers aanpast.STP-timers zijn afhankelijk van elkaar en van de netwerktopologie. STP werkt mogelijk niet goed met willekeurige wijzigingen die aan de timers zijn aangebracht. Voor meer informatie over STP-timers raadpleegt u Spanning Tree Protocol-timers begrijpen en afstemmen.
7. Als de ontkenning van de dienstaanvallen mogelijk is, moet u de STP-perimeter van het netwerk met Root Guard beveiligen.Root Guard en BPDU Guard staan u toe STP te beveiligen tegen invloed van buitenaf. Als zo'n aanval mogelijk is, moeten Root Guard en BPDU Guard worden gebruikt om het netwerk te beschermen. Raadpleeg deze documenten voor meer informatie over Root Guard en BPDU Guard:Verbetering in Spanning-Tree

Protocol Root GuardVerbetering in Spanning Tree Portfast BPDU Guard

8. Schakel BPDU Guard op portfast-enabled poorten in om te voorkomen dat STP wordt beïnvloed door onbevoegde netwerkapparaten (zoals hubs, switches en overbruggingsrouters) die met de poorten zijn verbonden.Als Root Guard goed is geconfigureerd zal dit al voorkomen dat de STP van buitenaf wordt beïnvloed. Als de BPDU Guard is ingeschakeld, sluit u de poorten af die BPDU's ontvangen (niet alleen superieure BPDU's). Dit kan handig zijn als dergelijke incidenten moeten worden onderzocht, omdat de BPDU Guard het waarschuwingsbericht produceert en de haven sluit. Opgemerkt moet worden dat korte-levende loops niet door Root of BPDU Guards worden voorkomen, als twee havens die met portfast-mogelijkheid zijn verbonden direct of door de hub worden verbonden.
9. Vermijd gebruikersverkeer op het beheer VLAN. Het beheer VLAN is ingesloten in een bouwsteen, niet het gehele netwerk.De interface voor het beheer van de switch ontvangt uitzendingspakketten op het beheer VLAN. Mocht er buitensporige uitzendingen plaatsvinden (zoals een uitzending-storm of een slecht functionerende toepassing), dan kan de switch CPU worden overbelast, wat de STP-werking mogelijk kan verstoren.
10. Een voorspelbare (harde) STP root en back-up STP root plaatsing.De STP wortel en de backup-STP wortel moeten zo worden geconfigureerd dat convergentie, in het geval van fouten, op een voorspelbare manier plaatsvindt en in elk scenario een optimale topologie oplevert. Laat de STP-prioriteit niet aan de standaardwaarde staan om onvoorspelbare switch te voorkomen.

Gerelateerde informatie

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