

# HSRP-problemen oplossen in Catalyst Switch-netwerken

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[HSRP begrijpen](#)

[Achtergrondinformatie](#)

[Basiswerking](#)

[HSRP-begrippen](#)

[HSRP-adressering](#)

[Communicatie tussen HSRP-routers](#)

[Communicatie via stand-by-IP-adres voor HSRP op alle media behalve Token Ring](#)

[ICMP-omleidingen](#)

[Matrix van HSRP-functionaliteit](#)

[HSRP-functies](#)

[Indeling van pakketten](#)

[HSRP-toestanden](#)

[HSRP-timers](#)

[HSRP-gebeurtenissen](#)

[HSRP-acties](#)

[HSRP-toestandstabel](#)

[Pakketstroom](#)

[Configuratie van router A \(actieve router\)](#)

[Configuratie van router B \(stand-byrouter\)](#)

[Casestudy's voor troubleshooting van HSRP](#)

[Case Study #1: HSRP Standby IP-adres wordt als dubbel IP-adres gemeld](#)

[Case Study #2: HSRP-status verandert voortdurend \(actief, stand-by, spreken\) of %HSRP-6-STATUS](#)

[Case Study #3: HSRP herkent peer niet](#)

[Case Study #4: Veranderingen in HSRP-status en rapporten van de Switch SYS-4-P2 WARN: 1/Host](#)

[Case Study #5: asymmetrische routing en HSRP \(buitensporige overstroming van Unicast-verkeer in netwerk met routers die HSRP uitvoeren\)](#)

[MSFC1](#)

[MSFC2](#)

[Gevolgen van asymmetrische routing](#)

[Case Study #6: HSRP virtueel IP-adres wordt als een ander IP-adres gemeld](#)

[Case Study #7: HSRP veroorzaakt schending van MAC op een beveiligde poort](#)

[Case Study #9: %interface hardware kan geen meerdere groepen ondersteunen](#)

[Probleemoplossing voor HSRP in Catalyst Switches](#)

## [A. Configuratie van HSRP-routers verifiëren](#)

- [1. Uniek IP-adres van routerinterface verifiëren](#)
- [2. Stand-by-IP-adressen \(HSRP\) en stand-bygroepsnummers verifiëren](#)
- [3. Verifiëren of stand-by-IP-adres \(HSRP\) per interface verschilt](#)
- [4. Wanneer u de opdracht 'standby use-bia' moet gebruiken](#)
- [5. Configuratie van toegangslijsten verifiëren](#)

## [B. Fast EtherChannel- en trunking-configuratie bij Catalyst verifiëren](#)

- [1. Trunking-configuratie verifiëren](#)
- [2. Fast EtherChannel-configuratie \(poortkanalen\) verifiëren](#)
- [3. Doorstuurtabel voor MAC-adressen van switches onderzoeken](#)

## [C. Connectiviteit van fysieke laag verifiëren](#)

- [1. Interfacestatus controleren](#)
- [2. Wijziging in links en poortfouten](#)
- [3. IP-connectiviteit verifiëren](#)
- [4. Controleren op unidirectionele link](#)
- [5. Aanvullende verwijzingen voor troubleshooting van fysieke laag](#)

## [D. HSRP-foutopsporing voor Layer 3](#)

- [1. Standaard HSRP-foutopsporing](#)
- [2. Voorwaardelijke HSRP-foutopsporing \(output beperken gebaseerd op stand-bygroep en/of VLAN\)](#)
- [3. Uitgebreide HSRP-foutopsporing](#)

## [E. Spanning Tree-problemen troubleshooten](#)

- [1. Spanning Tree-configuratie verifiëren](#)
- [2. Lusvoorwaarden bij Spanning Tree](#)
- [3. Melding van gewijzigde topologie](#)
- [4. Niet-verbonden geblokkeerde poorten](#)
- [5. Broadcast onderdrukking](#)
- [6. Console- en Telnet-toegang](#)
- [7. Spanning Tree-functies: Portfast, UplinkFast en BackboneFast](#)

## [8. BPDU Guard](#)

## [9. VTP-pruning](#)

## [F. Delen en veroveren](#)

### [Bekende problemen](#)

[HSRP-status flappen/instabiel bij gebruik van Cisco 2620/2621, Cisco 3600 met Fast Ethernet](#)

### [Gerelateerde informatie](#)

## **Inleiding**

Dit document beschrijft veel voorkomende problemen en manieren om HSRP-problemen (Hot Standby Router Protocol) op te lossen.

## **Voorwaarden**

## **Vereisten**

Er zijn geen specifieke vereisten van toepassing op dit document.

## Gebruikte componenten

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

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.

## HSRP begrijpen

### Achtergrondinformatie

In dit document worden veelvoorkomende problemen in verband met HSRP behandeld:

- Routermelding van een dubbel stand-by-IP-adres voor HSRP
- Doorlopende verandering van de HSRP-toestand (active, standby, speak)
- HSRP-peers niet aanwezig
- Foutberichten van switches met betrekking tot HSRP
- Overmatige unicast flooding van netwerk naar HSRP-configuratie

**Opmerking:** in dit document wordt uitgelegd hoe u HSRP kunt oplossen in Catalyst switch-omgevingen. Het document bevat veel verwijzingen naar softwareversies en het ontwerp van de netwerktopologie. Niettemin is het enige doel van dit document om engineers te ondersteunen bij het troubleshooten van HSRP-problemen. Dit document is niet bedoeld als ontwerphandleiding, als document met software-aanbevelingen of als document met best practices.

Bedrijven en consumenten die voor hun bedrijfskritische communicatie gebruik maken van intranet- en internetservices eisen en verwachten dat hun netwerken en toepassingen ononderbroken beschikbaar zijn. Klanten kunnen vrijwel 100% netwerktuptime garanderen door HSRP te gebruiken in Cisco IOS®-software. HSRP is uniek voor Cisco-platforms. Het biedt netwerkredundantie voor IP-netwerken op zo'n manier dat gebruikersverkeer direct en transparant herstelt van 'first hop'-fouten in apparaten aan de netwerk-edge of access circuits.

Twee of meer routers kunnen fungeren als één virtuele router als ze een IP-adres en een MAC-adres (Layer 2 [L2]) delen. Het adres is nodig voor redundantie van de standaardgateway van het hostwerkstation. De meeste hostwerkstations bevatten geen routingtabellen en gebruiken slechts één IP- en MAC-adres van de volgende hop. Dit adres is de standaardgateway. Met HSRP wisselen leden van de virtuele routergroep doorlopend statusberichten uit. De ene router kan de routingverantwoordelijkheid van de andere op zich nemen als een router om geplande of ongeplande redenen buiten gebruik wordt gesteld. Hosts worden geconfigureerd met één standaardgateway en blijven IP-pakketten doorsturen naar een consistent IP- en MAC-adres. De wisseling tussen apparaten die de routing regelen is transparant voor de eindwerkstations.

**Opmerking:** u kunt hostwerkstations configureren die Microsoft OS uitvoeren voor meerdere standaardgateways. Maar de meerdere standaardgateways zijn niet dynamisch. Het besturingssysteem gebruikt slechts één standaardgateway tegelijk. Het systeem selecteert

alleen een aanvullende geconfigureerde standaardgateway tijdens het opstarten als het Internet Control Management Protocol (ICMP) bepaalt dat de eerste geconfigureerde standaardgateway onbereikbaar is.

## Basiswerking

Een reeks routers met HSRP werkt in overleg, zodat het voor de hosts op het LAN lijkt of er één standaardgatewayrouter is. Deze reeks routers is een HSRP-groep of stand-bygroep. Eén router die uit de groep is geselecteerd, is verantwoordelijk voor het doorsturen van de pakketten die hosts naar de virtuele router verzenden. Deze router is de actieve router. Een andere router wordt geselecteerd als stand-byrouter. Als de actieve router niet goed werkt, neemt de stand-byrouter het doorsturen van pakketten over. Hoewel een willekeurig aantal routers HSRP kan uitvoeren, stuurt alleen de actieve router de pakketten door die naar het virtuele router IP-adres worden verzonden.

Om het netwerkverkeer te minimaliseren, verzenden alleen de actieve en stand-byrouters periodieke HSRP-berichten nadat het protocol het selectieproces heeft voltooid. Aanvullende routers in de HSRP-groep blijven de toestand `Listen` behouden. Als de actieve router niet goed werkt, neemt de stand-byrouter de rol van actieve router over. Als de stand-byrouter niet goed werkt of de actieve router wordt, wordt een andere router geselecteerd als de stand-byrouter.

Elke stand-bygroep emuleert één virtuele router (standaardgateway). Aan elke groep wordt één bekend MAC- en IP-adres toegewezen. Meerdere stand-bygroepen kunnen naast elkaar bestaan en elkaar overlappen op een LAN, en afzonderlijke routers kunnen aan meerdere groepen deelnemen. In dat geval behoudt de router een afzonderlijke toestand en afzonderlijke timers voor elke groep.

## HSRP-begrippen

Begrip	Definitie
Actieve router	De router die op dat moment pakketten doorstuurt voor de virtuele router
Stand-byrouter	De primaire back-uprouter
Stand-bygroep	De reeks routers die aan HSRP deelnemen en gezamenlijk een virtuele router emuleren
Hello-tijd	Het interval tussen opeenvolgende hello-berichten voor HSRP afkomstig van een bepaalde router
Wachtstandtijd	Het interval tussen de ontvangst van een hello-bericht en de aanname dat de verzendende router niet goed werkt

## HSRP-adressering

### Communicatie tussen HSRP-routers

Routers met HSRP communiceren HSRP-informatie met elkaar door middel van hello-pakketten voor HSRP. Deze pakketten worden naar het IP-multicast adres 224.0.0.2 van de bestemming op UDP-poort (User Datagram Protocol) 1985 verzonden. IP-multicast adres 224.0.0.2 is een gereserveerd multicast adres dat wordt gebruikt om met alle routers te communiceren. De actieve router haalt hello-pakketten op via het geconfigureerde IP-adres en het virtuele MAC-adres voor HSRP. De stand-byrouter haalt hello-pakketten op via het geconfigureerde IP-adres en het ingebrande MAC-adres (BIA). Dit gebruik van bron-adressering is nodig om ervoor te zorgen dat HSRP-routers elkaar correct kunnen identificeren.

Wanneer u routers configureert als onderdeel van een HSRP-groep, luisteren deze in de meeste gevallen naar het MAC-adres voor HSRP voor die groep en hun eigen BIA. Alleen Cisco 2500, 4000 en 4500 routers reageren anders. Deze routers hebben Ethernet-hardware die slechts één MAC-adres herkent. Daarom gebruiken deze routers het MAC-adres voor HSRP wanneer ze als actieve router fungeren. De routers gebruiken hun BIA wanneer ze stand-byrouter fungeren.

## Communicatie via stand-by-IP-adres voor HSRP op alle media behalve Token Ring

Omdat hostwerkstations zijn geconfigureerd met hun standaardgateway als het stand-by-IP-adres voor HSRP, moeten hosts communiceren met het MAC-adres dat gekoppeld is aan het stand-by-IP-adres voor HSRP. Dit MAC-adres is een virtueel MAC-adres in de vorm 0000.0c07.ac\*\*. \*\* is het HSRP-groepsnummer in hexadecimale, gebaseerd op de respectieve interface. HSRP groep 1 gebruikt bijvoorbeeld het HSRP virtuele MAC-adres van 0000.0c07.ac01. Hosts op het aangrenzende LAN-segment maken gebruik van het normale ARP-proces (Address Resolution Protocol) om de gekoppelde MAC-adressen op te lossen.

## ICMP-omleidingen

HSRP-peerrouters die een subnet beschermen kunnen toegang verlenen tot alle andere subnetten in het netwerk. Dit is de basis van HSRP. Daarom maakt het niet uit welke router de actieve HSRP-router wordt. In Cisco IOS-software-releases lager dan Cisco IOS-software-release 12.1(3)T worden ICMP-omleidingen automatisch uitgeschakeld op een interface wanneer HSRP op die interface wordt gebruikt. Zonder deze configuratie kunnen de hosts worden weggeleid van het virtuele IP-adres voor HSRP en omgeleid naar het IP- en MAC-adres van de interface van één router. Redundantie gaat verloren.

Cisco IOS-software introduceert een methode om ICMP-omleidingen met HSRP toe te staan. Deze methode filtert uitgaande ICMP-omleidingsberichten via HSRP. Het IP-adres van de volgende hop wordt gewijzigd in een virtueel adres voor HSRP. Het IP-adres van de gateway in het uitgaande ICMP-omleidingsbericht wordt vergeleken met een lijst van actieve routers met HSRP die op dat netwerk aanwezig zijn. Als de router die overeenkomt met het IP-adres van de gateway een actieve router is voor een HSRP-groep, wordt het IP-adres van de gateway vervangen door het virtuele IP-adres van die groep. Deze oplossing staat hosts toe optimale routes naar externe netwerken te leren en tegelijkertijd de veerkracht te behouden die HSRP biedt.

## Matrix van HSRP-functionaliteit

Raadpleeg de sectie [Cisco IOS-release en matrix van HSRP-functionaliteit](#) in [Kenmerken en functionaliteit van Hot Standby Router Protocol](#) voor meer informatie over de functies en Cisco IOS-software-releases die HSRP ondersteunen.

## HSRP-functies

Raadpleeg [Kenmerken en functionaliteit van Hot Standby Router Protocol](#) voor meer informatie over de HSRP-functies. Dit document bevat informatie over de volgende HSRP-functies:

- Tijdelijke onderbreking
- Interfacetracering
- Gebruik van een BIA

- Meerdere HSRP-groepen
- Configureerbare MAC-adressen
- Syslog-ondersteuning
- HSRP-foutopsporing
- Uitgebreide HSRP-foutopsporing
- Verificatie
- IP-redundantie
- MIB voor Simple Network Management Protocol (SNMP)
- HSRP voor Multiprotocol Label Switching (MPLS)

**Opmerking:** u kunt de zoekfunctie van uw browser gebruiken om deze secties in het document te vinden.

## Indeling van pakketten

Deze tabel toont de notatie van het datagedeelte van het HSRP-frame voor UDP:

<b>Versie</b>	<b>Op-code</b>	<b>Toestand</b>	<b>Hello-tijd</b>
Wachtstandtijd	Prioriteit	Groep	Gereserveerd
Verificatiegegevens			
Verificatiegegevens			
Virtueel IP-adres			

In deze tabel wordt elk veld in het HSRP-pakket beschreven:

<b>Pakketveld</b>	<b>Beschrijving</b>
Op-code (1 octet)	De op-code beschrijft het type bericht dat het pakket bevat. Mogelijke waarden zijn: 0 - hello, 1 - coup en 2 - aftreden. Hello-berichten worden verzonden om aan te geven dat een router HSRP gebruikt en de actieve router kan worden. Coup-berichten worden verzonden wanneer een router de actieve router wil worden. Resign-berichten worden verzonden wanneer een router niet langer de actieve router wil zijn.
Toestand (1 octet)	Elke router in de stand-bygroep implementeert een toestandsautomaat. Het veld Toestand beschrijft de huidige toestand van de router die het bericht verzendt. Dit zijn details over de individuele staten: 0 - initieel, 1 - leren, 2 - luisteren, 4 - spreken, 8 - stand-by, en 16 - actief.
Hello-tijd (1 octet)	Dit veld is alleen nuttig in hello-berichten. Hierin wordt de geschatte tijdsduur tussen o hello-berichten die de router verzendt opgegeven. De tijd wordt in seconden aangegeven.
Wachtstandtijd (1 octet)	Dit veld is alleen nuttig in hello-berichten. Hierin wordt opgegeven hoe lang routers o een hello-bericht wachten voordat ze een toestandswijziging initiëren.
Prioriteit (1 octet)	Dit veld wordt gebruikt om de actieve router en de stand-byrouter te selecteren. Bij e vergelijking van de prioriteiten van twee routers wordt de router met de hoogste wa de actieve router. Bij gelijke prioriteiten wordt de router met het hogere IP-adres de actieve router.
Groep (1 octet)	Dit veld identificeert de stand-bygroep.
Verificatiegegevens (8 octetten)	Dit veld bevat een leesbaar wachtwoord bestaande uit acht tekens.
Virtueel IP-adres (4 octetten)	Als het virtuele IP-adres niet op een router is geconfigureerd, kan het adres uit het hello-bericht van de actieve router worden geleerd. Een adres wordt alleen geleerd a er geen stand-by-IP-adres voor HSRP is geconfigureerd en het hello-bericht is geverifieerd (als verificatie is geconfigureerd).

## HSRP-toestanden

### Toestand Definitie

Initial	Dit is de initiële toestand. Deze toestand geeft aan dat HSRP niet actief is. De toestand wordt ingesteld via een configuratiewijziging of wanneer een interface voor het eerst beschikbaar komt.
Learn	De router heeft het virtuele IP-adres niet bepaald en heeft nog geen geverifieerd hello-bericht van de actieve router gezien. In deze toestand wacht de router nog om van de actieve router te horen.
Listen	De router kent het virtuele IP-adres, maar de router is noch de actieve noch de stand-byrouter. De router luistert naar hello-berichten van deze routers.
Speak	De router verzendt periodieke hello-berichten en neemt actief deel aan de selectie van de actieve en/of stand-byrouter. Een router kan alleen de toestand <code>speak</code> krijgen als deze het virtuele IP-adres heeft.
Standby	De router is kandidaat om de volgende actieve router te worden en verzendt periodieke hello-berichten. Met uitzondering van tijdelijke omstandigheden heeft maximaal één router in de groep de toestand <code>standby</code> .
Active	De router stuurt momenteel pakketten door die naar het virtuele MAC-adres van de groep worden verzonden. De router verzendt periodieke hello-berichten. Met uitzondering van tijdelijke omstandigheden moet maximaal één router in de groep de toestand <code>active</code> hebben.

## HSRP-timers

Elke router gebruikt slechts drie timers in HSRP. De timers timen hello-berichten. Het HSRP converteert wanneer een foutstoring optreedt, afhankelijk van de manier waarop de hello-timers en wachtstandtimers zijn geconfigureerd. Deze timers worden standaard respectievelijk ingesteld op 3 en 10 seconden. Dit betekent dat elke 3 seconden een hello-pakket wordt verzonden tussen de HSRP-apparaten in de stand-bygroep en dat het stand-byapparaat actief wordt wanneer gedurende 10 seconden geen hello-pakket is ontvangen. U kunt deze timer-instellingen verlagen om de failover of het voorrang te versnellen, maar om een toename van het CPU-gebruik en onnodige klappen in de stand-by status te voorkomen, dient u de hello-timer niet lager in te stellen dan één (1) seconde of de hold-timer lager dan 4 seconden. Als u het HSRP-traceringsmechanisme gebruikt en de getraceerde link werkt niet, dan zal de failover of tijdelijke onderbreking direct plaatsvinden, ongeacht de hello- en wachtstandtimers. Wanneer een timer afloopt, gaat de router over naar een nieuwe HSRP-toestand. De timers kunnen met deze opdracht worden gewijzigd: **stand-by [group-number] timers hellotime holdtime**. Bijvoorbeeld: **standby 1 timers 5 15**.

Deze tabel geeft meer informatie over deze timers:

Timer	Beschrijving
Actieve timer	Deze timer wordt gebruikt om de actieve router te monitoren. Deze timer start elke keer dat de actieve router een hello-pakket ontvangt. Deze timer verloopt in overeenstemming met de waarde van de wachtstandtijd die in het bijbehorende veld van het hello-bericht voor HSRP is ingesteld.
Stand-bytimer	Deze timer wordt gebruikt om de stand-byrouter te monitoren. De timer start elke keer dat de stand-byrouter een hello-pakket ontvangt. Deze timer verloopt in overeenstemming met de waarde van de wachtstandtijd die in het desbetreffende hello-pakket is ingesteld.
Hello-timer	Deze timer wordt gebruikt om hello-pakketten te timen. Alle HSRP-routers, ongeacht de HSRP-toestand, genereren een hello-pakket wanneer deze hello-timer verloopt.

## HSRP-gebeurtenissen

In deze tabel worden de gebeurtenissen in de eindigetoestandsautomaat voor HSRP

weergegeven:

### Sleutel Gebeurtenissen

- 1 HSRP wordt geconfigureerd op een ingeschakelde interface.
- 2 HSRP wordt uitgeschakeld op een interface of de interface wordt uitgeschakeld.
- 3 Aflopen van actieve timer: De actieve timer is ingesteld op de wachtstandtijd op het moment dat het laatste hello-bericht van de actieve router is ontvangen.
- 4 Aflopen van stand-by-timer: De stand-by-timer is ingesteld op de wachtstandtijd op het moment dat het laatste hello-bericht van de stand-by-router is ontvangen.
- 5 Aflopen van hello-timer: De periodieke timer voor het verzenden van hello-berichten is afgelopen.
- 6 Ontvangst van een hello-bericht van hogere prioriteit van een router in de toestand `Speak`
- 7 Ontvangst van een hello-bericht van hogere prioriteit van de actieve router
- 8 Ontvangst van een hello-bericht van lagere prioriteit van de actieve router
- 9 Ontvangst van een resign-bericht van de actieve router
- 10 Ontvangst van een coup-bericht van een router met hogere prioriteit
- 11 Ontvangst van een hello-bericht van hogere prioriteit van de stand-by-router
- 12 Ontvangst van een hello-bericht van lagere prioriteit van de stand-by-router

### HSRP-acties

Deze tabel specificeert de acties die in het kader van de toestandsautomaat moeten worden uitgevoerd:

#### Letter Actie

- |   |  |
|---|--|
| A | Actieve timer starten—Als deze actie optreedt als het resultaat van het ontvangen van een geverifieerd hello-bericht van de actieve router, wordt de actieve timer ingesteld op het veld Tijd in het hello-bericht. In alle andere gevallen wordt de actieve timer ingesteld op de huidige waarde van de wachtstandtijd door deze router wordt gebruikt. Vervolgens start de actieve timer.  |
| B | Start stand-by timer—Als deze actie optreedt als resultaat van het ontvangen van een geverifieerd bericht van de standby-router, wordt de standby-timer ingesteld op het veld wachtstandtijd in het hello-bericht. In alle andere gevallen wordt de stand-by-timer ingesteld op de huidige waarde van de wachtstandtijd door deze router wordt gebruikt. Vervolgens start de stand-by-timer. |
| C | Stop actieve timer: De actieve timer stopt.  |
| D | Stop stand-by-timer: De standby-timer stopt.   |
| E | Leer parameters: Deze actie wordt uitgevoerd wanneer een geverifieerd bericht van de actieve router wordt ontvangen. Als het virtuele IP-adres voor deze groep niet handmatig is geconfigureerd, kan het virtuele IP-adres uit het bericht worden geleerd. De router kan de hello-tijd en de waarden van de wachtstandtijd leren uit het bericht.  |
| F | Verzend hello-bericht: De router verzendt een hello-bericht met zijn huidige toestand, hello-tijd, en wachtstandtijd.  |
| G | Verzend coup-bericht: De router verzendt een coup-bericht om de actieve router te informeren dat een router met hogere prioriteit beschikbaar is.  |
| H | Verzend resign-bericht: De router verzendt een resign-bericht om een andere router de mogelijkheid te geven om de actieve router te worden.  |
| I | Verzend gratis ARP-bericht: De router zendt een ARP-responspakket uit dat de virtuele IP- en MAC-adressen van de groep aanbiedt. Het pakket wordt verzonden met het virtuele MAC-adres als het binaire MAC-adres in de header van de koppelingslaag en binnen het ARP-pakket.  |

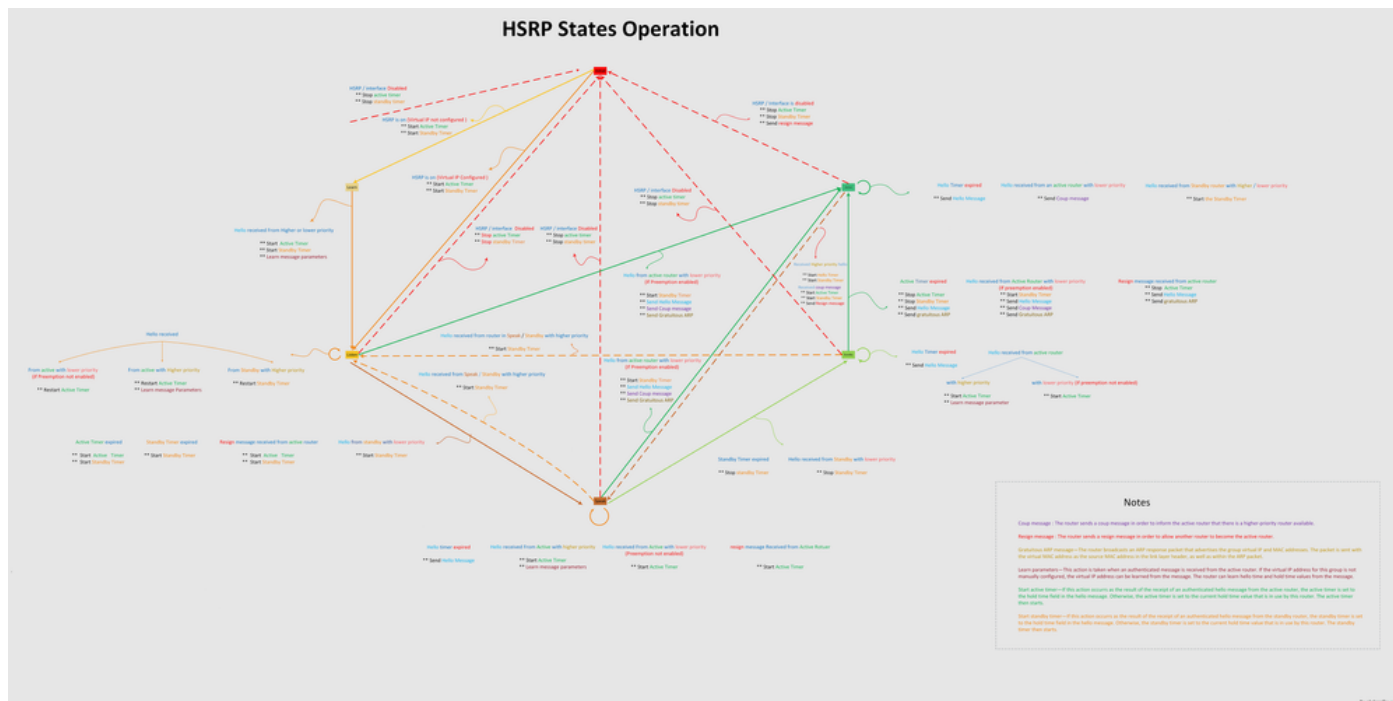
### HSRP-toestandstabel

In het schema in deze sectie worden de toestandsovergangen van de HSRP-toestandsautomaat weergegeven. Elke keer dat een gebeurtenis zich voordoet, vindt de bijbehorende actie plaats en

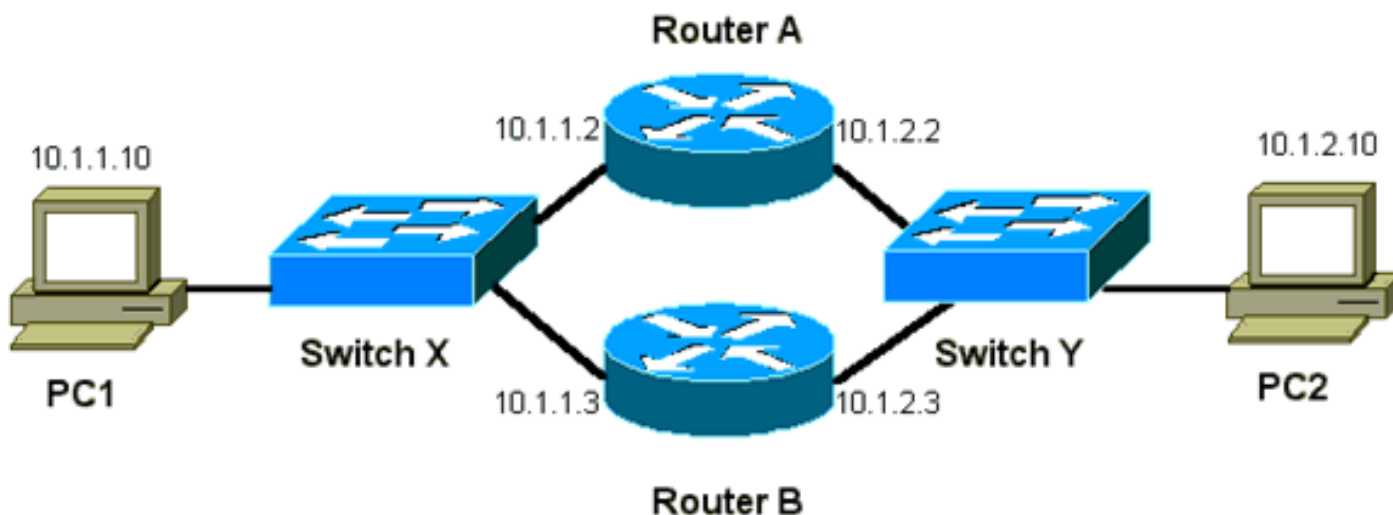


zal de router overgaan in de volgende HSRP-toestand. De getallen in het schema staan voor de gebeurtenissen en de letters staan voor de bijbehorende actie. In de tabel in de sectie [HSRP-gebeurtenissen](#) worden de getallen gedefinieerd en in de tabel in de sectie [HSRP-acties](#) worden de letters gedefinieerd. Gebruik dit schema uitsluitend ter referentie. Het diagram is gedetailleerd en is niet nodig voor algemene probleemoplossingsdoeleinden.

Zie Werking van HSRP-toestanden voor een gedetailleerde afbeelding van het schema.



## Pakketstroom



Apparaat	MAC-adres	IP-adres	Subnetmasker	Standaardgateway
PC1	0000.0c00.0001	10.1.1.10	255.255.255.0	10.1.1.1
PC2	0000.0c00.1110	10.1.2.10	255.255.255.0	10.1.2.1

## Configuratie van router A (actieve router)

```
interface GigabitEthernet 0/0
 ip address 10.1.1.2 255.255.255.0
 mac-address 4000.0000.0010
 standby 1 ip 10.1.1.1
 standby 1 priority 200
```

```
interface GigabitEthernet 0/1 ip address 10.1.2.2 255.255.255.0 mac-address 4000.0000.0011
 standby 1 ip 10.1.2.1 standby 1 priority 200
```

### Configuratie van router B (stand-byrouter)

```
interface GigabitEthernet 0/0
 ip address 10.1.1.3 255.255.225.0
 mac-address 4000.0000.0020
 standby 1 ip 10.1.1.1
```

```
interface GigabitEthernet 0/1 ip address 10.1.2.3 255.255.255.0 mac-address 4000.0000.0021
 standby 1 ip 10.1.2.1
```

**Opmerking:** deze voorbeelden configureren statische MAC-adressen alleen voor illustratiedoeleinden. Configureer geen statische MAC-adressen tenzij dit echt moet.

U moet het concept achter pakketstroom begrijpen wanneer u snuffelsporen verkrijgt om problemen met HSRP op te lossen. Router A gebruikt prioriteit 200 en wordt de actieve router op beide interfaces. In het voorbeeld in deze sectie hebben pakketten van de router die bestemd zijn voor een hostwerkstation, het bron-MAC-adres van het fysieke MAC-adres (BIA) van de router. Pakketten van de hostcomputers die bestemd zijn voor het IP-adres voor HSRP hebben het bestemmings-MAC-adres van het virtuele MAC-adres voor HSRP. Houd er rekening mee dat de MAC-adressen niet hetzelfde zijn voor elke stroom tussen de router en de host.

Deze tabel toont de MAC-adressen met bijbehorende IP-adressen per stroom op basis van een sniffer-trace die op Switch X wordt uitgevoerd.

Pakketstroom	Bron-MAC	Bestemmings-MAC	Bron-IP	Bestemming
Pakketten van PC1 die bestemd zijn voor PC2	PC1 (0000.0c00.0001)	Virtueel MAC-adres voor HSRP van interface Ethernet 0 van router A (0000.0c07.ac01)	10.1.1.10	10.1.2.10
Pakketten die via Router A van PC2 terugkeren en bestemd zijn voor PC1	BIA van Ethernet 0 van router A (4000.0000.0010)	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.10
Pakketten van PC1 die bestemd zijn voor het stand-by-IP-adres voor HSRP (ICMP, Telnet)	PC1 (0000.0c00.0001)	Virtueel MAC-adres voor HSRP van interface Ethernet 0 van router A (0000.0c07.ac01)	10.1.1.10	10.1.1.1
Pakketten die bestemd zijn voor het daadwerkelijke IP-adres van de actieve router (ICMP, Telnet)	PC1 (0000.0c00.0001)	BIA van Ethernet 0 van router A (4000.0000.0010)	10.1.1.10	10.1.1.2
Pakketten die bestemd zijn voor het statische IP-adres van de stand-byrouter (ICMP, Telnet)	PC1 (0000.0c00.0001)	BIA van Ethernet 0 van Router B (4000.0000.0020)	10.1.1.10	10.1.1.3

# Casestudy's voor troubleshooting van HSRP

## Case Study #1: HSRP Standby IP-adres wordt als dubbel IP-adres gemeld

De volgende foutmeldingen kunnen worden weergegeven:

```
Oct 12 13:15:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 13 16:25:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:31:02: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:41:01: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
```

Deze foutmeldingen duiden niet noodzakelijkerwijs op een HSRP-probleem. De foutmeldingen duiden eerder op een mogelijke STP-lus (Spanning Tree Protocol) of een probleem in de router- of switchconfiguratie. De foutmeldingen zijn slechts symptomen van een ander probleem.

Bovendien wordt door deze foutmeldingen de juiste werking voor HSRP niet gehinderd. Het dubbele HSRP-pakket wordt genegeerd. Deze foutmeldingen worden met tussenpozen van 30 seconden onderdrukt. Maar matige netwerkprestaties en pakketverlies kunnen het gevolg zijn van de netwerkinstabiliteit die de foutmeldingen `STANDBY-3-DUPADDR` voor het HSRP-adres veroorzaakt.

Deze berichten wijzen er specifiek op dat de router een gegevenspakket heeft ontvangen dat afkomstig was van het HSRP IP-adres op VLAN 25 met de MAC-adressen 0000.0c07.ac19. Aangezien het MAC-adres van HSRP 0000.0c07.ac19 is, ontving de router in kwestie zijn eigen pakketback of beide routers in de HSRP-groep gingen naar de `actieve` staat. Omdat de router zijn eigen pakket heeft ontvangen, ligt het probleem waarschijnlijk eerder bij het netwerk dan bij de router. Een verscheidenheid aan problemen kan dit gedrag veroorzaken. De mogelijke netwerkproblemen die de foutmeldingen veroorzaken, zijn onder meer:

- Kortstondige STP-lussen
- Problemen met de EtherChannel-configuratie
- Gedupliceerde frames

Wanneer u deze foutmeldingen oplost, raadpleegt u de stappen voor probleemoplossing in de sectie [Problemen oplossen HSRP in Catalyst Switches](#) van dit document. Alle probleemoplossingsmodules zijn van toepassing op deze sectie, die modules voor configuratie bevat. Let bovendien op fouten in het logbestand van de switch en raadpleeg zo nodig verdere casestudy's.

U kunt een toegangslijst gebruiken om te voorkomen dat de actieve router zijn eigen multicast hello-pakket ontvangt. Maar dit is slechts een tijdelijke oplossing voor de foutmeldingen en verbergt zelfs het symptoom van het probleem. De tijdelijke oplossing is het toepassen van een uitgebreide inkomende toegangslijst op de HSRP-interfaces. De toegangslijst blokkeert al het verkeer dat van het fysieke IP-adres afkomstig is en dat bestemd is voor multicast adres 224.0.0.2 van alle routers.

```
access-list 101 deny ip host 172.16.12.3 host 224.0.0.2
access-list 101 permit ip any any
```

```
interface GigabitEthernet 0/0
```

```
ip address 172.16.12.3 255.255.255.0
standby 1 ip 172.16.12.1
ip access-group 101 in
```

## Case Study #2: HSRP-status verandert voortdurend (actief, stand-by, spreken) of %HSRP-6-STATUS

De volgende foutmeldingen kunnen worden weergegeven:

```
Jan 9 08:00:42.623: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:00:56.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:03.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
Jan 9 08:01:29.427: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:01:36.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:43.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
```

```
Jul 29 14:03:19.441: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active Jul 29 16:27:04.133: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak Jul 29 16:31:49.035: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby
```

Deze foutmeldingen beschrijven een situatie waarin een stand-by HSRP-router geen drie opeenvolgende hello-pakketten voor HSRP van zijn HSRP-peer heeft ontvangen. De output toont dat de stand-by-router overgaat van de toestand `standby` naar de toestand `active`. Kort daarna keert de router terug naar de toestand `standby`. Tenzij deze foutmelding tijdens de eerste installatie optreedt, wordt de foutmelding waarschijnlijk niet veroorzaakt door een HSRP-probleem. De foutmeldingen duiden op het verlies van hello-pakketten voor HSRP tussen de peers. Wanneer u dit probleem troubleshoot, moet u de communicatie tussen de HSRP-peers verifiëren. Een willekeurig, tijdelijk verlies van datacommunicatie tussen de peers is het meest gangbare probleem dat tot deze berichten leidt. Veranderingen in de HSRP-toestand zijn vaak het gevolg van hoog CPU-gebruik. Als de foutmelding het gevolg is van een hoog CPU-gebruik, zet dan een sniffer op het netwerk en traceer het systeem dat het hoge CPU-gebruik veroorzaakt.

Er zijn verschillende mogelijke oorzaken voor het verlies van HSRP-pakketten tussen de peers. De meest gangbare problemen zijn [problemen met de fysieke laag](#), overmatig netwerkverkeer veroorzaakt door [Spanning Tree-problemen](#) of overmatig verkeer veroorzaakt door elk VLAN. Zoals bij [Case Study #1](#), zijn alle probleemoplossingsmodules van toepassing op de resolutie van HSRP-statuswijzigingen, met name op [Layer 3 HSRP-debugging](#).

Als het verlies voor HSRP-pakketten tussen peers het gevolg is van overmatig verkeer veroorzaakt door elk VLAN, zoals hierboven vermeld, dan kunt u de omvang van de Selective Packet Discard (SPD) en de wachtrij afstellen of vergroten om het afwijsp probleem van de invoerwachtrij te verhelpen.

Om de grootte van de Selective Packet Discard (SPD) te verhogen, ga naar de configuratiemodus en voer deze opdrachten uit op de Cat6500-switches:

```
(config)#ip spd queue max-threshold 600
```

```
!--- Hidden Command
```

```
(config)#ip spd queue min-threshold 500
```

```
!--- Hidden Command
```

Als u de omvang van de wachtrij wilt vergroten, gaat u naar de VLAN-interfacemodus en voert u deze opdracht uit:

```
(config-if)#hold-queue 500 in
```

Nadat u de grootte van de SPD en wachtrij hebt verhoogd, kunt u de interfacetellers wissen als u de opdracht voor de `duidelijke` teller-interface uitvoert.

### Case Study #3: HSRP herkent peer niet

De routeroutput in deze sectie toont een router die voor HSRP is geconfigureerd, maar zijn HSRP-peers niet herkent. Hiervoor moet de router geen hello-pakketten voor HSRP van de naburige router ontvangen. Zie de sectie [Connectiviteit van fysieke laag verifiëren](#) en de sectie [Configuratie van HSRP-routers verifiëren](#) van dit document voor het troubleshooten van dit probleem. Als de connectiviteit van de fysieke laag in orde is, controleer dan op verschillen in VTP-modus.

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

### Case Study #4: Veranderingen in HSRP-status en rapporten van de Switch SYS-4-P2\_WARN: 1/Host <mac\_address> knippert tussen poort <poort\_1> en poort <poort\_2> in Syslog

De volgende foutmeldingen kunnen worden weergegeven:

```
2001 Jan 03 14:18:43 %SYS-4-P2_WARN: 1/Host 00:00:0c:14:9d:08
  is flapping between port 2/4 and port 2/3
```

```
Feb 4 07:17:44 AST: %SW_MATM-4-MACFLAP_NOTIF: Host 0050.56a9.1f28 in vlan 1027 is flapping between port Te1/0/7 and
port Te2/0/2
```

In Catalyst Switches rapporteert de switch een host MAC-adres dat wordt verplaatst als het host MAC-adres twee keer binnen 15 seconden wordt verplaatst. Een mogelijke oorzaak is een STP-lus. De switch gooit gedurende ongeveer 15 seconden pakketten van deze host weg in een poging de impact van een STP-lus te minimaliseren. Als de gemelde MAC-adresverplaatsing tussen twee poorten het virtuele MAC-adres voor HSRP betreft, is het probleem waarschijnlijk dat beide HSRP-routers naar de toestand `active` overgaan.

Als het gemelde MAC-adres niet het virtuele MAC-adres voor HSRP is, kan het probleem een lus, duplicatie of terugkaatsing van pakketten in het netwerk zijn. Dergelijke omstandigheden kunnen bijdragen aan HSRP-problemen. De meest gangbare oorzaken voor het verplaatsen van MAC-adressen zijn [Spanning Tree-problemen](#) of [problemen met de fysieke laag](#).

Voor het troubleshooten van deze foutmelding voert u de volgende stappen uit:

**Opmerking:** voltooi ook de stappen in de sectie [Problemen oplossen in HSRP in Catalyst Switches](#) van dit document.

1. Bepaal de juiste bron (poort) van het host-MAC-adres.
2. Koppel de poort los die niet het MAC-adres van de host mag genereren.
3. Noteer de STP-topologie per VLAN en controleer op STP-fouten.
4. Verifieer de configuratie van de poortkanalen. Een onjuiste configuratie van poortkanalen kan tot een fluctuatie van foutmeldingen door het host-MAC-adres leiden. Dit komt door de taakverdeling die standaard plaatsvindt bij gebruik van poortkanalen.

## Case Study #5: asymmetrische routing en HSRP (buitensporige overstroming van Unicast-verkeer in netwerk met routers die HSRP uitvoeren)

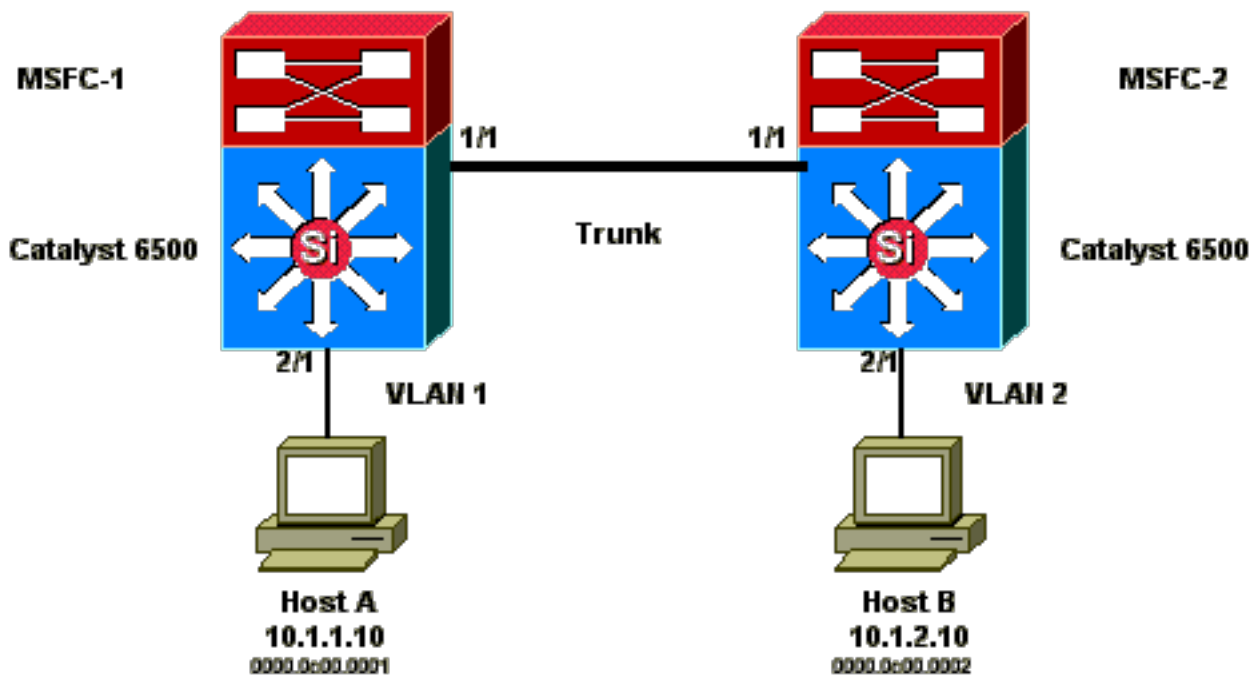
Met asymmetrische routing gebruiken, verzenden en ontvangen pakketten verschillende paden tussen een host en de peer waarmee het communiceert. Deze pakketstroom is een resultaat van de configuratie van taakverdeling tussen HSRP-routers, op basis van HSRP-prioriteit, waarbij de HSRP op actief of stand-by wordt ingesteld. Dit type pakketstroom in een switching-omgeving kan overmatige, onbekende unicast flooding tot gevolg hebben. Ook kunnen de MLS-vermeldingen (Multilayer Switching) afwezig zijn. Onbekende unicast flooding treedt op wanneer de switch een unicast pakket via alle poorten verzendt. De switch verzendt het pakket via alle poorten omdat er geen bestemmings-MAC-adres is. Dit gedrag verstoort de connectiviteit niet, omdat pakketten nog steeds worden doorgestuurd. Maar dit gedrag is niet de reden voor de flooding van extra pakketten via hostpoorten. Deze casestudy onderzoekt het gedrag van asymmetrische routing en waarom dit leidt tot unicast flooding.

Symptomen van asymmetrische routing omvatten:

- Overmatige flooding van unicast pakketten
- Ontbreken van MLS-vermelding voor stromen
- Sniffer-trace die laat zien dat pakketten op de hostpoort niet voor de host bestemd zijn
- Verhoogde netwerklatentie met L2-gebaseerde packet rewrite engines, zoals taakverdelers voor servers, webcache-apparaten en netwerkapplicaties. Voorbeelden zijn onder andere de Cisco LocalDirector en Cisco Cache Engine.
- Afgewezen pakketten op verbonden hosts en werkstations die niet in staat zijn de extra verkeersbelasting van unicast flooding af te handelen

**Opmerking:** de standaard ARP cache verouderingstijd op een router is vier uur. De standaard verouderingstijd van de CAM-vermelding (content-addressable memory) van de switch is vijf minuten. De ARP verouderingstijd van de host werkstations is niet significant voor deze discussie, maar het voorbeeld stelt de ARP verouderingstijd in op vier uur.

Dit schema geeft het probleem weer. Dit topologievoorbeeld bestaat uit twee Catalyst 6500's met MSFC's (functiekaart voor meerlaagse switch) in elke switch. Hoewel dit voorbeeld MSFC's gebruikt, kunt u in plaats van de MSFC ook een router gebruiken. Voorbeelden van routers die u kunt gebruiken zijn onder andere de routeswitch-module (RSM), Gigabit-switchrouter (GSR) en Cisco 7500. De hosts zijn rechtstreeks verbonden met de poorten op de switch. De switches zijn onderling verbonden via een trunk die verkeer voor VLAN 1 en VLAN 2 verwerkt.



Deze outputs zijn fragmenten van de configuratie met de opdracht **show standby** voor elke MSFC.

## MSFC1

```
interface Vlan 1
 mac-address 0003.6bf1.2a01
 ip address 10.1.1.2 255.255.255.0
 no ip redirects
 standby 1 ip 10.1.1.1
 standby 1 priority 110
```

```
interface Vlan 2
 mac-address 0003.6bf1.2a01
 ip address 10.1.2.2 255.255.255.0
 no ip redirects
 standby 2 ip 10.1.2.1
```

```
MSFC1#show standby
Vlan1 - Group 1
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.696
Hot standby IP address is 10.1.1.1 configured
Active router is local
Standby router is 10.1.1.3 expires in 00:00:07
Standby virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:20:40
Vlan2 - Group 2
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.776
Hot standby IP address is 10.1.2.1 configured
Active router is 10.1.2.3 expires in 00:00:09, priority 110
Standby router is local
4 state changes, last state change 00:00:51
MSFC1#exit
Console> (enable)
```

## MSFC2

```
interface Vlan 1
 mac-address 0003.6bf1.2a02
 ip address 10.1.1.3 255.255.255.0
 no ip redirects
 standby 1 ip 10.1.1.1
```

```
interface Vlan 2
 mac-address 0003.6bf1.2a02
 ip address 10.1.2.3 255.255.255.0
 no ip redirects
 standby 2 ip 10.1.2.1
 standby 2 priority 110
```

```
MSFC2#show standby
Vlan1 - Group 1
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.242
Hot standby IP address is 10.1.1.1 configured
Active router is 10.1.1.2 expires in 00:00:09, priority 110
Standby router is local
7 state changes, last state change 00:01:17
Vlan2 - Group 2
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.924
Hot standby IP address is 10.1.2.1 configured
Active router is local
Standby router is 10.1.2.2 expires in 00:00:09
Standby virtual mac address is 0000.0c07.ac02
2 state changes, last state change 00:40:08
MSFC2#exit
```

**Opmerking:** op MSFC1 bevindt VLAN 1 zich in de *actieve* staat HSRP en is VLAN 2 in de *stand-by* staat HSRP. Op MSFC2 is VLAN 2 in de *active* HSRP-toestand en VLAN 1 in de HSRP-toestand *standby*. De standaardgateway van elke host is het desbetreffende stand-by-IP-adres.

1. Aanvankelijk zijn alle caches leeg. Host A gebruikt MSFC1 als zijn standaardgateway. Host B gebruikt MSFC2.**ARP- en MAC-adrestabellen voordat ping is geïnitieerd** **Opmerking:** Kort gezegd zijn de Switch 1 MAC-adressen voor de router HSRP en MAC-adressen niet opgenomen in de andere tabellen die in deze sectie worden weergegeven.
2. Host A pingt host B, wat betekent dat host A een ICMP-echopakket verzendt. Omdat elke host zich op een aparte VLAN bevindt, stuurt host A zijn pakketten die bedoeld zijn voor host B door naar zijn standaardgateway. Om dit proces te laten plaatvinden, moet host A een ARP-verzoek verzenden om het MAC-adres 10.1.1.1 van zijn standaardgateway om te zetten.**ARP- en MAC-adrestabellen nadat host A ARP voor standaardgateway verzendt**
3. MSFC1 ontvangt het pakket, herschrijft het en stuurt het door naar host B. Om het pakket te herschrijven verzendt MSFC1 een ARP-aanvraag voor host B, omdat de host zich in een rechtstreeks verbonden interface bevindt. MSFC2 heeft nog geen pakketten in deze stroom ontvangen. Wanneer MSFC1 het ARP-antwoord van host B ontvangt, weten beide switches welke bronpoort aan host B is gekoppeld.**ARP- en MAC-adrestabellen nadat Host A het pakket naar de standaardgateway heeft verzonden en MSFC1 een ARP heeft verzonden voor Host B**
4. Host B ontvangt het echopakket van host A, via MSFC1. Host B moet nu een echoantwoord



verzenden naar host A. Aangezien host A zich op een ander VLAN bevindt, zal host B het antwoord doorsturen via zijn standaardgateway, MSFC2. Om het pakket door MSFC2 te versturen moet host B een ARP verzenden voor zijn standaard gateway IP-adres, 10.1.2.1. **ARP- en MAC-adrestabellen nadat host B ARP voor de standaardgateway heeft verzonden**

5. Host B stuurt nu het echo-antwoordpakket naar MSFC2. MSFC2 verzendt een ARP verzoek om host A omdat het direct verbonden is op VLAN 1. Switch 2 vult zijn MAC-adrestabel in met het MAC-adres van host B. **ARP- en MAC-adrestabellen nadat het echo-pakket is ontvangen door host A**
6. Het echo-antwoord bereikt host A en de stroom is voltooid.

## Gevolgen van asymmetrische routing

Neem het geval van het ononderbroken pingen van host B door host A. Denk eraan dat de host A het echo-pakket aan MSFC1 verzendt en host B het echo-antwoord verzendt naar MSFC2, die in een asymmetrische routertoestand is. De enige tijd dat Switch 1 de bron-MAC van host B leert is wanneer host B reageert op een ARP-verzoek van MSFC1. Dit komt doordat host B MSFC2 als standaardgateway gebruikt en geen pakketten naar MSFC1 en bijgevolg naar Switch 1 stuurt. Aangezien de ARP timeout standaard vier uur is, verouderd Switch 1 het MAC-adres van host B na vijf minuten standaard. Switch 2 leeftijden gastheer A na vijf minuten. Daardoor moet Switch 1 elk pakket met host B als bestemmings-MAC-adres als een onbekende unicast behandelen. De switch verzendt het pakket van host A dat bestemd is voor host B via alle poorten. Bovendien is er, omdat er geen MAC-adresvermelding voor host B is in Switch 1, ook geen MLS-vermelding.

## ARP- en MAC-adrestabellen na 5 minuten ononderbroken pingen van host B door host A

ARP-tabel van host A	MAC-adrestabel van Switch 1: MAC VLAN Poort	ARP-tabel van MSFC1	ARP-tabel van MSFC2	MAC-adrestabel van switch 2: MAC VLAN Poort	ARP-tabel van host B
10.1.1.1 : 000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 000.0001	10.1.2.10 0000.0c00.0002 2/1	0000.0c00.0002 2	10.1.2.2 : 003.6bf1.2a01
10.1.1.3 : 003.6bf1.2a0		10.1.2.10 : 000.0001	10.1.1.10 0000.0c00.0001		10.1.2.1 : 000.0c07.ac01

De echo antwoordpakketten die van host B komen ervaren dezelfde kwestie na de MAC-adresingang voor host A-leeftijden op Switch 2. Host B stuurt het echoantwoord door naar MSFC2, dat op zijn beurt het pakket routeert en het op VLAN 1 verstuurt. De switch heeft geen ingangshost A in de MAC-adrestabel en moet het pakket uit alle poorten in VLAN 1 overspoelen.

Asymmetrische routingproblemen verbreken de connectiviteit niet. Maar asymmetrische routing kan leiden tot overmatige unicast flooding en ontbrekende MLS-vermeldingen. Er zijn drie configuratiewijzigingen die deze situatie kunnen verhelpen:

- Stel de MAC-verouderingstijd op de respectievelijke switches in op 14.400 seconden (vier uur) of langer.
- Wijzig de ARP-time-out op de routers naar vijf minuten (300 seconden).
- Verander de MAC-verouderingstijd en ARP-time-out naar dezelfde time-outwaarde.

De beste methode is om de MAC-verouderingstijd te veranderen naar 14.400 seconden. Dit zijn

de configuratierichtlijnen:

- Cisco IOS-software: **MAC-adrestabel verouderingstijd <seconden> VLAN <vlan\_id>**

## Case Study #6: HSRP virtueel IP-adres wordt als een ander IP-adres gemeld

De foutmelding `STANDBY-3-DIFFVIP1` treedt op wanneer er lekkage tussen VLAN's is vanwege overbruggingslussen in de switch.

Als u deze foutmelding krijgt en er lekkage tussen VLAN's is vanwege overbruggingslussen in de switch, volg dan deze stappen om de fout te verhelpen:

1. Identificeer het pad dat de pakketten tussen de eindknooppunten nemen. Als zich een router op dit pad bevindt, voer dan de volgende stappen uit: Troubleshoot het pad van de eerste switch naar de router. Troubleshoot het pad van de router naar de tweede switch.
2. Maak verbinding met elke switch op het pad en controleer de status van de poorten die op het pad tussen de eindknooppunten worden gebruikt.

## Case Study #7: HSRP veroorzaakt schending van MAC op een beveiligde poort

Wanneer poort security is geconfigureerd op de switchpoorten die zijn verbonden met de HSRP-routers, veroorzaakt dit een MAC-schending omdat u niet hetzelfde beveiligde MAC-adres op meer dan één interface kunt hebben. Een security schending op een beveiligde poort vindt plaats in een van de volgende situaties:

- Het maximumaantal beveiligde MAC-adressen wordt aan de adrestabel toegevoegd en een station waarvan het MAC-adres niet in de adrestabel staat probeert toegang te krijgen tot de interface.
- Een adres dat is geleerd of geconfigureerd op de ene beveiligde interface wordt gezien op een andere beveiligde interface in hetzelfde VLAN.

Een schending van de poort security zorgt er standaard voor dat de interface van de switch direct wordt uitgeschakeld wegens een fout. Dit blokkeert de HSRP-statusberichten tussen de routers.

### Tijdelijke oplossing

- Gebruik de opdracht **standby use-bia** op de routers. Dit dwingt de routers om het ingebrande adres voor het HSRP te gebruiken in plaats van het virtuele MAC-adres.
- Schakel poort security uit op de switchpoorten die verbonden zijn met de HSRP-routers.

## Case Study #9: %interface hardware kan geen meerdere groepen ondersteunen

Als meerdere HSRP-groepen op dezelfde interface worden gemaakt, wordt de volgende foutmelding weergegeven:

```
%Interface hardware cannot support multiple groups
```

Deze foutmelding is het gevolg van de hardwarebeperkingen van bepaalde routers of switches. Het is niet mogelijk om deze beperking te verhelpen via software. Het probleem is namelijk dat elke HSRP-groep een extra MAC-adres op de interface gebruikt. Om meerdere HSRP-groepen mogelijk te maken, moet de Ethernet-MAC-chip dus meerdere programmeerbare MAC-adressen ondersteunen.

De tijdelijke oplossing is om de interface-configuratieopdracht **standby use-bia** te gebruiken. Deze gebruikt het ingebrande adres (BIA) van de interface als het virtuele MAC-adres, in plaats van het vooraf toegewezen MAC-adres.

## Probleemoplossing voor HSRP in Catalyst Switches

### A. Configuratie van HSRP-routers verifiëren

#### 1. Uniek IP-adres van routerinterface verifiëren

Verifieer of elke HSRP-router per interface een uniek IP-adres heeft voor elk subnet. Verifieer ook of elke interface het lijnprotocol `up` heeft. Gebruik de opdracht **show ip interface brief** om de huidige toestand van elke interface snel te verifiëren. Hierna volgt een voorbeeld:

```
Router_1#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.1 YES manual up up Vlan10 192.168.10.1 YES manual up up Vlan11 192.168.11.1 YES manual up up
```

```
Router_2#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.2 YES manual up up Vlan10 192.168.10.2 YES manual up up Vlan11 192.168.11.2 YES manual up up
```

#### 2. Stand-by-IP-adressen (HSRP) en stand-bygroepsnummers verifiëren

Verifieer of de geconfigureerde stand-by-IP-adressen (HSRP) en stand-bygroepsnummers overeenkomen met elke router die deelneemt via het HSRP. Een mismatch tussen stand-bygroepen of stand-by-adressen voor HSRP kan HSRP-problemen veroorzaken. De opdracht **show standby** toont de configuratie van de stand-bygroep en het stand-by-IP-adres van elke interface. Hierna volgt een voorbeeld:

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:01:34 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.144 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec) Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:00:27 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.096 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec) Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1 Router_2#show standby Vlan10 - Group 110 State is Standby 1 state change, last state change 00:03:15 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.088 secs Preemption disabled Active router is 192.168.10.1, priority 110 (expires in 11.584 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Standby 1 state change, last state change 00:02:53 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.352 secs Preemption disabled Active router is 192.168.11.1, priority 110 (expires in 9.120 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

#### 3. Verifiëren of stand-by-IP-adres (HSRP) per interface verschilt

Verifieer of het stand-by-IP-adres (HSRP) uniek is: anders dan het geconfigureerde IP-adres op elke interface. Met de opdracht **show standby** kan deze informatie snel worden getoond. Hierna volgt een voorbeeld:

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:01:34 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1
```

default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.144 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec) Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:00:27 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.096 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec) Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1 Router\_2#show standby Vlan10 - Group 110 State is Standby 1 state change, last state change 00:03:15 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.088 secs Preemption disabled Active router is 192.168.10.1, priority 110 (expires in 11.584 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Standby 1 state change, last state change 00:02:53 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.352 secs Preemption disabled Active router is 192.168.11.1, priority 110 (expires in 9.120 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1

#### 4. Wanneer u de opdracht 'standby use-bia' moet gebruiken

Gebruik de opdracht **standby use-bia** uitsluitend in bijzondere omstandigheden, tenzij het HSRP op een Token Ring-interface is geconfigureerd. Deze opdracht vertelt de router om zijn BIA te gebruiken voor de HSRP-groep in plaats van het virtuele MAC-adres voor HSRP. Op een Token Ring-netwerk kan de nieuwe actieve router, als Source-Route Bridging (SRB) wordt gebruikt, met de opdracht **standby use-bia** de RIF-cache (routinginformatieveld) van de host updaten met een gratis ARP-bericht. Maar niet alle host-implementaties verwerken het gratis ARP-bericht op de juiste manier. Een ander aandachtspunt voor de opdracht **standby use-bia** betreft proxy-ARP. Een stand-by-router kan de verloren proxy-ARP-database van de vastgelopen actieve router niet opvangen.

#### 5. Configuratie van toegangslijsten verifiëren

Verifieer of de toegangslijsten die op alle HSRP-peers zijn geconfigureerd geen van de HSRP-adressen filteren die op hun interfaces zijn geconfigureerd. Verifieer met name het multicast adres dat wordt gebruikt om verkeer naar alle routers op een subnet (**224.0.0.2**) te verzenden. Verifieer ook of het UDP-verkeer dat voor de HSRP-poort **1985** is bestemd, niet wordt gefilterd. HSRP gebruikt dit adres en deze poort voor het verzenden van hello-pakketten tussen peers. Gebruik de opdracht **show access-lists** om snel de toegangslijsten te bekijken die op de router zijn geconfigureerd. Hierna volgt een voorbeeld:

```
Router_1#show access-lists
Standard IP access list 77
    deny 10.19.0.0, wildcard bits 0.0.255.255
    permit any
Extended IP access list 144
    deny pim 238.0.10.0 0.0.0.255 any
    permit ip any any (58 matches)
```

## B. Fast EtherChannel- en trunking-configuratie bij Catalyst verifiëren

### 1. Trunking-configuratie verifiëren

Verifieer de trunking-configuraties op de routers en switches als een trunk wordt gebruikt om de HSRP-routers te verbinden. Er zijn vijf mogelijke trunking-modi:

- on

- desirable
- auto
- off
- nonegotiate

Verifieer of de trunking-modi zijn geconfigureerd om de gewenste trunking-methode te bieden.

Gebruik de configuratie `desirable` voor verbindingen van switch naar switch wanneer u HSRP-problemen troubleshoot. Deze configuratie kan problemen isoleren waarbij switchpoorten geen correcte trunks tot stand kunnen brengen. Stel een router-naar-switchconfiguratie in op `nonegotiate`, omdat de meeste Cisco IOS-routers onderhandeling van een trunk niet ondersteunen.

Controleer voor de trunkingmodus IEEE 802.1Q (`dot1q`) dat beide kanten van de trunk zijn geconfigureerd om hetzelfde native VLAN en dezelfde insluiting te gebruiken. Omdat Cisco-producten het native VLAN niet standaard taggen, leidt een mismatch tussen de configuraties van native VLAN's tot geen connectiviteit op deze VLAN's. Verifieer tot slot dat de trunk is geconfigureerd om de VLAN's die op de router zijn geconfigureerd te verwerken en verifieer of de VLAN's niet zijn verwijderd via pruning en in de STP-toestand verkeren voor poorten die met de router verbonden zijn. Geef de opdracht **show interfaces <interface> trunk uit** voor een snelle verwijzing die deze informatie toont. Hierna volgt een voorbeeld:

```
L2Switch_1#show interfaces gigabitEthernet1/0/13 trunk Port Mode Encapsulation Status Native vlan Gi1/0/13 on 802.1q trunking
1 Port Vlans allowed on trunk Gi1/0/13 1-4094 Port Vlans allowed and active in management domain Gi1/0/13 1,10-11,70,100,300-
309 Port Vlans in spanning tree forwarding state and not pruned Gi1/0/13 1,10-11,70,100,300-309
Router_1#show interfaces gigabitEthernet1/0/1 trunk Port Mode Encapsulation Status Native vlan Gi1/0/1 on 802.1q trunking 1
Port Vlans allowed on trunk Gi1/0/1 1-4094 Port Vlans allowed and active in management domain Gi1/0/1 1,10-
11,100,206,301,307,401,900,3001-3002 Port Vlans in spanning tree forwarding state and not pruned Gi1/0/1 1,10-
11,100,206,301,307,401,900,3001-3002
```

## 2. Fast EtherChannel-configuratie (poortkanalen) verifiëren

Verifieer de EtherChannel-configuratie op beide routers en switches als een poortkanaal wordt gebruikt om de HSRP-routers te verbinden. Configureer aan tenminste één kant een poortkanaal van switch naar switch als `desirable`. De andere kant kan in een van deze modi staan:

- on
- desirable
- auto

In dit voorbeeld zijn interfaces echter geen lid van een poortkanaal:

```
Router_1#show etherchannel summary Flags: D - down P - bundled 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 M - not in use, minimum links not met u - unsuitable
for bundling w - waiting to be aggregated d - default port A - formed by Auto LAG Number of channel-groups in use: 0 Number of
aggregators: 0 Group Port-channel Protocol Ports -----+-----+-----+----- Router_1#
Router_2#show etherchannel summary Flags: D - down P - bundled 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 M - not in use, minimum links not met u - unsuitable
for bundling w - waiting to be aggregated d - default port A - formed by Auto LAG Number of channel-groups in use: 0 Number of
aggregators: 0 Group Port-channel Protocol Ports -----+-----+-----+----- Router_2#
```

## 3. Doorstuurtabel voor MAC-adressen van switches onderzoeken

Verifieer of de vermeldingen in de MAC-adrestabel bestaan op de switch voor de HSRP-routers, voor zowel het virtuele MAC-adres voor HSRP als de fysieke BIA's. De opdracht **show standby op**

de router geeft het virtuele MAC-adres. De opdracht **show interface** geeft het fysieke BIA. Hier zijn voorbeeldoutputs:

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:37:03 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.768 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.368 sec) Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:35:56 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.472 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.336 sec) Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

```
Router_1#show interfaces vlan 10 Vlan10 is up, line protocol is up , Autostate Enabled Hardware is Ethernet SVI, address is d4e8.801f.4846 (bia d4e8.801f.4846) Internet address is 192.168.10.1/24 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:01, output hang never Last clearing of "show interface" counters never Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 9258 packets input, 803066 bytes, 0 no buffer Received 0 broadcasts (0 IP multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 3034 packets output, 368908 bytes, 0 underruns Output 0 broadcasts (0 IP multicasts) 0 output errors, 2 interface resets 0 unknown protocol drops 0 output buffer failures, 0 output buffers swapped out
```

```
L2Switch_1#show mac address-table address 0000.0c07.ac6e Mac Address Table ----- Vlan Mac Address Type Ports ---- - 10 0000.0c07.ac6e DYNAMIC Gi1/0/13 Total Mac Addresses for this criterion: 1 L2Switch_1#show mac address-table address 0000.0c07.ac6f Mac Address Table ----- Vlan Mac Address Type Ports ---- - 11 0000.0c07.ac6f DYNAMIC Gi1/0/13 Total Mac Addresses for this criterion: 1
```

Controleer de CAM-verouderingstijd om na te gaan hoe snel de vermeldingen verouderd zijn. Als de tijd gelijk is aan de geconfigureerde waarde voor STP-doorstuurvertraging, die standaard 15 seconden is, bestaat er een grote kans dat zich een STP-lus in het netwerk bevindt. Hieronder staat voorbeeldoutput van de opdracht:

```
L2Switch_1#show mac address-table aging-time vlan 10 Global Aging Time: 300 Vlan Aging Time ---- 10 300 L2Switch_1#show mac address-table aging-time vlan 11 Global Aging Time: 300 Vlan Aging Time ---- 11 300
```

## C. Connectiviteit van fysieke laag verifiëren

Als meer dan één router in een HSRP-groep actief wordt, ontvangen deze routers niet consequent hello-pakketten van mede-HSRP-peers. Problemen met de fysieke laag kunnen de consequente verkeersdoorgang tussen peers hinderen en deze situatie veroorzaken. Verifieer daarom de fysieke connectiviteit en IP-connectiviteit tussen HSRP-peers wanneer u HSRP troubleshoot. Gebruik de opdracht **show standby** om de connectiviteit te verifiëren. Hierna volgt een voorbeeld:

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:54:03 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.848 secs Preemption enabled Active router is local Standby router is unknown Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:52:56 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.512 secs Preemption enabled Active router is local Standby router is unknown Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

```
Router_2#show standby Vlan10 - Group 110 State is Init (interface down) 2 state changes, last state change 00:00:42 Virtual IP address is 192.168.10.100 Active virtual MAC address is unknown (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Preemption disabled Active router is unknown Standby router is unknown Priority 109 (configured 109) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Init (interface down) 2 state changes, last state change 00:00:36 Virtual IP address is 192.168.11.100 Active virtual MAC address is unknown (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Preemption disabled Active router
```

is unknown Standby router is unknown Priority 109 (configured 109) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1

## 1. Interfacestatus controleren

Controleer de interfaces. Verifieer of alle interfaces die volgens het HSRP zijn geconfigureerd `up/up` zijn, zoals in het volgende voorbeeld:

```
Router_1#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.1 YES manual up up Vlan10 192.168.10.1 YES manual up up Vlan11 192.168.11.1 YES manual up up Router_2#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.2 YES manual up up Vlan10 192.168.10.2 YES manual administratively down down Vlan11 192.168.11.2 YES manual administratively down down
```

Als er interfaces zijn die administratief `down/down` zijn, voer dan de interface-specifieke opdracht **no shutdown** uit in de configuratiemodus van de router. Hierna volgt een voorbeeld:

```
Router_2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router_2(config)#interface vlan 10
Router_2(config-if)#no shutdown
Router_2(config-if)#end
```

```
Router_2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router_2(config)#interface vlan 11
Router_2(config-if)#no shutdown Router_2(config-if)#end
```

```
Router_2#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.2 YES manual up up Vlan10 192.168.10.2 YES manual up down Vlan11 192.168.11.2 YES manual up up
```

Als er interfaces zijn die `down/down` or `up/down` zijn, ga dan in het logbestand na of er wijzigingsmeldingen voor de interface zijn. Bij switches met Cisco IOS-software worden de volgende meldingen weergegeven in het geval van link `up/down`:

```
%LINK-3-UPDOWN: Interface "interface", changed state to up
%LINK-3-UPDOWN: Interface "interface", changed state to down
```

```
Router_1#show log
3d04h: %STANDBY-6-STATECHANGE: Standby: 0: Vlan10 state Active-> Speak
3d04h: %LINK-5-CHANGED: Interface Vlan10, changed state to down
3d04h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
```

Controleer de poorten, kabels en alle transceivers en andere apparaten die zich tussen de HSRP-peers bevinden. Heeft iemand kabels verwijderd of aansluitingen losgemaakt? Zijn er interfaces die herhaaldelijk een link verliezen? Zijn de juiste typen kabels gebruikt? Controleer de interfaces op fouten, zoals in het onderstaande voorbeeld:

```
Router_2#show interface vlan 10 Vlan10 is down, line protocol is down , Autostate Enabled Hardware is Ethernet SVI, address is 1880.90d8.5946 (bia 1880.90d8.5946) Internet address is 192.168.10.2/24 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:10, output 00:00:08, output hang never Last clearing of "show interface" counters never Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 1243 packets input, 87214 bytes, 0 no buffer Received 0 broadcasts (0 IP multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 23 packets output, 1628 bytes, 0 underruns Output 0 broadcasts (0 IP multicasts) 0 output errors, 2 interface resets 0 unknown protocol drops 0 output buffer failures, 0 output buffers swapped out
```

## 2. Wijziging in links en poortfouten

Controleer de wijzigingen in links in de switchpoorten en andere fouten. Gebruik deze opdrachten en ga de output na:

- logboekregistratie tonen
- toon interfaces <interface> tellers
- toon interfaces <interface> status

Deze opdrachten helpen u bepalen of er een probleem met connectiviteit is tussen switches en andere apparaten.

Deze berichten zijn normaal in het geval van link `up/down`:

```
L2Switch_1#show logging Syslog logging: enabled (0 messages dropped, 5 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled) No Active Message Discriminator. No Inactive Message Discriminator. Console logging: level informational, 319 messages logged, xml disabled, filtering disabled Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled Buffer logging: level debugging, 467 messages logged, xml disabled, filtering disabled Exception Logging: size (4096 bytes) Count and timestamp logging messages: disabled File logging: disabled Persistent logging: disabled No active filter modules. Trap logging: level informational, 327 message lines logged Logging Source-Interface: VRF Name: Log Buffer (10000 bytes): *Jul 26 17:52:07.526: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up *Jul 26 17:52:09.747: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down *Jul 26 17:57:11.716: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307. *Jul 26 17:57:11.716: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type. *Jul 26 17:57:13.583: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up *Jul 26 17:57:16.237: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down *Jul 26 18:02:16.481: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307. *Jul 26 18:02:16.481: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type. *Jul 26 18:02:18.367: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up *Jul 26 18:02:20.561: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down
```

Geef de opdracht **status van de showinterfaces <interface> uit** om de algemene status van een poort te bepalen. Hierna volgt een voorbeeld:

```
L2Switch_1#show interfaces gigabitEthernet 1/0/13 status Port Name Status Vlan Duplex Speed Type Gi1/0/13 connected trunk a-full a-1000 10/100/1000BaseTX
```

Is de interfacestatus `verbonden`, `niet verbonden`, of `onbruikbaar gemaakt`? Als de status `notconnect` is, controleer dan of de kabel aan beiden kanten is aangesloten. Controleer of de juiste kabel is gebruikt. Als de status `errdisable` is, controleer dan de tellers op overmatige fouten. Raadpleeg [Herstel van de Errunk-poortstatus op Cisco IOS-platforms](#) voor meer informatie.

Voor welk VLAN is deze poort geconfigureerd? Controleer of de andere kant van de verbinding voor hetzelfde VLAN is geconfigureerd. Als de link als trunk is geconfigureerd, controleer dan of beide kanten van de trunk dezelfde VLAN's verwerken.

Wat is de configuratie voor snelheid en duplex? Als de instelling wordt voorafgegaan door een 'a-', is de poort geconfigureerd om automatisch te onderhandelen over de snelheid en duplex. Anders heeft de netwerkbeheerder deze configuratie vooraf bepaald. Voor het configureren van de snelheid en duplex voor een link moeten de instellingen aan beide kanten van de link overeenkomen. Als één switchpoort is configureert voor automatische onderhandeling, moet de andere kant van de link hier ook voor worden geconfigureerd. Als aan één kant een specifieke snelheid en duplex is vastgelegd, moet dit voor de andere kant ook worden vastgelegd. Als u één kant op automatisch onderhandelen laat staan terwijl de andere kant is vastgelegd, mislukt het automatische onderhandelingsproces.

```
L2Switch_1#show interfaces gi1/0/13 counters errors Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards Gi1/0/13 0 0 0 0 0 0 Port Single-Col Multi-Col Late-Col Excess-Col Carri-Sen Runts Gi1/0/13 0 0 0 0 0 0
```

Zijn er veel `Align-Err`, `FCS-Err` of `Runts`? Deze wijzen op een snelheid- of duplex-mismatch tussen de poort en het aangesloten apparaat. Pas de snelheids- of duplexinstellingen aan voor die poort





Een andere optie die kan helpen om een Unidirectionele Link te verifiëren als UDLD niet beschikbaar is, is met het gebruik van Cisco Discovery Protocol (CDP). Het inschakelen van het CDP is een andere manier om het bestaan van unidirectionele links te detecteren. Als slechts één kant van de link het naburige apparaat kan zien, vervang dan de kabel tussen de apparaten en controleer op defecte interfaces.

```
Router_1#show cdp Global CDP information: Sending CDP packets every 60 seconds Sending a holdtime value of 180 seconds
Sending CDPv2 advertisements is enabled Router_1#show cdp neighbors gi1/0/1 detail ----- Device ID:
L2Switch_1.cisco.com Entry address(es): IP address: 192.168.70.1 IPv6 address: 2001:420:140E:2101::1 (global unicast) IPv6
address: FE80::2FE:C8FF:FED3:86C7 (link-local) Platform: cisco WS-C3650-12X48UR, Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): GigabitEthernet1/0/13 Holdtime : 173 sec Version : Cisco IOS Software
[Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.8, RELEASE SOFTWARE (fc3) Technical
Support: http://www.cisco.com/techsupport Copyright (c) 1986-2019 by Cisco Systems, Inc. Compiled Wed 13-Feb-19 03:00 by
mcpred advertisement version: 2 VTP Management Domain: 'CALOnet' Native VLAN: 1 Duplex: full Management address(es): IP
address: 192.168.70.1 Spare Pair PoE: Yes, Spare Pair Detection Required: No Spare Pair PD Config: Disable, Spare Pair PSE
Operational: No Total cdp entries displayed : 1
```

## 5. Aanvullende verwijzingen voor troubleshooting van fysieke laag

Raadpleeg deze documenten:

- [Automatische onderhandeling voor Ethernet 10/100/1000 Mb half/full duplex configureren en problemen ermee oplossen](#)
- [Herstel de uitgeschakelde poortstatus op Cisco IOS-platforms](#)
- [Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues \(NIC-compatibiliteitsproblemen bij Cisco Catalyst-switches oplossen\)](#)
- De sectie [Datalinkfouten begrijpen](#) van [NIC-compatibiliteitsproblemen troubleshooten bij Cisco Catalyst-switches](#)
- [Problemen met switchpoorten en interfaces troubleshooten](#)

## D. HSRP-foutopsporing voor Layer 3

Als de wijzigingen in de HSRP-status frequent zijn, gebruikt u de HSRP-debug-opdrachten (in inschakelen) op de router om op HSRP-activiteit te letten. Deze informatie helpt u om te bepalen welke HSRP-pakketten worden ontvangen en verzonden door de router. Verzamel deze informatie als u een serviceaanvraag doet bij Cisco Technical Support. De debug-output toont ook informatie over de HSRP-toestand, samen met gedetailleerde beschrijvingen van hello-pakketten voor HSRP.

### 1. Standaard HSRP-foutopsporing

In Cisco IOS inschakelen van de HSRP-debugfunctie met de opdracht **debug standby**. Deze informatie is nuttig bij onregelmatig optredende problemen die slechts een klein aantal interfaces beïnvloeden. Met de debug kunt u ook bepalen of de betreffende HSRP-router hello-pakketten op specifieke intervallen ontvangt en verzendt. Als de router geen hello-pakketten ontvangt, kunt u daaruit afleiden dat de peer geen hello-pakketten verzendt of dat het netwerk de pakketten afwijst.

Opdracht	Doel
<b>debug standby</b>	Schakelt HSRP-foutopsporing in

Hieronder staat voorbeeldoutput van de opdracht:

```
Router_1#debug standby HSRP debugging is on Jul 29 16:12:16.889: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100 Jul 29 16:12:16.996: HSRP: V111 Grp 111 Hello in 192.168.11.2 Standby pri 109 vIP 192.168.11.100 Jul 29 16:12:17.183: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100 Jul 29 16:12:17.366: HSRP: V111 Grp 111 Hello out 192.168.11.1 Active pri 110 vIP 192.168.11.100 Jul 29 16:12:18.736: HSRP: V110 Interface adv in, Passive, active 0, passive 1, from 192.168.10.2 Jul 29 16:12:19.622: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
```

## 2. Voorwaardelijke HSRP-foutopsporing (output beperken gebaseerd op stand-bygroep en/of VLAN)

In Cisco IOS-software release 12.0(3) is een debug-voorwaarde geïntroduceerd waarmee de output van de opdracht **debug standby** kan worden gefilterd op basis van interface en groepsnummer. Deze opdracht maakt gebruik van het concept debug condition dat in Cisco IOS-software release 12.0 is geïntroduceerd.

### Opdracht

```
debug voorwaarde stand-by <interface>
<groep>
```

### Doel

Schakelt voorwaardelijke foutopsporing voor HSRP van de groep (0–255) in

De interface moet een geldige interface zijn die HSRP kan ondersteunen. De groep kan om het even welke groep zijn, van 0 tot 255. Een debug voorwaarde kan worden ingesteld voor groepen die niet bestaan. Hierdoor kan debug-informatie worden vastgelegd tijdens de initialisatie van een nieuwe groep. Debug standby moet ingeschakeld zijn om debug-output te kunnen produceren. Als er geen stand-by debug-voorwaarde bestaat, wordt debug-output voor alle groepen op alle interfaces geproduceerd. Als er tenminste één stand-by debug-voorwaarde bestaat, wordt stand-by debug-output gefilterd gebaseerd op alle stand-by debug-voorwaarden. Hieronder staat voorbeeldoutput van de opdracht:

```
Router_1#debug condition standby vlan 10 110
Condition 1 set
Router_1#
Jul 29 16:16:20.284: V110 HSRP110 Debug: Condition 1, hsrp V110 HSRP110 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
Jul 29 16:16:44.797: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:45.381: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:16:47.231: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:48.248: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
```

## 3. Uitgebreide HSRP-foutopsporing

Cisco IOS-software release 12.1(1) heeft verbeterde HSRP-foutopsporing toegevoegd. Verbeterde HSRP-foutopsporing helpt bij het vinden van nuttige informatie door de ruis van periodieke hello-berichten te beperken en bevat aanvullende toestandsinformatie. Deze informatie is met name nuttig wanneer u met een Cisco Technical Support-engineer werkt als u een serviceaanvraag doet.

### Opdracht

```
debug standby
debug standby errors
debug standby events [[all] | [hsrp | redundancy |
track]] [detail]
debug standby packets [[all | terse] | [advertise | coup
| hello | resign]] [detail]
```

### Doel

Toont alle HSRP-fouten, -gebeurtenissen en -pakketten  
Toont HSRP-fouten  
Toont HSRP-gebeurtenissen  
Toont HSRP-pakketten

## debug stand-by modus

Een beperkt bereik van HSRP-fouten, -gebeurtenissen en -pakketten weergeven

Hieronder staat voorbeeldoutput van de opdracht:

```
Router_2#debug standby terse HSRP: HSRP Errors debugging is on HSRP Events debugging is on (protocol, neighbor, redundancy, track, ha, arp, interface) HSRP Packets debugging is on (Coup, Resign) Router_2# *Jul 29 16:49:35.416: HSRP: V110 Grp 110 Resign in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:49:35.416: HSRP: V110 Grp 110 Standby: i/Resign rcvd (110/192.168.10.1) *Jul 29 16:49:35.416: HSRP: V110 Grp 110 Active router is local, was 192.168.10.1 *Jul 29 16:49:35.416: HSRP: V110 Nbr 192.168.10.1 no longer active for group 110 (Standby) *Jul 29 16:49:35.417: HSRP: V110 Nbr 192.168.10.1 Was active or standby - start passive holddown *Jul 29 16:49:35.417: HSRP: V110 Grp 110 Standby router is unknown, was local *Jul 29 16:49:35.417: HSRP: V110 Grp 110 Standby -> Active *Jul 29 16:49:35.418: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active *Jul 29 16:49:35.418: HSRP: Peer not present *Jul 29 16:49:35.418: HSRP: V110 Grp 110 Redundancy "hsrp-V110-110" state Standby -> Active *Jul 29 16:49:35.419: HSRP: V110 Grp 110 Added 192.168.10.100 to ARP (0000.0c07.ac6e) *Jul 29 16:49:35.420: HSRP: V110 IP Redundancy "hsrp-V110-110" standby, local -> unknown *Jul 29 16:49:35.421: HSRP: V110 IP Redundancy "hsrp-V110-110" update, Standby -> Active *Jul 29 16:49:38.422: HSRP: V110 IP Redundancy "hsrp-V110-110" update, Active -> Active
```

U kunt voorwaardelijke foutopsporing van interfaces en/of HSRP-groepen gebruiken om deze debug-output te filteren.

### Opdracht

**debug condition interface interface**

**debug voorwaarde stand-by <interface> <groep>**

### Doel

Schakelt voorwaardelijke foutopsporing voor een interface

Schakelt voorwaardelijke HSRP-foutopsporing in

In dit voorbeeld sluit de router zich aan bij een al bestaande HSRP-groep:

```
Router_2#debug condition standby vlan 10 110 Condition 1 set Router_2#debug condition interface gigabitEthernet 1/0/1 vlan-id 10 Condition 2 set Router_2#debug standby HSRP debugging is on Router_2# *Jul 29 16:54:12.496: HSRP: V110 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:15.122: HSRP: V110 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:17.737: HSRP: V110 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:18.880: HSRP: V110 Nbr 192.168.10.1 is passive *Jul 29 16:54:20.316: HSRP: V110 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:20.322: HSRP: V110 Grp 110 Coup in 192.168.10.1 Listen pri 110 vIP 192.168.10.100 *Jul 29 16:54:20.323: HSRP: V110 Grp 110 Active: j/Coup rcvd from higher pri router (110/192.168.10.1) *Jul 29 16:54:20.323: HSRP: V110 Grp 110 Active router is 192.168.10.1, was local *Jul 29 16:54:20.323: HSRP: V110 Nbr 192.168.10.1 is no longer passive *Jul 29 16:54:20.324: HSRP: V110 Nbr 192.168.10.1 active for group 110 *Jul 29 16:54:20.324: HSRP: V110 Grp 110 Active -> Speak *Jul 29 16:54:20.325: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak *Jul 29 16:54:20.325: HSRP: Peer not present *Jul 29 16:54:20.325: HSRP: V110 Grp 110 Redundancy "hsrp-V110-110" state Active -> Speak *Jul 29 16:54:20.326: HSRP: V110 Grp 110 Removed 192.168.10.100 from ARP *Jul 29 16:54:20.326: HSRP: V110 Grp 110 Deactivating MAC 0000.0c07.ac6e *Jul 29 16:54:20.327: HSRP: V110 Grp 110 Removing 0000.0c07.ac6e from MAC address filter *Jul 29 16:54:20.328: HSRP: V110 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:20.328: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:23.104: HSRP: V110 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:23.226: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:25.825: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:25.952: HSRP: V110 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:28.427: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:28.772: HSRP: V110 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:30.727: HSRP: V110 Grp 110 Speak: d/Standby timer expired (unknown) *Jul 29 16:54:30.727: HSRP: V110 Grp 110 Standby router is local *Jul 29 16:54:30.727: HSRP: V110 Grp 110 Speak -> Standby *Jul 29 16:54:30.727: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby *Jul 29 16:54:30.728: HSRP: Peer not present *Jul 29 16:54:30.728: HSRP: V110 Grp 110 Redundancy "hsrp-V110-110" state Speak -> Standby *Jul 29 16:54:30.728: HSRP: V110 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:31.082: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:33.459: HSRP: V110 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:33.811: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:36.344: HSRP: V110 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:36.378: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.856: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.876: HSRP: V110 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.688: HSRP: V110 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.717: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100
```

## E. Spanning Tree-problemen troubleshooten

Een STP-lusvoorwaarde of instabiliteit in een netwerk kan goede communicatie tussen HSRP-peers belemmeren. Door deze slechte communicatie wordt iedere peer een actieve router. STP-lussen kunnen broadcast storms, gedupliceerde frames en tegenstrijdige MAC-tabellen veroorzaken. Al deze problemen hebben invloed op het gehele netwerk en vooral op HSRP. HSRP-foutmeldingen kunnen de eerste aanwijzingen zijn van een STP-probleem.

Wanneer u problemen met STP troubleshoot, *moet* u de STP-topologie van het netwerk op elk VLAN begrijpen. U moet bepalen welke switch de root-brug is en welke poorten op de switch de toestanden blocking (blokkeren) en forwarding (doorsturen) hebben. Omdat elk VLAN zijn eigen STP-topologie heeft, is deze informatie zeer belangrijk op elk VLAN.

## 1. Spanning Tree-configuratie verifiëren

Zorg ervoor dat STP op elke switch en elk overbruggingsapparaat in het netwerk is geconfigureerd. Noteer waar de root-brug zich volgens elke switch bevindt. Noteer ook de waarden van de volgende timers:

- Root Max Age: de maximale ouderdom van de root
- Hello Time: de hello-tijd
- Forward Delay: de doorstuurvertraging

Geef het bevel uit van de **show over\*spannen-boom** om al deze informatie te zien. In de standaardinstelling wordt deze informatie voor alle VLAN's getoond. Maar u kunt ook andere VLAN-informatie filteren als u het VLAN-nummer met de opdracht levert. Deze informatie is zeer nuttig wanneer u STP-problemen troubleshoot.

Deze drie timers die u in de **show** opmerkt worden **overspannen-boom** output geleerd van de root-brug. Deze timers hoeven niet overeen te komen met de timers die op die specifieke brug zijn ingesteld. Maar zorg er wel voor dat de timers overeenkomen met de root-brug in het geval dat deze switch op enig moment de root-brug wordt. Het overeenkomen van de timers met de root-brug helpt bij het behouden van continuïteit en biedt beheergemak. Het overeenkomen voorkomt ook dat de switch het netwerk verstoort met onjuiste timers.

**Opmerking:** STP altijd inschakelen voor alle VLAN's, ongeacht of er redundante koppelingen in het netwerk zijn. Als u STP inschakelt op niet-redundante netwerken, voorkomt u breuken. Een breuk kan zich voordoen als iemand switches met hubs of andere switches overbrugt en per ongelijk een fysieke lus creëert. STP is ook zeer nuttig voor de isolatie van specifieke problemen. Als het inschakelen van STP de werking van iets in het netwerk beïnvloedt, kan dit een bestaand probleem aangeven dat u moet isoleren.

Hier is voorbeeldoutput van het bevel van de **show over\*spannen-boom**:

```
L2Switch_1#show spanning-tree vlan 10 VLAN0010 Spanning tree enabled protocol rstp Root ID Priority 32778 Address
00fe.c8d3.8680 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32778 (priority
32768 sys-id-ext 10) Address 00fe.c8d3.8680 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 300 sec
Interface Role Sts Cost Prio.Nbr Type ----- Gi1/0/3 Desg FWD 4 128.3 P2p
Gi1/0/10 Desg FWD 4 128.10 P2p Edge Gi1/0/11 Desg FWD 4 128.11 P2p Gi1/0/13 Desg FWD 4 128.13 P2p Gi1/0/14 Desg FWD
4 128.14 P2p Gi1/0/15 Desg FWD 4 128.15 P2p Gi1/0/16 Desg FWD 4 128.16 P2p Gi1/0/35 Desg FWD 4 128.35 P2p
L2Switch_1#show spanning-tree vlan 11 VLAN0011 Spanning tree enabled protocol rstp Root ID Priority 32779 Address
00fe.c8d3.8680 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32779 (priority
32768 sys-id-ext 11) Address 00fe.c8d3.8680 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 300 sec
Interface Role Sts Cost Prio.Nbr Type ----- Gi1/0/3 Desg FWD 4 128.3 P2p
Gi1/0/10 Desg FWD 4 128.10 P2p Edge Gi1/0/11 Desg FWD 4 128.11 P2p Gi1/0/13 Desg FWD 4 128.13 P2p Gi1/0/14 Desg FWD
4 128.14 P2p Gi1/0/15 Desg FWD 4 128.15 P2p Gi1/0/16 Desg FWD 4 128.16 P2p Gi1/0/35 Desg FWD 4 128.35 P2p
```

Switch L2Switch\_1 is de basis van VLAN 10 en VLAN 11.

## 2. Lusvoorwaarden bij Spanning Tree

Om een STP-lus te laten optreden, moet er fysieke redundantie op L2 in het netwerk zijn. Een STP-lusvoorwaarde treedt niet op als er geen mogelijkheid tot een fysieke lusvoorwaarde is. Symptomen van een STP-lusvoorwaarde zijn:

- Totale netwerkuitval
- Verlies van connectiviteit
- Netwerkapparatuur meldt hoog gebruik van processen en systemen

Als bij één VLAN een STP-lusvoorwaarde optreedt, kan dit een link overbelasten en de andere VLAN's van bandbreedte beroven. De **show interfaces <interface> controller** opdrachtnotities die poorten verzenden of ontvangen een buitensporig aantal pakketten. Overmatige broadcast en multicast kunnen aangeven welke poorten deel zijn een STP-lus. Over het algemeen is het telkens wanneer multicast of broadcast het aantal unicast pakketten overtreft waarschijnlijk dat bij een link sprake is van een STP-lusvoorwaarde.

**Opmerking:** de switch telt ook STP bridge protocol data units (BPDU's) die worden ontvangen en verzonden als multicast frames. Een poort in de STP-toestand blocking verzendt en ontvangt nog steeds STP-BPDU's.

```
Router_2#show interfaces gi1/0/1 controller GigabitEthernet1/0/1 is up, line protocol is up (connected) Hardware is Gigabit Ethernet, address is 1880.90d8.5901 (bia 1880.90d8.5901) Description: PNP STARTUP VLAN MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX input flow-control is on, output flow-control is unsupported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:04, output hang never Last clearing of "show interface" counters never Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 33000 bits/sec, 31 packets/sec 5 minute output rate 116000 bits/sec, 33 packets/sec 9641686 packets input, 1477317083 bytes, 0 no buffer Received 1913802 broadcasts (1151766 multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 1151766 multicast, 0 pause input 0 input packets with dribble condition detected 10702696 packets output, 4241534645 bytes, 0 underruns Output 3432 broadcasts (0 multicasts) 0 output errors, 0 collisions, 2 interface resets 9582 unknown protocol drops 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier, 0 pause output 0 output buffer failures, 0 output buffers swapped out Transmit GigabitEthernet1/0/1 Receive 4241534645 Total bytes 1477317083 Total bytes 10562003 Unicast frames 7727884 Unicast frames 4229489212 Unicast bytes 1291270617 Unicast bytes 137261 Multicast frames 1151766 Multicast frames 11812065 Multicast bytes 91096867 Multicast bytes 3432 Broadcast frames 762036 Broadcast frames 233368 Broadcast bytes 94949599 Broadcast bytes 0 System FCS error frames 0 IpgViolation frames 0 MacUnderrun frames 0 MacOverrun frames 0 Pause frames 0 Pause frames 0 Cos 0 Pause frames 0 Cos 0 Pause frames 0 Cos 1 Pause frames 0 Cos 1 Pause frames 0 Cos 2 Pause frames 0 Cos 2 Pause frames 0 Cos 3 Pause frames 0 Cos 3 Pause frames 0 Cos 4 Pause frames 0 Cos 4 Pause frames 0 Cos 5 Pause frames 0 Cos 5 Pause frames 0 Cos 6 Pause frames 0 Cos 6 Pause frames 0 Cos 7 Pause frames 0 Cos 7 Pause frames 0 Oam frames 0 OamProcessed frames 0 Oam frames 0 OamDropped frames 38144 Minimum size frames 4165201 Minimum size frames 4910833 65 to 127 byte frames 3126489 65 to 127 byte frames 1237675 128 to 255 byte frames 750243 128 to 255 byte frames 1029126 256 to 511 byte frames 1279281 256 to 511 byte frames 2205966 512 to 1023 byte frames 103668 512 to 1023 byte frames 1280952 1024 to 1518 byte frames 205229 1024 to 1518 byte frames 0 1519 to 2047 byte frames 11575 1519 to 2047 byte frames 0 2048 to 4095 byte frames 0 2048 to 4095 byte frames 0 4096 to 8191 byte frames 0 4096 to 8191 byte frames 0 8192 to 16383 byte frames 0 8192 to 16383 byte frames 0 16384 to 32767 byte frame 0 16384 to 32767 byte frame 0 > 32768 byte frames 0 > 32768 byte frames 0 Late collision frames 0 SymbolErr frames 0 Excess Defer frames 0 Collision fragments 0 Good (1 coll) frames 0 ValidUnderSize frames 0 Good (>1 coll) frames 0 InvalidOverSize frames 0 Deferred frames 0 ValidOverSize frames 0 Gold frames dropped 0 FcsErr frames 0 Gold frames truncated 0 Gold frames successful 0 1 collision frames 0 2 collision frames 0 3 collision frames 0 4 collision frames 0 5 collision frames 0 6 collision frames 0 7 collision frames 0 8 collision frames 0 9 collision frames 0 10 collision frames 0 11 collision frames 0 12 collision frames 0 13 collision frames 0 14 collision frames 0 15 collision frames 0 Excess collision frames LAST UPDATE 2384 msecs AGO
```

## 3. Melding van gewijzigde topologie

Een ander bevel dat voor de diagnose van STP kwesties essentieel is is het bevel van het **show overspannen-boomdetail**. Deze opdracht herleidt meldingen van topologiewijzigingen (TCN) naar de opdrachtgever. Deze berichten, die als speciale BPDU's tussen switches worden verstuurd, wijzen op een topologiewijziging op een switch. Die switch verzendt een TCN naar zijn root-poort. De TCN verplaatst zich upstream naar de root-brug. De root-brug verzendt dan vanuit al haar poorten een andere speciale BPDU: een erkenning van de topologiewijziging (TCA). De root-brug stelt het TCN-bit in de configuratie-BPDU in. Hierdoor stellen alle nonroot-bruggen de veroudering van hun MAC-adrestabellen in op de geconfigureerde doorstuurvertraging voor STP.

Om dit probleem te isoleren, hebt u toegang tot de root-brug van elk VLAN en geeft u de opdracht **Show Spanning-Tree <interface> Detail** voor de met de switch verbonden poorten uit. De laatste wijziging geeft de tijd dat de laatste TCN werd ontvangen. In dit geval is het al te laat om te zien wie de TCN's die de mogelijke STP-lus kunnen hebben veroorzaakt, heeft uitgegeven. Het aantal topologiewijzigingen geeft u een idee over het aantal TCN's dat voorkomt. Tijdens een STP-lus kan dit getal iedere minuut toenemen. Raadpleeg [Overwegingen bij problemen met het Spanning Tree Protocol en gerelateerd ontwerp](#) voor meer informatie.

Andere nuttige informatie:

- Poorten van de laatste TCN
- Tijdstip van de laatste TCN
- Huidig aantal TCN's

Hieronder staat voorbeeldoutput van de opdracht:

```
L2Switch_1#show spanning-tree vlan 10 detail VLAN0010 is executing the rstp compatible Spanning Tree protocol Bridge Identifier has priority 32768, sysid 10, address 00fe.c8d3.8680 Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6 We are the root of the spanning tree Topology change flag not set, detected flag not set Number of topology changes 8 last change occurred 03:21:48 ago from GigabitEthernet1/0/35 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 Port 3 (GigabitEthernet1/0/3) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.3. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.3, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 0 Port 10 (GigabitEthernet1/0/10) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.10. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.10, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 The port is in the portfast mode by portfast trunk configuration Link type is point-to-point by default BPDU: sent 6063, received 0 Port 11 (GigabitEthernet1/0/11) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.11. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.11, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 0 Port 13 (GigabitEthernet1/0/13) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.13. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.13, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 3 Port 14 (GigabitEthernet1/0/14) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.14. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.14, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 3 Port 15 (GigabitEthernet1/0/15) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.15. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.15, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0 Port 16 (GigabitEthernet1/0/16) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.16. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.16, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0 Port 35 (GigabitEthernet1/0/35) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.35. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.35, designated path cost 0 Timers: message age 0, forward delay 0, hold
```



0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDUs: sent 6067, received 0

Deze output toont aan dat de laatste topologieverandering van apparaat voorkwam dat van interface Gigabit Ethernet1/0/35 wordt aangesloten. Geef vervolgens dezelfde opdracht **show Spanning-Tree Detail** uit van dit apparaat om te proberen het probleem te volgen. Als deze switch die de TCN's genereert alleen op een PC of endpoints is aangesloten, zorg dan dat STP PortFast op deze poorten is ingeschakeld. STP PortFast onderdrukt STP-TCN's wanneer een poort overgaat naar een andere toestand.

Raadpleeg deze documenten voor informatie over STP en hoe u de link-overgangen kunt troubleshooten die verband houden met netwerkinterfacekaarten (NIC's):

- [PortFast en andere opdrachten gebruiken om connectiviteitsvertragingen bij het opstarten van werkstations op te lossen](#)
- [Begrijp Rapid Spanning Tree Protocol \(802.1w\)](#)
- [Overwegingen bij problemen met STP en gerelateerd ontwerp](#)

#### 4. Niet-verbonden geblokkeerde poorten

Door de taakverdeling van Fast EtherChannel (FEC) (port-channeling) kunnen FEC-problemen bijdragen aan de problemen met zowel HSRP als STP. Wanneer u problemen met STP of HSRP oplost, kunt u de configuratie voor alle FEC-verbindingen verwijderen. Nadat de configuratieveranderingen op zijn plaats zijn, geef het bevel van **show over:spannen-boom blockedports** op beide switches uit. Zorg ervoor dat ten minste één van de poorten aan beide zijden van de verbinding blokkeert.

Raadpleeg deze documenten voor informatie over Fast EtherChannel:

- [EtherChannel-taakverdeling en redundantie op Catalyst Switches begrijpen](#)
- [EtherChannel configureren](#)

#### 5. Broadcast onderdrukking

Schakel broadcast onderdrukking in om de impact van een broadcast storm te verminderen. Een broadcast storm is een van de belangrijkste neveneffecten van een STP-lus. Hieronder staat voorbeeldoutput van de opdracht:

```
L2Switch_1#show run interface TenGigabitEthernet1/1/5 Building configuration... Current configuration : 279 bytes ! interface
TenGigabitEthernet1/1/5 switchport trunk allowed vlan 300-309 switchport mode trunk storm-control broadcast level 30.00 storm-
control multicast level 30.00 storm-control unicast level 30.00 spanning-tree guard root end L2Switch_1#show storm-control
broadcast Key: U - Unicast, B - Broadcast, M - Multicast Interface Filter State Upper Lower Current Action Type -----
-----
----- Te1/1/5 Forwarding 30.00% 30.00% 0.00% None B Te1/1/7 Link Down 30.00% 30.00% 0.00%
None B Te1/1/8 Forwarding 10.00% 10.00% 0.00% None B L2Switch_1#show storm-control multicast Key: U - Unicast, B -
Broadcast, M - Multicast Interface Filter State Upper Lower Current Action Type -----
-----
---- Te1/1/5 Forwarding 30.00% 30.00% 0.00% None M Te1/1/7 Link Down 30.00% 30.00% 0.00% None M
```

#### 6. Console- en Telnet-toegang

Console- of Telnet-verkeer naar de switch wordt tijdens een STP-lus vaak te traag om het apparaat in kwestie goed te kunnen traceren. Om het netwerk te dwingen om onmiddellijk te herstellen, verwijdert u alle redundante fysieke links. Nadat het STP wordt toegestaan om op de nieuwe niet-redundante topologie opnieuw te convergeren, verbindt u de redundante links één voor één opnieuw. Als de STP-lus weer ontstaat nadat u één bepaald segment toevoegt, heeft u



het apparaat geïdentificeerd.

## 7. Spanning Tree-functies: Portfast, UplinkFast en BackboneFast

Verifieer of PortFast, UplinkFast en BackboneFast correct zijn geconfigureerd. Bij het troubleshooten van STP-problemen schakelt u alle geavanceerde STP-functies (UplinkFast en BackboneFast) uit. Controleer bovendien dat STP PortFast alleen is ingeschakeld op poorten die rechtstreeks verbonden zijn met niet-overbruggende hosts. Niet-overbruggende hosts zijn bijvoorbeeld werkstations van gebruikers en routers zonder overbruggingsgroepen. Schakel PortFast niet in op poorten die zijn verbonden met hubs of andere switches. Hier zijn een aantal documenten die u kunnen helpen bij het begrijpen en configureren van deze functies:

[Configureren van Spanning Tree Port Fast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast en Loop Guard](#)

[De Cisco UplinkFast-functie begrijpen en configureren](#)

## 8. BPDU Guard

Wanneer u PortFast BPDU Guard inschakelt, wordt een niet-trunking PortFast-poort in de errdisable-toestand geplaatst bij ontvangst van een BPDU op die poort. Deze functie helpt u de poorten te vinden die onjuist zijn geconfigureerd voor PortFast. De functie detecteert ook waar apparaten pakketten reflecteren of STP BPDU's in het netwerk injecteren. Wanneer u problemen met STP oplost, kunt u deze functie inschakelen om te helpen de STP-kwestie te isoleren.

```
L2Switch_1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. L2Switch_1(config)#spanning-tree portfast bpduguard L2Switch_1(config)#end
```

## 9. VTP-pruning

Wanneer VTP-pruning in het netwerk is ingeschakeld, kan het de apparaten van een HSRP-groep actief maken. Dit leidt tot IP-conflicten tussen de gateways en veroorzaakt verkeersproblemen. Zorg ervoor dat het VLAN van een HSRP-groep niet te maken krijgt met VTP-pruning in het netwerk.

## F. Delen en veroveren

Als alle andere pogingen om HSRP te isoleren of te verhelpen mislukken, is de methode 'verdeel en heers' de volgende stap. Deze methode helpt bij het isoleren van het netwerk en de componenten die samen het netwerk vormen. Verdeel en heers heeft betrekking op alle richtlijnen in deze lijst:

**N.B.:** Deze lijst bevat een aantal richtsnoeren uit andere delen van dit document.

- Maak een test-VLAN voor HSRP en een geïsoleerd VLAN om met HSRP-routers te switchen.
- Verbreek de verbinding met alle redundante poorten.
- Maak van FEC-poorten enkele, verbonden poorten.
- Breng de HSRP-groep terug tot twee leden.

- Voer pruning uit op trunkpoorten zodat alleen noodzakelijke VLAN's via die poorten worden doorgegeven.
- Verbreek de verbinding van verbonden switches in het netwerk totdat de problemen opgelost zijn.

## Bekende problemen

### HSRP-status flappen/instabiel bij gebruik van Cisco 2620/2621, Cisco 3600 met Fast Ethernet

Dit probleem kan voorkomen bij Fast Ethernet-interfaces wanneer de netwerkconnectiviteit verstoord wordt of een HSRP-router met hogere prioriteit aan een netwerk wordt toegevoegd. Wanneer de HSRP-toestand van Active naar Speak wisselt, stelt de router de interface opnieuw in om het MAC-adres voor HSRP uit het MAC-adresfilter van de interface te verwijderen. Alleen specifieke hardware die op de Fast Ethernet-interfaces voor Cisco 2600s, 3600s, en 7500s wordt gebruikt heeft dit probleem. Het resetten van de routerinterface veroorzaakt een verandering in de linktoestand op Fast Ethernet-interfaces. De switch detecteert deze verandering. Als de switch STP gebruikt, veroorzaakt de verandering een STP-overgang. De STP zet binnen 30 seconden de poort in de toestand forwarding. Dit is twee keer de standaardtijd voor de doorstuurvertraging van 15 seconden. Tegelijkertijd gaat de sprekende router na 10 seconden over naar toestand `standby` en dit is even lang als de HSRP-wachtstandtijd. STP staat nog niet op forwarding, dus er worden van de actieve router geen hello-berichten voor HSRP ontvangen. Hierdoor wordt de stand-byrouter na ongeveer 10 seconden actief. Beide routers zijn nu `actief`. Wanneer de STP-poorten op forwarding staan, verandert de router met lagere prioriteit van Active naar Speak, en wordt het gehele proces herhaald.

Platform	Beschrijving	Cisco bug-ID	Oplossen	Tijdelijke oplossing
Cisco 2620/2621	Fast Ethernet-interface begint te fluctueren wanneer HSRP is geconfigureerd en de kabel is verwijderd.		Een software upgrade; raadpleeg de bug voor revisie details.	Schakelt Spanning Tree PortFast in op de aangesloten switchpoort.
Cisco 2620/2621	HSRP-toestand fluctueert bij 2600 met Fast Ethernet.		Cisco IOS-softwarerelease 12.1.3	Schakelt Spanning Tree PortFast in op de aangesloten switchpoort.
Cisco 3600 met NM-1FE-TX <sup>1</sup>	HSRP-toestand fluctueert bij 2600 en 3600 met Fast Ethernet.		Cisco IOS-softwarerelease 12.1.3	Schakelt Spanning Tree PortFast in op de aangesloten switchpoort.
Cisco 4500 met Fast Ethernet-interface	HSRP-toestand fluctueert bij 4500 Fast Ethernet.	Cisco bug-id <a href="#">CSCs16055</a>	Cisco IOS-softwarerelease 12.1.5	Schakelt Spanning Tree PortFast in op de aangesloten switchpoort.

<sup>1</sup>NM-1FE-TX = één-poorts Fast Ethernet-netwerkmodule (10/100BASE-TX interface).

Een alternatieve tijdelijke oplossing is het aanpassen van de HSRP-timers zodat de STP-

doorstuurvertraging minder dan de helft van de standaard HSRP-wachtstandtijd is. De standaard STP-doorstuurvertraging is 15 seconden, terwijl de standaard HSRP-wachtstandtijd 10 seconden is.

Wanneer u de opdracht **track** gebruikt onder het HSRP-proces, raadt Cisco u aan een bepaalde decrement-waarde te gebruiken om de HSRP-fluctuatie te voorkomen.

Dit is een voorbeeldconfiguratie in een actieve HSRP-router bij het gebruiken van de opdracht **track**:

```
standby 1 ip 10.0.0.1
standby 1 priority 105
standby 1 preempt delay minimum 60
standby 1 name TEST
standby 1 track <object> decrement 15
```

Waarbij 15 de afbraakwaarde is wanneer het object flapt. Om meer te weten te komen over de track commando, navigeer dan naar de document [Track Option in HSRPv2 Configuration Voorbeeld](#).

## Gerelateerde informatie

- [Campus LAN Catalyst Switches - Access](#)
- [LAN-switching](#)
- [Technische ondersteuning en documentatie – 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.