Fehlerbehebung bei HSRP-Problemen in Catalyst Switch-Netzwerken

Inhalt

Einleitung

In diesem Dokument werden häufige Probleme und Möglichkeiten zur Behebung von HSRP-Problemen (Hot Standby Router Protocol) beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Informationen zu HSRP

Hintergrundinformationen

In diesem Dokument werden die häufigsten Probleme im Zusammenhang mit HSRP behandelt:

- Router meldet eine doppelte HSRP-Standby-IP-Adresse
- Ständige HSRP-Statusänderungen (aktiv/Standby/Kommunikation)
- HSRP-Peers nicht vorhanden
- Switch-Fehlermeldungen im Zusammenhang mit HSRP
- Übermäßiges Netzwerk-Unicast-Flooding zur HSRP-Konfiguration

> **Hinweis:** In diesem Dokument wird die Fehlerbehebung bei HSRP in Catalyst Switch-Umgebungen beschrieben. Das Dokument enthält zahlreiche Verweise auf Software-Versionen und das Design der Netzwerktopologie. Dennoch dient dieses Dokument einzig und allein dazu, Technikern die Fehlerbehebung bei HSRP zu erleichtern. Dieses Dokument ist nicht als Designleitfaden, Softwareempfehlungsdokument oder Best-Practice-Dokument gedacht.

Unternehmen und Verbraucher, die für ihre geschäftskritische Kommunikation Intranet- und Internet-Services nutzen, benötigen und erwarten kontinuierliche Verfügbarkeit bei Netzwerken und Anwendungen. Kunden können ihre Anforderungen an eine nahezu hundertprozentige Netzwerkverfügbarkeit erfüllen, wenn sie HSRP in Cisco IOS®-Software nutzen. HSRP, das nur bei Cisco Plattformen verfügbar ist, bietet Netzwerkredundanz für IP-Netzwerke in einer Weise, die sicherstellt, dass der Benutzerdatenverkehr nach First-Hop-Ausfällen auf Netzwerk-Edge-Geräten oder in Zugriffsschaltkreisen sofort und transparent wiederhergestellt wird.

Zwei oder mehr Router können als ein einziger virtueller Router fungieren, wenn sie dieselbe IP-Adresse und MAC-Adresse (Layer 2 [L2]) haben. Die Adresse ist für die Standard-Gateway-Redundanz der Host-Workstation erforderlich. Die meisten Host-Workstations enthalten keine Routing-Tabellen und verwenden nur eine einzelne IP- und MAC-Adresse für den nächsten Hop. Diese Adresse wird als das Standardgateway bezeichnet. Bei HSRP tauschen Mitglieder der virtuellen Router-Gruppe kontinuierlich Statusmeldungen aus. Ein Router kann die Routing-Zuständigkeit eines anderen übernehmen, wenn ein Router aus geplanten oder ungeplanten Gründen außer Betrieb genommen wird. Hosts werden mit einem einzelnen Standardgateway konfiguriert und leiten IP-Pakete weiterhin an eine konsistente IP- und MAC-Adresse weiter. Der Wechsel der Geräte, die das Routing durchführen, ist für die End-Workstations transparent.

> **Hinweis**: Sie können Host-Workstations konfigurieren, auf denen Microsoft OS für mehrere

Standard-Gateways ausgeführt wird. Die verschiedenen Standard-Gateways sind jedoch nicht dynamisch. Das Betriebssystem verwendet jeweils nur ein Standardgateway. Das System wählt nur dann beim Booten ein zusätzliches konfiguriertes Standardgateway aus, wenn das erste konfigurierte Standardgateway von ICMP (Internet Control Management Protocol) als nicht erreichbar identifiziert wurde.

Grundlegender Betrieb

Eine Reihe von Routern, auf denen HSRP ausgeführt wird, arbeitet zusammen, um den Hosts im LAN die Illusion eines einzelnen Standard-Gateway-Routers zu vermitteln. Diese Gruppe von Routern wird als HSRP-Gruppe oder Standby-Gruppe bezeichnet. Ein einzelner Router, der aus der Gruppe ausgewählt wird, ist für die Weiterleitung der Pakete verantwortlich, die Hosts an den virtuellen Router senden. Dieser Router wird als der aktive Router bezeichnet. Ein anderer Router wird als der Standby-Router ausgewählt. Wenn der aktive Router ausfällt, übernimmt der Standby-Router die Paketweiterleitungsaufgaben. Obwohl HSRP auf einer beliebigen Anzahl von Routern ausgeführt werden kann, leitet nur der aktive Router die an die IP-Adresse des virtuellen Routers gesendeten Pakete weiter.

Um den Netzwerkverkehr zu minimieren, senden nur der aktive und der Standby-Router regelmäßig HSRP-Nachrichten, nachdem das Protokoll den Auswahlprozess abgeschlossen hat. Weitere Router in der HSRP-Gruppe verbleiben im `empfangsbereiten` Status. Wenn der aktive Router ausfällt, übernimmt der Standby-Router die Rolle des aktiven Routers. Wenn der Standby-Router ausfällt oder zum aktiven Router wird, wird ein anderer Router als Standby-Router ausgewählt.

Jede Standby-Gruppe emuliert einen einzelnen virtuellen Router (Standardgateway). Jeder Gruppe wird eine einzige bekannte MAC- und IP-Adresse zugewiesen. Mehrere Standby-Gruppen können in einem LAN nebeneinander bestehen und sich überschneiden, und einzelne Router können zu mehreren Gruppen gehören. In diesem Fall behält der Router für jede Gruppe einen separaten Status und Timer bei.

Begriffe bei HSRP

Begriff	Definition
Aktiver Router	Der Router, der aktuell Pakete für den virtuellen Router weiterleitet
Standby-Router	Der primäre Backup-Router
Standby-Gruppe	Die Gruppe von Routern, die an HSRP teilnehmen und gemeinsam einen virtuellen Rou emulieren
Hello-Zeit	Das Intervall zwischen aufeinanderfolgenden HSRP-Hello-Nachrichten von einem bestimmten Router
Haltezeit	Das Intervall zwischen dem Empfang einer Begrüßungsnachricht und der Annahme, das sendende Router ausgefallen ist

Adressierung bei HSRP

Router-Kommunikation bei HSRP

Router, auf denen HSRP ausgeführt wird, kommunizieren HSRP-Informationen untereinander über HSRP-Hello-Pakete. Diese Pakete werden an die Ziel-IP-Multicast-Adresse 224.0.0.2 an UDP-Port 1985 (User Datagram Protocol) gesendet. Die IP-Multicast-Adresse 224.0.0.2 ist eine

reservierte Multicast-Adresse, die für die Kommunikation mit allen Routern verwendet wird. Der aktive Router bezieht Hello-Pakete von seiner konfigurierten IP-Adresse und der virtuellen HSRP-MAC-Adresse. Der Standby-Router bezieht Hellos von seiner konfigurierten IP-Adresse und der festen MAC-Adresse (Burned-In-Adresse, BIA). Diese Verwendung der Quelladressierung ist erforderlich, damit sich HSRP-Router gegenseitig korrekt identifizieren können.

Wenn Sie Router als Teil einer HSRP-Gruppe konfigurieren, überwachen in den meisten Fällen die Router die HSRP-MAC-Adresse für diese Gruppe sowie ihre eigene BIA. Die einzige Ausnahme von diesem Verhalten gilt bei den Cisco Routern 2500, 4000 und 4500. Diese Router verfügen über Ethernet-Hardware, die nur eine einzige MAC-Adresse erkennt. Daher verwenden diese Router die HSRP-MAC-Adresse, wenn sie als aktiver Router fungieren. Die Router verwenden ihre BIA, wenn sie als Standby-Router fungieren.

HSRP-Standby-IP-Adresskommunikation bei allen Medien außer Token Ring

Da auf Host-Workstations das Standardgateway als HSRP-Standby-IP-Adresse konfiguriert ist, müssen Hosts mit der MAC-Adresse kommunizieren, die der HSRP-Standby-IP-Adresse zugeordnet ist. Diese MAC-Adresse ist eine virtuelle MAC-Adresse, die sich aus 0000.0c07.ac** zusammensetzt. Die beiden Sternchen (**) stehen für die HSRP-Gruppennummer im Hexadezimalformat, basierend auf der jeweiligen Schnittstelle. Beispiel: Für HSRP-Gruppe 1 wird die virtuelle HSRP-MAC-Adresse 0000.0c07.ac01 verwendet. Für Hosts im angrenzenden LAN-Segment wird der normale ARP-Prozess (Address Resolution Protocol) verwendet, um die zugehörigen MAC-Adressen aufzulösen.

ICMP adressiert um

HSRP-Peer-Router, die ein Subnetz schützen, können Zugriff auf alle anderen Subnetze im Netzwerk bieten. Dies ist die Grundlage von HSRP. Daher ist es unerheblich, welcher Router zum aktiven HSRP-Router wird. In Cisco IOS-Software-Versionen vor Cisco IOS-Software Version 12.1(3)T werden ICMP-Weiterleitungen an einer Schnittstelle automatisch deaktiviert, wenn HSRP an dieser Schnittstelle verwendet wird. Ohne diese Konfiguration können die Hosts weg von der virtuellen HSRP-IP-Adresse und hin zu einer Schnittstellen-IP und MAC-Adresse eines einzelnen Routers umgeleitet werden. Die Redundanz geht verloren.

Die Cisco IOS Software führt eine Methode ein, die ICMP-Umleitungen mit HSRP ermöglicht. Bei dieser Methode werden ausgehende ICMP-Umleitungsnachrichten über HSRP gefiltert. Die IP-Adresse des nächsten Hops wird in eine virtuelle HSRP-Adresse geändert. Die Gateway-IP-Adresse in der ausgehenden ICMP-Umleitungsnachricht wird mit einer Liste aktiver HSRP-Router abgeglichen, die in diesem Netzwerk vorhanden sind. Wenn der Router, der der Gateway-IP-Adresse entspricht, ein aktiver Router für eine HSRP-Gruppe ist, wird die Gateway-IP-Adresse durch die virtuelle IP-Adresse dieser Gruppe ersetzt. Diese Lösung ermöglicht es Hosts, optimale Routen zu Remote-Netzwerken zu ermitteln und gleichzeitig die Widerstandsfähigkeit von HSRP aufrechtzuerhalten.

HSRP-Funktionsmatrix

Weitere Informationen zu den Funktionen und Cisco IOS-Software-Versionen, die HSRP unterstützen, finden Sie bei den Informationen über Merkmale und Funktionen von Hot Standby Router Protocol im Abschnitt mit der Funktionsmatrix für Cisco IOS-Versionen und HSRP.

HSRP-Funktionen

Informationen zu den meisten HSRP-Funktionen finden Sie bei den Informationen über Merkmale und Funktionen von Hot Standby Router Protocol. Dieses Dokument enthält Informationen zu folgenden HSRP-Funktionen:

- Zwangstrennung
- Schnittstellennachverfolgung
- Verwendung einer BIA
- Mehrere HSRP-Gruppen
- Konfigurierbare MAC-Adressen
- Syslog-Unterstützung
- HSRP-Debugging
- Erweitertes HSRP-Debugging
- Authentifizierung
- IP-Redundanz
- Simple Network Management Protocol (SNMP) MIB
- HSRP für Multiprotocol Label Switching (MPLS)

Hinweis: Sie können die Suchfunktion Ihres Browsers verwenden, um nach diesen Abschnitten im Dokument zu suchen.

Paketformat

Diese Tabelle zeigt das Format des Datenteils des UDP-HSRP-Frames:

Version	**Op-Code**	**Status**	**Hello-Zeit**
Haltefrist	Priorität	Gruppe	Reserviert
Authentifizierungsdaten			
Authentifizierungsdaten			
Virtuelle IP-Adresse			

In dieser Tabelle werden die Felder aus dem HSRP-Paket beschrieben:

Paketfeld	Beschreibung
Op-Code (1 Oktett)	Der Op-Code beschreibt die Art der Nachricht, die das Paket enthält. Mögliche Werte sind: 0 - hello, 1 - Coup und 2 - resign. Hello-Nachrichten werden gesende um anzuzeigen, dass ein Router HSRP ausführt und zum aktiven Router werden kann. Coup-Nachrichten werden gesendet, wenn ein Router zum aktiven Router werden möchte. Resign-Nachrichten werden gesendet, wenn ein Router nicht me der aktive Router sein möchte.
Status (1 Oktett)	Jeder Router in der Standby-Gruppe implementiert ein Statusmodul. Aus dem Statusfeld geht der aktuelle Status des Routers hervor, der die Nachricht sendet. Dies sind Details zu den einzelnen Zuständen: 0 - initial, 1 - lernen, 2 - hören, 4 - sprechen, 8 - standby und 16 - aktiv.
Hello-Zeit (1 Oktett)	Dieses Feld ist nur bei Hello-Nachrichten von Bedeutung. Es enthält den ungefähren Zeitraum zwischen den Hello-Nachrichten, die der Router sendet. Die Zeit wird in Sekunden angegeben.
Haltezeit (1 Oktett)	Dieses Feld ist nur bei Hello-Nachrichten von Bedeutung. Es enthält die Zeitdaue die die Router auf eine Begrüßungsnachricht warten, bevor sie eine Statusänderung initiieren.
Priorität (1 Oktett)	In diesem Feld werden der aktive und der Standby-Router ausgewählt. Bei einem Vergleich der Prioritäten von zwei Routern wird der Router mit dem höchsten We

	zum aktiven Router. Im Zweifelsfall wird der Router mit der höheren IP-Adresse vorgezogen.
Gruppe (1 Oktett)	Dieses Feld identifiziert die Standby-Gruppe.
Authentifizierungsdaten (8 Oktette)	Dieses Feld enthält ein aus acht Zeichen bestehendes Klartextkennwort.
Virtuelle IP-Adresse (4 Oktette)	Wenn die virtuelle IP-Adresse auf einem Router nicht konfiguriert ist, kann die Adresse der Hello-Nachricht des aktiven Routers entnommen werden. Eine Adresse wird nur ermittelt, wenn keine HSRP-Standby-IP-Adresse konfiguriert wurde und die Hello-Nachricht authentifiziert wurde (sofern Authentifizierung konfiguriert ist).

HSRP-Status

Status	Definition
`Initial`	Dies ist der Status zu Beginn. Dieser Status gibt an, dass HSRP nicht ausgeführt wird. Dies Status wird durch eine Konfigurationsänderung oder die erstmalige Verfügbarkeit einer Schnittstelle initiiert.
`Lernen`	Der Router hat die virtuelle IP-Adresse nicht ermittelt und noch keine authentifizierte Hello-Nachricht des aktiven Routers erkannt. In diesem Status wartet der Router weiterhin auf Nachricht vom aktiven Router.
`Zuhören`	Der Router kennt die virtuelle IP-Adresse, aber er ist weder der aktive Router noch der Star Router. Es wartet auf Hello-Nachrichten von diesen Routern.
`Kommunikation`	Der Router sendet regelmäßig Hello-Nachrichten und nimmt aktiv an der Auswahl des aktiv und/oder Standby-Routers teil. Ein Router kann nur dann in den `Kommunikationsstatus` wechs wenn er über die virtuelle IP-Adresse verfügt.
`Standby`	Der Router ist ein Anwärter auf den nächsten aktiven Router und sendet regelmäßig Hello-Nachrichten. Mit Ausnahme von vorübergehenden Bedingungen befindet sich maximal ein Router in der Gruppe im `Standby-Status`.
`Aktiv`	Der Router leitet derzeit Pakete weiter, die an die virtuelle MAC-Adresse der Gruppe gesen werden. Der Router sendet regelmäßig Hello-Nachrichten. Mit Ausnahme von vorübergehe Bedingungen darf in der Gruppe maximal ein Router im `aktiven Status` vorhanden sein.

HSRP-Timer

Jeder Router verwendet bei HSRP nur drei Timer. Die Timer regeln die Taktung der Hello-Nachrichten. Wie HSRP konvergiert, wenn ein Fehler auftritt, hängt davon ab, wie die HSRP-Hello- und Hold-Timer konfiguriert sind. Standardmäßig sind diese Timer auf 3 bzw. 10 Sekunden eingestellt, was bedeutet, dass alle 3 Sekunden ein Hello-Paket zwischen den HSRP-Standby-Gruppengeräten gesendet wird und das Standby-Gerät aktiv wird, wenn 10 Sekunden lang kein Hello-Paket empfangen wurde. Sie können diese Timer-Einstellungen verringern, um das Failover oder die Freischaltung zu beschleunigen. Um jedoch eine erhöhte CPU-Nutzung und unnötiges Flapping im Standby-Status zu vermeiden, sollten Sie den Hello-Timer nicht auf weniger als eine (1) Sekunde oder den Hold-Timer auf weniger als vier Sekunden einstellen. Wenn Sie den HSRP-Nachverfolgungsmechanismus verwenden und der nachverfolgte Link fehlschlägt, erfolgt das Failover oder die Zwangstrennung unabhängig von den Hello- und Hold-Timern sofort. Wenn ein Timer abläuft, geht der Router in einen neuen HSRP-Status über. Die Timer können mit dem folgenden Befehl geändert werden: **standby [Gruppennummer] timers hellotime holdtime**. Beispiel: **standby 1 timers 5 15**.

Diese Tabelle enthält weitere Informationen zu diesen Timern:

Timer	Beschreibung

Aktiv-Timer	Dieser Timer wird zur Überwachung des aktiven Routers verwendet. Der Timer startet jed Mal, wenn ein aktiver Router ein Hello-Paket empfängt. Der Timer läuft in Übereinstimmur dem Wert für die Haltezeit ab, der im entsprechenden Feld der HSRP-Hello-Nachricht festgelegt ist.
Standby-Timer	Dieser Timer wird zur Überwachung des Standby-Routers verwendet. Der Timer startet je Mal, wenn der Standby-Router ein Hello-Paket empfängt. Der Timer läuft in Übereinstimm mit dem Wert für die Haltezeit ab, der im jeweiligen Hello-Paket festgelegt ist.
Hello-Timer	Dieser Timer wird verwendet, um Hello-Pakete zu takten. Alle HSRP-Router in einem beliebigen HSRP-Status generieren ein Hello-Paket, wenn dieser Hello-Timer abläuft.

HSRP-Ereignisse

Diese Tabelle enthält die Ereignisse aus dem HSRP-Statusmodul (Finite State Machine, FSM):

Wichtigste Events	
1	HSRP wird an einer aktivierten Schnittstelle konfiguriert.
2	HSRP ist an einer Schnittstelle deaktiviert, oder die Schnittstelle selbst ist deaktiviert.
3	Ablauf des Aktiv-Timers. Der aktive Timer wird auf die Haltezeit festgelegt, wenn die letzte Hel Nachricht des aktiven Routers erkannt wird.
4	Ablauf des Standby-Timers. Der Standby-Timer wird auf die Haltezeit festgelegt, wenn die letz Hello-Nachricht des Standby-Routers erkannt wird.
5	Ablauf des Hello-Timers. Der periodische Timer für das Senden von Hello-Nachrichten ist abgelaufen.
6	Empfang einer Hello-Nachricht mit höherer Priorität von einem Router im `Kommunikationsstatus`
7	Empfang einer Hello-Nachricht mit höherer Priorität vom aktiven Router
8	Empfang einer Hello-Nachricht mit niedrigerer Priorität vom aktiven Router
9	Empfang einer Resign-Nachricht vom aktiven Router
10	Empfang einer Coup-Nachricht von einem Router mit höherer Priorität
11	Empfang einer Hello-Nachricht mit höherer Priorität vom Standby-Router
12	Empfang einer Hello-Nachricht mit niedrigerer Priorität vom Standby-Router

HSRP-Aktionen

Diese Tabelle enthält die Aktionen, die im Rahmen des Statusmoduls durchgeführt werden sollen:

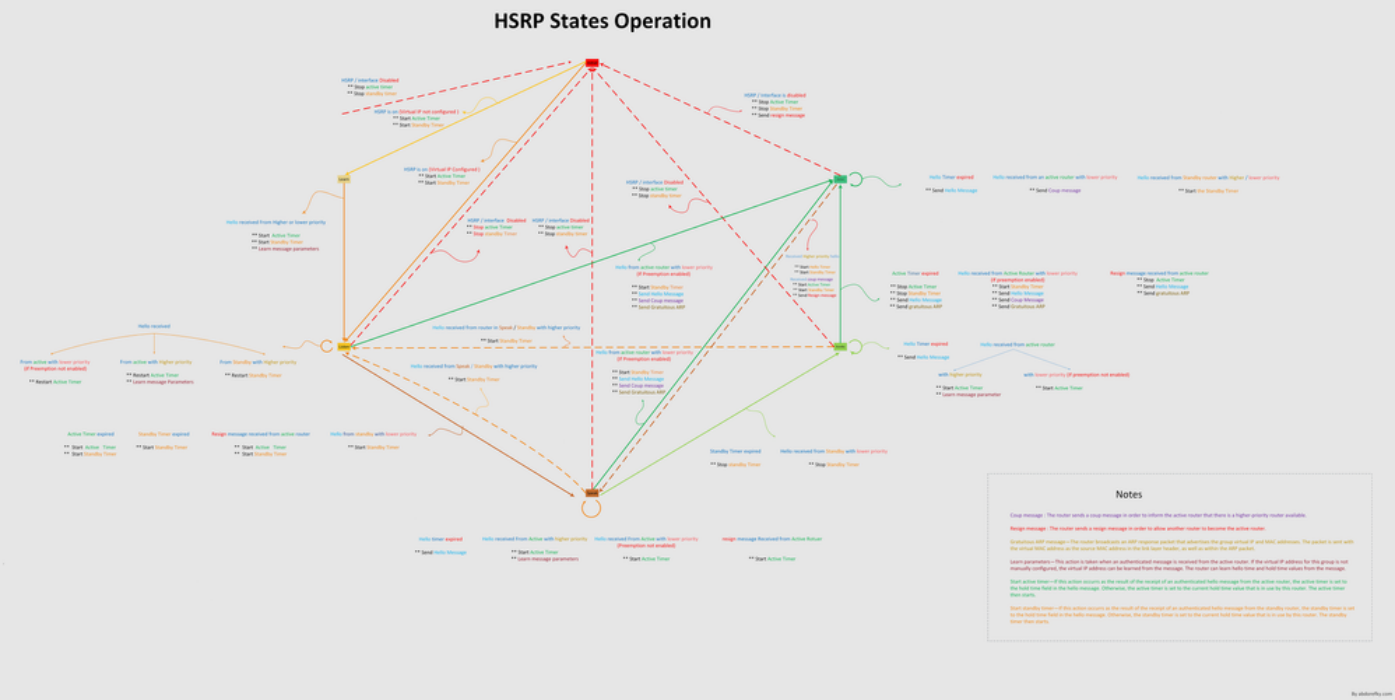
Brief	Aktion
A	Start active timer (Aktiver Zeitgeber starten): Wenn diese Aktion auftritt, nachdem eine authentifizier Hello-Nachricht vom aktiven Router empfangen wurde, wird der aktive Zeitgeber auf das Haltezeitfe der Hello-Nachricht gesetzt. Andernfalls wird der Aktiv-Timer auf den aktuellen Wert für die Haltezeit festgelegt, der von diesem Router verwendet wird. Danach wird der Aktiv-Timer gestartet.
B	Standby-Timer starten: Wenn diese Aktion aufgrund des Empfangs einer authentifizierten Hello-Nac vom Standby-Router erfolgt, wird der Standby-Timer auf das Feld "Hold Time" (Haltezeit) in der Hell Nachricht gesetzt. Andernfalls wird der Standby-Timer auf den aktuellen Wert für die Haltezeit festge der von diesem Router verwendet wird. Danach wird der Standby-Timer gestartet.
C	Aktiv-Timer stoppen. Der Aktiv-Timer wird angehalten.
G	Standby-Timer stoppen. Der Standby-Timer wird angehalten.
O	Parameter lernen. Diese Aktion wird ausgeführt, wenn eine authentifizierte Nachricht vom aktiven R empfangen wird. Wenn die virtuelle IP-Adresse für diese Gruppe nicht manuell konfiguriert wurde, k die virtuelle IP-Adresse aus der Nachricht ermittelt werden. Der Router kann die Werte für die Hello- und die Haltezeit aus der Nachricht ermitteln.
F	Hello-Nachricht senden: Der Router sendet eine Hello-Nachricht mit dem aktuellen Status, der Hello und der Haltezeit.
G	Coup-Nachricht senden. Der Router sendet eine Coup-Nachricht, um den aktiven Router darüber zu

	informieren, dass ein Router mit höherer Priorität verfügbar ist.
H	Resign-Nachricht senden. Der Router sendet eine Resign-Nachricht, damit ein anderer Router zum aktiven Router werden kann.
I	Gratuitous-ARP-Nachricht senden. Der Router überträgt ein ARP-Antwortpaket, das die virtuellen IP MAC-Adressen der Gruppe ankündigt. Das Paket wird mit der virtuellen MAC-Adresse als Quell-MA Adresse im Link-Layer-Header sowie innerhalb des ARP-Pakets gesendet.

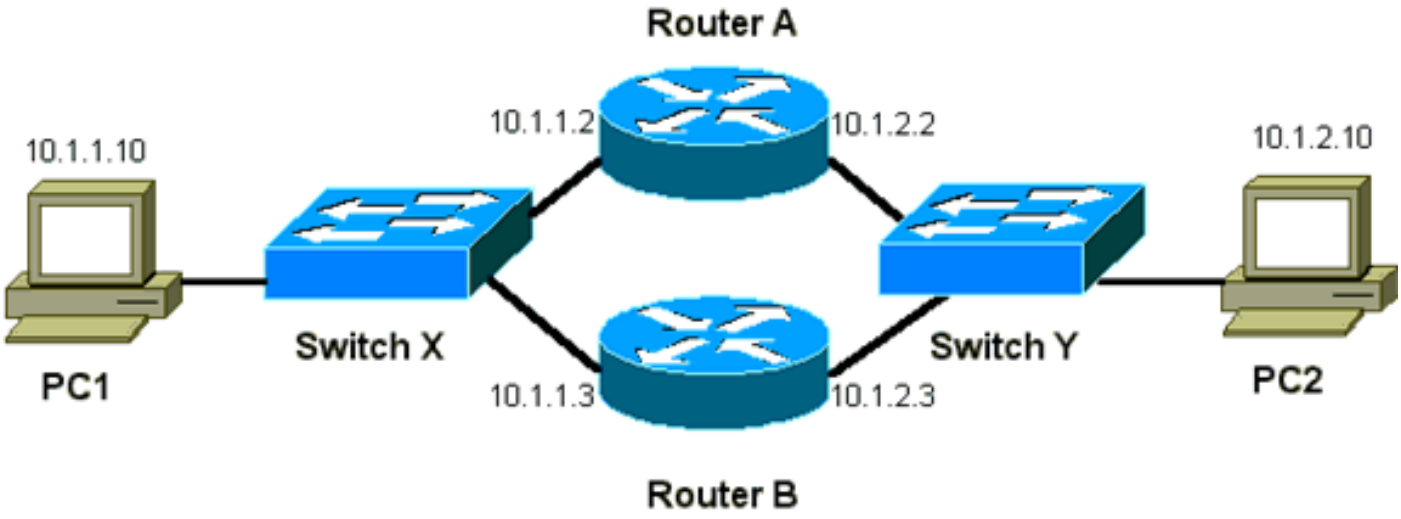
HSRP-Statustabelle

Das Diagramm in diesem Abschnitt zeigt die Statusübergänge des HSRP-Statusmoduls. Jedes Mal, wenn ein Ereignis auftritt, führt dies zu der zugehörigen Aktion, und der Router wechselt in den nächsten HSRP-Status. Im Diagramm kennzeichnen Zahlen Ereignisse und Buchstaben die zugehörige Aktion. In der Tabelle im Abschnitt HSRP-Ereignisse werden die Zahlen definiert, in der Tabelle im Abschnitt HSRP-Aktionen die Buchstaben. Verwenden Sie dieses Diagramm nur als Referenz. Das Diagramm ist detailliert und für allgemeine Fehlerbehebungszwecke nicht erforderlich.

Ein hochauflösendes Bild des Diagramms finden Sie bei den Informationen zur Funktionsweise der HSRP-Status.



Paketfluss



"Slot0:"	MAC-Adresse	IP-Adresse	Subnetzmaske	Standardgateway
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

Konfiguration von Router A (aktiver 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
```

Konfiguration von Router B (Standby-Router)

```
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
```

> **Hinweis**: In diesen Beispielen werden statische MAC-Adressen nur zur Veranschaulichung konfiguriert. Konfigurieren Sie statische MAC-Adressen nur, wenn es unbedingt nötig ist.

Wenn Sie Sniffer-Traces erhalten, um HSRP-Probleme zu beheben, müssen Sie das Konzept hinter Packet Flow verstehen. Router A verwendet die Priorität 200 und wird an beiden Schnittstellen zum aktiven Router. Im Beispiel in diesem Abschnitt haben Pakete vom Router, die für eine Host-Workstation bestimmt sind, die Quell-MAC-Adresse der physischen MAC-Adresse (BIA) des Routers. Pakete von den Host-Systemen, die für die HSRP-IP-Adresse bestimmt sind, weisen die Ziel-MAC-Adresse der virtuellen HSRP-MAC-Adresse auf. Beachten Sie, dass die MAC-Adressen nicht für jeden Flow zwischen dem Router und dem Host identisch sind.

Diese Tabelle zeigt die jeweiligen MAC- und IP-Adressinformationen pro Flow basierend auf

einem Sniffer-Trace von Switch X.

Paketfluss	Quell-MAC-Adresse	Ziel-MAC-Adresse	Quell-IP	Ziel-IP
Pakete von PC1, die für PC2 bestimmt sind	PC1 (0000.0c00.0001)	Virtuelle HSRP-MAC-Adresse von Router-A-Schnittstelle Ethernet 0 (0000.0c07.ac01)	10.1.1.10	10.1.2.10
Pakete, die von PC2 über Router A zurückgesendet werden und für PC1 bestimmt sind	Router A Ethernet 0 BIA (4000.0000.0010)	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.10
Pakete von PC1, die für die HSRP-Standby-IP-Adresse bestimmt sind (ICMP, Telnet)	PC1 (0000.0c00.0001)	Virtuelle HSRP-MAC-Adresse von Router-A-Schnittstelle Ethernet 0 (0000.0c07.ac01)	10.1.1.10	10.1.1.1
Pakete, die für die tatsächliche IP-Adresse des aktiven Routers bestimmt sind (ICMP, Telnet)	PC1 (0000.0c00.0001)	Router A Ethernet 0 BIA (4000.0000.0010)	10.1.1.10	10.1.1.2
Pakete, die für die tatsächliche IP-Adresse des Standby-Routers bestimmt sind (ICMP, Telnet)	PC1 (0000.0c00.0001)	Router B Ethernet 0 BIA (4000.0000.0020)	10.1.1.10	10.1.1.3

Fehlerbehebung bei HSRP – Fallstudien

Anwenderbericht #1: HSRP-Standby-IP-Adresse wird als doppelte IP-Adresse gemeldet

Diese Fehlermeldungen werden unter Umständen angezeigt:

```
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
```

Diese Fehlermeldungen weisen nicht unbedingt auf ein HSRP-Problem hin. Sie deuten eher auf ein mögliches Problem mit einer STP-Schleife (Spanning Tree Protocol) oder ein Router-/Switch-Konfigurationsproblem hin. Die Fehlermeldungen sind nur Symptome eines anderen Problems.

Darüber hinaus ist der ordnungsgemäße Betrieb von HSRP bei diesen Fehlermeldungen nicht beeinträchtigt. Das doppelte HSRP-Paket wird ignoriert. Diese Fehlermeldungen werden in 30-Sekunden-Intervallen gedrosselt. Allerdings können eine langsame Netzwerkleistung und Paketverluste aus der Netzwerkinstabilität resultieren, die zu den `STANDBY-3-DUPADDR`-Fehlermeldungen bei der HSRP-Adresse führt.

Diese Nachrichten weisen konkret darauf hin an, dass der Router ein Datenpaket erhalten hat, das von der HSRP-IP-Adresse in VLAN 25 mit den MAC-Adressen 0000.0c07.ac19 stammt. Da

die HSRP-MAC-Adresse 0000.0c07.ac19 lautet, hat entweder der betreffende Router sein eigenes Paket zurückerhalten, oder beide Router in der HSRP-Gruppe sind in den `aktiven Status` übergegangen. Da der Router sein eigenes Paket empfangen hat, ist das Problem höchstwahrscheinlich im Netzwerk und nicht im Router begründet. Dieses Verhalten kann durch verschiedene Probleme verursacht werden. Zu den möglichen Netzwerkproblemen, die diese Fehlermeldungen verursachen, zählen Folgende:

- Vorübergehende STP-Schleifen
- EtherChannel-Konfigurationsprobleme
- Doppelte Frames

Wenn Sie diese Fehlermeldungen beheben, lesen Sie die Schritte zur Fehlerbehebung im Abschnitt Fehlerbehebung bei HSRP in Catalyst Switches dieses Dokuments. Alle Module zur Fehlerbehebung sind in diesem Abschnitt beschrieben, der Module zur Konfiguration enthält. Notieren Sie außerdem alle Fehler aus dem Switch-Protokoll, und ziehen Sie bei Bedarf weitere Fallstudien zurate.

Sie können eine Zugriffsliste verwenden, um zu verhindern, dass der aktive Router sein eigenes Multicast-Hello-Paket empfängt. Dies ist jedoch nur eine Problemumgehung für die Fehlermeldungen und kaschiert das Symptom des Problems. Die Problemumgehung besteht darin, eine erweiterte eingehende Zugriffsliste auf die HSRP-Schnittstellen anzuwenden. Die Zugriffsliste blockiert den gesamten Datenverkehr, der von der physischen IP-Adresse stammt und an die Multicast-Adresse 224.0.0.2 aller Router gerichtet ist.

```
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
```

Anwenderbericht #2: Kontinuierliche Änderungen des HSRP-Status (aktiv, Standby, Sprechen) oder %HSRP-6-STATECHANGE

Diese Fehlermeldungen werden unter Umständen angezeigt:

```
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

Diese Fehlermeldungen beschreiben eine Situation, in der ein Standby-HSRP-Router nicht drei aufeinander folgende HSRP-Hello-Pakete von seinem HSRP-Peer empfangen hat. Die Ausgabe

zeigt, dass der Standby-Router vom `Standby-Status` in den `aktiven Status` wechselt. Kurz darauf kehrt der Router in den `Standby-Status` zurück. Sofern diese Fehlermeldung nicht während der Erstinstallation auftritt, ist sie wahrscheinlich nicht auf ein HSRP-Problem zurückzuführen. Die Fehlermeldungen deuten auf den Verlust von HSRP-Hellos zwischen den Peers hin. Um dieses Problem beheben zu können, müssen Sie die Kommunikation zwischen den HSRP-Peers überprüfen. Ein zufälliger, vorübergehender Verlust der Datenkommunikation zwischen den Peers ist das häufigste Problem, das zu diesen Meldungen führt. HSRP-Statusänderungen sind oft auf eine hohe CPU-Auslastung zurückzuführen. Wenn die Fehlermeldung durch eine hohe CPU-Auslastung verursacht wird, setzen Sie einen Sniffer im Netzwerk ein, und ermitteln Sie, welches System die hohe CPU-Auslastung verursacht.

Es gibt mehrere mögliche Ursachen für den Verlust von HSRP-Paketen zwischen den Peers. Am gängigsten sind Probleme auf der physischen Ebene, übermäßiger Netzwerkverkehr durch Spanning Tree-Probleme oder übermäßiger Datenverkehr durch die einzelnen VLANs. Wie bei Fallstudie Nr. 1 können alle Module zur Fehlerbehebung auf die Auflösung von HSRP-Statusänderungen angewendet werden, insbesondere auf das Layer-3-HSRP-Debugging.

Wenn der Verlust von HSRP-Paketen zwischen Peers auf übermäßigen Datenverkehr zurückzuführen ist, der von den einzelnen VLANs verursacht wird, können Sie SPD (Selective Packet Discard) optimieren oder erhöhen und die Warteschlangengröße beibehalten, um das Problem mit dem Verwerfen in der Eingabewarteschlange zu beheben.

Um die Größe von Selective Packet Discard (SPD) zu erhöhen, wechseln Sie in den Konfigurationsmodus, und führen Sie die folgenden Befehle auf den Cat6500-Switches aus:

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

!--- Hidden Command

(config)#ip spd queue min-threshold 500

!--- Hidden Command
```

Um die Größe der Warteschlange zu erhöhen, wechseln Sie in den VLAN-Schnittstellenmodus, und führen Sie den folgenden Befehl aus:

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

Nachdem Sie die Größe der SPD- und Haltewarteschlange erhöht haben, können Sie die Schnittstellenzähler löschen, wenn Sie den Befehl **`clear counter`** interface ausführen.

Anwenderbericht #3: HSRP erkennt Peer-Anwendungen nicht

Die Router-Ausgabe in diesem Abschnitt zeigt einen Router, der für HSRP konfiguriert ist, aber seine HSRP-Peers nicht erkennt. Dies geschieht, wenn der Router keine HSRP-Hellos vom Nachbarrouter empfängt. Um dieses Problem zu beheben, lesen Sie in diesem Dokument die Abschnitte Verifizieren der physischen Netzwerkverbindungen und Verifizieren der HSRP-Router-Konfiguration. Wenn die physischen Netzwerkverbindungen korrekt sind, überprüfen Sie, ob die VTP-Modi nicht übereinstimmen.

```
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
```

Anwenderbericht #4: HSRP-Statusänderungen und Switch-Berichte SYS-4-P2_WARN: 1/Host <mac_address> wechselt zwischen Port <port_1> und Port <port_2> in Syslog

Diese Fehlermeldungen werden unter Umständen angezeigt:

```
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

Bei Catalyst Switches meldet der Switch eine verschobene Host-MAC-Adresse, wenn sich die Host-MAC-Adresse innerhalb von 15 Sekunden zweimal verschiebt. Eine mögliche Ursache ist eine STP-Schleife. Der Switch verwirft Pakete von diesem Host etwa 15 Sekunden lang, um die Auswirkungen einer STP-Schleife zu minimieren. Wenn es sich bei der angegebenen MAC-Adressverschiebung zwischen zwei Ports um die virtuelle HSRP-MAC-Adresse handelt, ist das Problem höchstwahrscheinlich darauf zurückzuführen, dass beide HSRP-Router in den `aktiven Status` wechseln.

Wenn die angegebene MAC-Adresse nicht die virtuelle HSRP-MAC-Adresse ist, kann das Problem auf eine Schleife, Duplizierung oder Rücksendung von Paketen im Netzwerk hindeuten. Diese Bedingungen können zu HSRP-Problemen beitragen. Die häufigsten Ursachen für die Verschiebung von MAC-Adressen sind Probleme mit Spanning Tree oder Probleme auf der physischen Ebene.

Gehen Sie beim Beheben dieser Fehlermeldung folgendermaßen vor:

> **Hinweis**: Führen Sie außerdem die Schritte im Abschnitt Fehlerbehebung bei HSRP in Catalyst-Switches dieses Dokuments aus.

1. Ermitteln Sie die richtige Quelle (Port) für die MAC-Adresse des Hosts.
2. Trennen Sie den Port, der nicht die Host-MAC-Adresse beziehen darf.
3. Dokumentieren Sie die STP-Topologie pro VLAN, und überprüfen Sie sie auf STP-Fehler.
4. Überprüfen Sie die Port-Channeling-Konfiguration.Eine falsche Port-Channel-Konfiguration kann zum Flapping von Fehlermeldungen nach MAC-Adresse des Hosts führen. Dies ist auf das Load Balancing beim Port-Channeling zurückzuführen.

Anwenderbericht #5: Asymmetric Routing und HSRP (Excessive Flooding of Unicast Traffic in Netzwerken mit Routern, auf denen HSRP ausgeführt wird)

Beim asymmetrischen Routing verwenden die Sende- und Empfangspakete unterschiedliche Pfade zwischen dem Host und dem Peer, mit dem er kommuniziert. Dieser Paketfluss ist das Ergebnis der Konfiguration des Lastenausgleichs zwischen HSRP-Routern, die auf der HSRP-

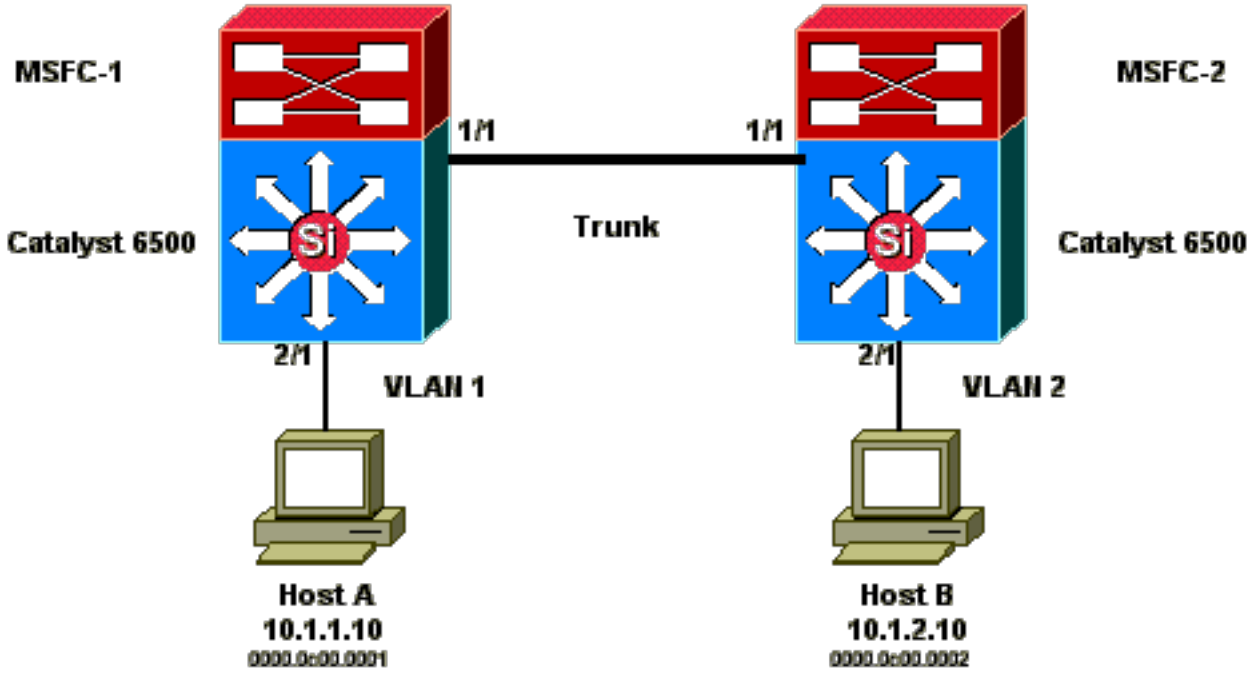
Priorität basieren und das HSRP auf "Aktiv" oder "Standby" setzen. Diese Art von Paketfluss in einer Switching-Umgebung kann zu übermäßigem Flooding mit unbekanntem Unicast führen. Außerdem können MLS-Einträge (Multilayer Switching) fehlen. Flooding mit unbekanntem Unicast tritt auf, wenn der Switch von allen Ports jeweils ein Unicast-Paket überträgt. Der Switch überträgt das Paket, da es keinen Eintrag für die Ziel-MAC-Adresse gibt. Durch dieses Verhalten wird die Verbindung nicht unterbrochen, da Pakete weiterhin weitergeleitet werden. Das Verhalten erklärt jedoch die vielen zusätzlichen Pakete an den Host-Ports. In dieser Fallstudie werden das Verhalten von asymmetrischem Routing und die Ursache des daraus folgenden Unicast-Flooding untersucht.

Symptome für asymmetrisches Routing:

- Übermäßiges Unicast-Flooding
- Fehlender MLS-Eintrag für Flows
- Sniffer-Trace, der zeigt, dass Pakete am Host-Port nicht für den Host bestimmt sind
- Erhöhte Netzwerklatenz bei L2-basierten Modulen für das Umschreiben von Paketen, z. B. Server-Load-Balancer, Web-Cache-Geräte und Netzwerk-AppliancesBeispiele hierfür sind Cisco LocalDirector und Cisco Cache Engine.
- Verworfene Pakete auf verbundenen Hosts und Workstations, die die zusätzliche Unicast-Flooding-Datenverkehrslast nicht verarbeiten können

  Hinweis: Die Standardalterungszeit für den ARP-Cache eines Routers beträgt vier Stunden. Die standardmäßige Alterungszeit des CAM-Eintrags (Content-Addressable Memory) auf dem Switch beträgt fünf Minuten. Die ARP-Alterungszeit der Host-Workstations ist für diese Diskussion nicht von Bedeutung. Im Beispiel wird jedoch die ARP-Alterungszeit auf vier Stunden festgelegt.

Dieses Diagramm veranschaulicht dieses Problem. Dieses Topologiebeispiel umfasst Catalyst 6500 mit Multilayer-Switch-Funktionskarten (MSFCs) auf jedem Switch. In diesem Beispiel werden zwar MSFCs verwendet, Sie können jedoch stattdessen einen beliebigen Router verwenden. Beispiele für Router, die Sie verwenden können, sind das Route Switch-Modul (RSM), der Gigabit-Switch-Router (GSR) und Cisco 7500. Die Hosts sind direkt mit den Ports am Switch verbunden. Die Switches sind über einen Trunk miteinander verbunden, der als Träger für Datenverkehr für VLAN 1 und VLAN 2 fungiert.



Diese Ausgaben sind Auszüge aus der Konfiguration des Befehls **show standby** von jedem MSF.

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
```

Hinweis: Auf MSFC1 befindet sich VLAN 1 im `aktiven` HSRP-Status und VLAN 2 im HSRP-`Standby-`Status. Auf MSFC2 befindet sich VLAN 2 im `aktiven HSRP-Status` und VLAN 1 im HSRP-`Standby-Status`. Das Standardgateway der Hosts ist die jeweilige Standby-IP-Adresse.

1. Zu Beginn sind alle Caches leer. Host A nutzt MSFC1 als Standardgateway. Host B nutzt MSFC2.**ARP- und MAC-Adresstabellen, bevor ein Ping initiiert wird Hinweis:** Aus Gründen der Kürze sind die Switch 1-MAC-Adresse für den Router, die HSRP- und die MAC-Adresse, nicht in den anderen Tabellen in diesem Abschnitt enthalten.
2. Host A sendet einen Ping an Host B, woraufhin Host A ein ICMP-Echo-Paket sendet. Da sich jeder Host in einem separaten VLAN befindet, leitet Host A seine für Host B bestimmten Pakete an sein Standardgateway weiter. Damit dieser Prozess stattfinden kann, muss Host A ein ARP senden, um seine Standardgateway-MAC-Adresse 10.1.1.1 aufzulösen.**ARP- und MAC-Adresstabellen, wenn Host A ein ARP für das Standardgateway gesendet hat**
3. MSFC1 empfängt das Paket, schreibt das Paket neu und leitet es an Host B weiter. Um das Paket neu zu schreiben, sendet MSFC1 eine ARP-Anforderung für Host B, da sich der Host an einer direkt verbundenen Schnittstelle befindet. MSFC2 hat noch keine Pakete in diesem Flow empfangen. Wenn MSFC1 die ARP-Antwort von Host B empfängt, ermitteln beide Switches den Quellport, der Host B zugeordnet ist.**ARP- und MAC-Adresstabellen, wenn Host A ein Paket an das Standardgateway und MSFC1 ARP für Host B gesendet hat**
4. Host B empfängt das Echopaket von Host A über MSFC1. Host B muss nun eine Echo-Antwort an Host A senden. Da Host A sich in einem anderen VLAN befindet, leitet Host B die

Antwort über sein Standard-Gateway MSFC2 weiter. Um das Paket über MSFC2 weiterzuleiten, muss Host B ein ARP für seine Standardgateway-IP-Adresse 10.1.2.1 senden.**ARP- und MAC-Adresstabellen, wenn Host B ein ARP für sein Standardgateway gesendet hat**

5. Host B leitet das Echo-Antwortpaket jetzt an MSFC2 weiter. MSFC2 sendet eine ARP-Anfrage für Host A, da er direkt mit VLAN 1 verbunden ist. Switch 2 trägt die MAC-Adresse von Host B in seiner MAC-Adresstabelle ein.**ARP- und MAC-Adresstabellen, nachdem das Echopaket von Host A empfangen wurde**
6. Die Echo-Antwort erreicht Host A, und der Flow ist abgeschlossen.

Folgen von asymmetrischem Routing

Betrachten Sie den Fall des kontinuierlichen Pings von Host B nach Host A. Denken Sie daran, dass Host A das Echo-Paket an MSFC1 sendet, und Host B die Echo-Antwort an MSFC2, das sich in einem asymmetrischen Routing-Zustand befindet. Switch 1 ermittelt die Quell-MAC-Adresse von Host B nur dann, wenn Host B auf eine ARP-Anfrage von MSFC1 antwortet. Dies liegt daran, dass Host B MSFC2 als Standardgateway verwendet und keine Pakete an MSFC1 und folglich auch nicht an Switch 1 sendet. Da die ARP-Zeitüberschreitung standardmäßig vier Stunden beträgt, veraltet die MAC-Adresse von Host B auf Switch 1 standardmäßig nach fünf Minuten. Switch 2 altert Host A nach fünf Minuten. Infolgedessen muss Switch 1 jedes Paket mit einer Ziel-MAC-Adresse von Host B als unbekannten Unicast behandeln. Der Switch überträgt das Paket, das von Host A stammt und für Host B bestimmt ist, von allen Ports. Darüber hinaus gibt es auch keinen MLS-Eintrag, da kein MAC-Adresseintrag für Host B auf Switch 1 vorhanden ist.

ARP- und MAC-Adresstabellen nach 5 Minuten mit kontinuierlichen Pings von Host A an Host B

ARP-Tabelle Host A	MAC-Adresstabelle MAC-VLAN-Port Switch 1	ARP-Tabelle MSFC1	ARP-Tabelle MSFC2	MAC-Adresstabelle MAC-VLAN-Port Switch 2	ARP-Tabelle Host B
10.1.1.1 : 0000.0c07.ac01 10.1.1.3 : 0003.6bf1.2a0	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001 10.1.2.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002 10.1.1.10 0000.0c00.0001	0000.0c00.0002 2 2/1	10.1.2.2 : 0003.6bf1.2a0 10.1.2.1 : 0000.0c07.ac0

Bei den Echoantwortpaketen von Host B tritt dasselbe Problem auf, wenn der MAC-Adresseintrag für Host A auf Switch 2 veraltet ist. Host B leitet die Echo-Antwort an MSFC2 weiter, die das Paket wiederum weiterleitet und an VLAN 1 sendet. Der Switch hat keinen Eintrag für Host A in der MAC-Adresstabelle und muss das Paket von allen Ports in VLAN 1 übertragen.

Probleme mit asymmetrischem Routing unterbrechen die Verbindung nicht. Asymmetrisches Routing kann jedoch zu übermäßigem Unicast-Flooding und fehlenden MLS-Einträgen führen. Es gibt drei Konfigurationsänderungen, die diese Situation beheben können:

- Ändern Sie die MAC-Alterungszeit auf den jeweiligen Switches in 14.400 Sekunden (4 Stunden) oder länger.
- Ändern Sie die ARP-Zeitüberschreitung auf den Routern in 5 Minuten (300 Sekunden).
- Setzen Sie die MAC-Alterungszeit und die ARP-Zeitüberschreitung auf denselben Zeitüberschreitungswert.

Die bevorzugte Methode ist, die MAC-Alterungszeit in 14.400 Sekunden zu ändern. Konfigurationsrichtlinien:

- Cisco IOS Software:**mac address-table aging-time <Sekunden> vlan <vlan_id>**

Anwenderbericht #6: Virtuelle HSRP-IP-Adresse wird als andere IP-Adresse gemeldet

Die Fehlermeldung `STANDBY-3-DIFFVIP1` tritt auf, wenn aufgrund von Bridging-Schleifen auf dem Switch ein Inter-VLAN-Leck vorliegt.

Wenn diese Fehlermeldung angezeigt wird und ein Inter-VLAN-Leck aufgrund von Bridging-Schleifen auf dem Switch vorliegt, gehen Sie wie folgt vor, um den Fehler zu beheben:

1. Identifizieren Sie den Pfad, über den die Pakete zwischen den Endknoten übertragen werden.Wenn sich auf diesem Pfad ein Router befindet, gehen Sie wie folgt vor:Führen Sie eine Fehlerbehebung für den Pfad vom ersten Switch zum Router durch.Führen Sie eine Fehlerbehebung für den Pfad vom Router zum zweiten Switch durch.
2. Stellen Sie eine Verbindung zu jedem Switch auf dem Pfad her, und überprüfen Sie den Status der Ports, die auf dem Pfad zwischen den Endknoten verwendet werden.

Anwenderbericht #7: HSRP verursacht Verletzung der MAC-Adresse an einem sicheren Port

Wenn Port-Sicherheit an den Switch-Ports konfiguriert ist, die mit den HSRP-fähigen Routern verbunden sind, führt dies zu einer MAC-Verletzung, da nicht die gleiche sichere MAC-Adresse an mehreren Schnittstellen verwendet werden kann. In diesen Situationen tritt eine Sicherheitsverletzung an einem sicheren Port auf:

- Die maximale Anzahl sicherer MAC-Adressen wird der Adresstabelle hinzugefügt, und eine Station, deren MAC-Adresse nicht in der Adresstabelle enthalten ist, versucht, auf die Schnittstelle zuzugreifen.
- Eine Adresse, die an einer sicheren Schnittstelle ermittelt oder konfiguriert wurde, wird an einer anderen sicheren Schnittstelle im selben VLAN erkannt.

Standardmäßig führt eine Port-Sicherheitsverletzung dazu, dass die Switch-Schnittstelle durch den Fehler deaktiviert und sofort heruntergefahren wird, wodurch die HSRP-Statusmeldungen zwischen den Routern blockiert werden.

Problemumgehung

- Führen Sie auf den Routern den Befehl **standby use-bia** aus. Dadurch werden die Router gezwungen, statt der virtuellen MAC-Adresse eine BIA für HSRP zu verwenden.
- Deaktivieren Sie Port-Sicherheit an den Switch-Ports, die mit den HSRP-fähigen Routern verbunden sind.

Fallstudie #9: %Interface Hardware unterstützt nicht mehrere Gruppen

Wenn mehrere HSRP-Gruppen an der Schnittstelle erstellt werden, wird diese Fehlermeldung angezeigt:

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

Diese Fehlermeldung ist auf die Hardwarebeschränkung auf einigen Routern oder Switches

zurückzuführen. Es ist nicht möglich, die Einschränkung durch Softwaremethoden zu umgehen. Das Problem ist, dass jede HSRP-Gruppe eine zusätzliche MAC-Adresse an der Schnittstelle verwendet, sodass der Ethernet-MAC-Chip mehrere programmierbare MAC-Adressen unterstützen muss, um mehrere HSRP-Gruppen zu aktivieren.

Sie können dieses Problem umgehen, indem Sie den Schnittstellenkonfigurationsbefehl **standby use-bia** ausführen, der die Burned-In-Adresse (BIA) der Schnittstelle anstelle der vorab zugewiesenen MAC-Adresse als virtuelle MAC-Adresse verwendet.

Fehlerbehebung bei HSRP in Catalyst-Switches

A. Überprüfen der HSRP-Router-Konfiguration

1. Überprüfung der eindeutigen IP-Adresse der Router-Schnittstelle

Vergewissern Sie sich, dass jeder HSRP-Router pro Schnittstelle eine eindeutige IP-Adresse für jedes Subnetz hat. Stellen Sie außerdem sicher, dass bei jeder Schnittstelle der Status des Leitungsprotokolls `up` (aktiv) lautet. Um den aktuellen Status jeder Schnittstelle schnell zu überprüfen, führen Sie den Befehl **show ip interface brief** aus. Hier ein Beispiel:

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. Überprüfung der Standby-IP-Adressen (HSRP) und Standby-Gruppennummern

Überprüfen Sie, ob die konfigurierten Standby-IP-Adressen (HSRP) und Standby-Gruppennummern mit jedem an HSRP teilnehmenden Router übereinstimmen. Eine Nichtübereinstimmung von Standby-Gruppen oder HSRP-Standby-Adressen kann zu HSRP-Problemen führen. Der Befehl **show standby** gibt die Konfiguration der Standby-Gruppe und der Standby-IP-Adresse jeder Schnittstelle zurück. Hier ein Beispiel:

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-Vl10-110" (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-Vl11-111" (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-Vl10-110" (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-Vl11-111" (default) FLAGS: 0/1

3. Überprüfen Sie, ob sich die Standby-IP-Adresse (HSRP) je nach Schnittstelle unterscheidet.

Vergewissern Sie sich, dass die Standby-IP-Adresse (HSRP) gegenüber der konfigurierten IP-Adresse an jeder Schnittstelle eindeutig ist. Der Befehl **show standby** ist eine Kurzreferenz, um diese Informationen anzuzeigen. Hier ein Beispiel:

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-Vl10-110" (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-Vl11-111" (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-Vl10-110" (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-Vl11-111" (default) FLAGS: 0/1

4. Verwenden des Befehls "standy use-bia"

Sofern HSRP nicht an einer Token Ring-Schnittstelle konfiguriert ist, wird der Befehl **standby use-bia** nur unter besonderen Umständen verwendet. Dieser Befehl weist den Router an, seine BIA anstelle der virtuellen HSRP-MAC-Adresse für die HSRP-Gruppe zu verwenden. Wenn in einem Token Ring-Netzwerk SRB (Source-Route Bridging) verwendet wird, ermöglicht der Befehl **standby use-bia** dem neuen aktiven Router, den RIF-Cache (Routing Information Field) des Hosts mit einem Gratuitous-ARP zu aktualisieren. Allerdings verarbeiten nicht alle Host-Implementierungen das Gratuitous-ARP korrekt. Eine weitere Einschränkung für den Befehl **standby use-bia** betrifft Proxy-ARP. Ein Standby-Router kann die nicht mehr verfügbare Proxy-ARP-Datenbank des ausgefallenen aktiven Routers nicht ersetzen.

5. Konfiguration der Zugriffsliste überprüfen

Stellen Sie sicher, dass die auf allen HSRP-Peers konfigurierten Zugriffslisten keine HSRP-Adressen filtern, die an ihren Schnittstellen konfiguriert sind. Überprüfen Sie insbesondere, welche Multicast-Adresse verwendet wird, um Datenverkehr an alle Router in einem Subnetz (**224.0.0.2**) zu senden. Stellen Sie außerdem sicher, dass der UDP-Datenverkehr, der für den HSRP-Port **1985** bestimmt ist, nicht gefiltert wird. HSRP verwendet diese Adresse und diesen Port, um Hello-Pakete zwischen Peers zu senden. Führen Sie den Befehl **show access-lists** als Kurzreferenz aus, um die auf dem Router konfigurierten Zugriffslisten zu notieren. Hier ein Beispiel:

```
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. Überprüfen der Catalyst Fast EtherChannel- und Trunking-Konfiguration

1. Überprüfen der Trunking-Konfiguration

Wenn ein Trunk zum Verbinden der HSRP-Router verwendet wird, überprüfen Sie die Trunking-Konfigurationen auf den Routern und Switches. Es gibt fünf mögliche Trunking-Modi:

- on
- desirable (gewünscht)
- auto (automatisch)
- off
- nonegotiate (Keine Aushandlung)

Stellen Sie sicher, dass die konfigurierten Trunking-Modi die gewünschte Trunking-Methode bereitstellen.

Verwenden Sie die `gewünschte` Konfiguration für Switch-zu-Switch-Verbindungen, wenn Sie HSRP-Probleme beheben. Diese Konfiguration kann Probleme isolieren, bei denen Switch-Ports die Trunks nicht korrekt einrichten können. Legen Sie eine Router-zu-Switch-Konfiguration auf „nonegotiate“ (keine Aushandlung) fest, da die meisten Cisco IOS-Router die Aushandlung eines Trunks nicht unterstützen.

Überprüfen Sie für den IEEE 802.1Q (dot1q) Trunking-Modus, ob beide Seiten des Trunks für die Verwendung desselben nativen VLAN und der gleichen Kapselung konfiguriert sind. Da Cisco Produkte das native VLAN standardmäßig nicht taggen, führt eine Nichtübereinstimmung der nativen VLAN-Konfigurationen zu keiner Konnektivität in nicht übereinstimmenden VLANs. Überprüfen Sie abschließend, ob der Trunk als Träger für die auf dem Router konfigurierten VLANs konfiguriert ist, und stellen Sie sicher, dass die VLANs nicht entfernt wurden und im Fall von mit dem Router verbundenen Ports im STP-Status sind. Geben Sie den Befehl **show interfaces <Schnittstelle> trunk** ein, um eine Kurzreferenz mit diesen Informationen zu erhalten. Hier ein Beispiel:

```
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. Überprüfen der Fast EtherChannel-Konfiguration (Port-Channel)

Wenn ein Port-Channel zum Verbinden der HSRP-Router verwendet wird, überprüfen Sie die EtherChannel-Konfiguration auf den Routern und Switches. Konfigurieren Sie einen Switch-zu-Switch-Port-Channel auf mindestens einer Seite wie gewünscht. Die andere Seite kann sich in einem der folgenden Modi befinden:

- on
- desirable (gewünscht)
- auto (automatisch)

In diesem Beispiel gehören Schnittstellen jedoch nicht zu einem Port-Channel:

```
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. MAC-Adressenweiterleitungstabelle des Switches untersuchen

Überprüfen Sie, ob die Einträge der MAC-Adresstabelle auf dem Switch für die HSRP-Router für die virtuelle HSRP-MAC-Adresse und die physischen BIAs vorhanden sind. Der Befehl **show standby** auf dem Router gibt die virtuelle MAC-Adresse zurück. Der Befehl **show interface** gibt die physische BIA zurück. Beispielausgaben:

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-Vl10-110" (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-Vl11-111" (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

Überprüfen Sie unbedingt die CAM-Alterungszeit, um festzustellen, wie schnell die Einträge veralten. Wenn die Zeit dem konfigurierten Wert für die STP-Weiterleitungsverzögerung entspricht, der standardmäßig 15 Sekunden beträgt, besteht sehr wahrscheinlich eine STP-Schleife im Netzwerk. Beispiel für die Befehlsausgabe:

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. Verifizieren der physischen Netzwerkverbindungen

Wenn mehr als ein Router in einer HSRP-Gruppe aktiv wird, empfangen diese Router die Hello-Pakete von anderen HSRP-Peers nicht konsistent. Probleme auf der physischen Ebene können die konsistente Weitergabe von Datenverkehr zwischen Peers verhindern und dieses Szenario verursachen. Denken Sie daran, die physische Verbindung und die IP-Verbindung zwischen den HSRP-Peers zu überprüfen, um HSRP-Fehler beheben zu können. Führen Sie den Befehl **show standby** aus, um die Konnektivität zu überprüfen. Hier ein Beispiel:

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-Vl10-110" (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-Vl11-111" (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-Vl10-110" (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. Schnittstellenstatus überprüfen

Überprüfen Sie die Schnittstellen. Überprüfen Sie, ob der Status aller für HSRP konfigurierten Schnittstellen `up/up` (aktiv/aktiv) lautet, wie dieses Beispiel zeigt:

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

Wenn der administrative Status einer Schnittstelle `down/down` lautet, wechseln Sie auf dem Router in den Konfigurationsmodus, und führen Sie den schnittstellenspezifischen Befehl **no shutdown** aus. Hier ein Beispiel:

```
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

Wenn der Status von Schnittstellen `down/down` (inaktiv/inaktiv) oder `up/down` (aktiv/inaktiv) lautet, überprüfen Sie das Protokoll auf Benachrichtigungen zu Schnittstellenänderungen. Bei softwarebasierten Cisco IOS-Switches werden diese Meldungen in Situationen angezeigt, in denen der Link-Status `up/down` (aktiv/inaktiv) lautet:

```
%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
```

Überprüfen Sie die Ports, Kabel und alle Transceiver oder anderen Geräte zwischen den HSRP-Peers. Hat jemand physische Verbindungen getrennt oder gelockert? Gibt es Schnittstellen, die den Link immer wieder verlieren? Wurden die richtigen Kabeltypen verwendet? Überprüfen Sie die Schnittstellen auf Fehler, wie dieses Beispiel zeigt:

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. Verbindungswechsel und Portfehler

Überprüfen Sie die Switch-Ports auf Link-Änderungen und andere Fehler. Führen Sie diese Befehle aus, und überprüfen Sie die Ausgabe:

- **show logging**
- **show interfaces <interface> counters**
- **show interfaces <interface> status**

Mit diesen Befehlen können Sie feststellen, ob ein Problem mit der Verbindung zwischen Switches und anderen Geräten besteht.

Diese Meldungen sind in Situationen mit dem Link-Status `up/down` (aktiv/inaktiv) normal:

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

Führen Sie den Befehl **show interfaces <interface> status** aus, um den allgemeinen Status eines Ports zu bestimmen. Hier ein Beispiel:

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

Ist der Schnittstellenstatus "`Verbunden`", "Verbindung" oder "`errdisable`"? Wenn der Status `notconnect` (nicht verbunden) lautet, überprüfen Sie, ob das Kabel auf beiden Seiten eingesteckt ist. Überprüfen Sie, ob das richtige Kabel verwendet wurde. Wenn der Status `errdisable` (wegen Fehler deaktiviert) lautet, überprüfen Sie die Zähler auf übermäßige Fehler. Weitere Informationen finden Sie unter Recover Erdisable Port State on Cisco IOS Platforms.

Für welches VLAN ist dieser Port konfiguriert? Vergewissern Sie sich, dass die andere Seite der Verbindung für dasselbe VLAN konfiguriert ist. Wenn der Link als Trunk konfiguriert ist, vergewissern Sie sich, dass beide Seiten des Trunks als Träger für dieselben VLANs fungieren.

Wie lautet die Geschwindigkeits- und Duplexkonfiguration? Wenn der Einstellung „a-“ vorangestellt ist, ist der Port so konfiguriert, dass Geschwindigkeit und Duplex automatisch ausgehandelt werden. Andernfalls hat der Netzwerkadministrator eine Konfiguration voreingestellt. Bei der Konfiguration von Geschwindigkeit und Duplex für eine Verbindung müssen die Einstellungen auf beiden Seiten des Links übereinstimmen. Wenn ein Switch-Port für automatische Aushandlung konfiguriert ist, muss auch die andere Seite der Verbindung für automatische Aushandlung konfiguriert werden. Wenn auf einer Seite eine bestimmte Geschwindigkeits- und Duplexeinstellung fest eingestellt ist, muss die andere Seite ebenfalls fest eingestellt werden. Wenn Sie auf einer Seite die automatische Aushandlung beibehalten, während Sie für die andere Seite feste Einstellungen vornehmen, funktioniert der Prozess der automatischen Aushandlung nicht mehr.

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**

Ist eine hohe Anzahl von `Align-Err`, `FCS-Err` oder `Runts` vorhanden? Diese weisen auf eine Geschwindigkeits- oder Duplex-Diskrepanz zwischen dem Port und dem verbundenen Gerät hin. Ändern Sie die Geschwindigkeits- und Duplexeinstellungen für diesen Port, um diese Fehler zu beheben.

Führen Sie den Befehl **show mac** aus, um zu überprüfen, ob der Port Datenverkehr durchlässt. Die Spalten `In` und `Out` geben die Anzahl der Unicast-, Multicast- und Broadcast-Pakete an, die an einem bestimmten Port empfangen und übertragen werden. Die unteren Zähler zeigen, wie viele Pakete verworfen wurden oder verloren gegangen sind und ob diese Pakete Teil des eingehenden oder ausgehenden Datenverkehrs waren. `Lrn-Discrd`, `In-Lost` und `Out-Lost` geben die Anzahl der Pakete an, die aufgrund unzureichender Puffer irrtümlich weitergeleitet oder verworfen wurden.

`L2Switch_1`#show interfaces gi1/0/13 counters Port InOctets InUcastPkts InMcastPkts InBcastPkts Gi1/0/13 304933333 1180453 1082538 14978 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Gi1/0/13 282752538 276716 824562 588960

3. Überprüfen der IP-Verbindung

Verifizieren Sie die IP-Konnektivität. Geben Sie einen IP-Ping vom verbundenen Router zum Remote-HSRP-Gerät ein. Dies hilft, vorübergehende Verbindungsverluste aufzudecken. Ein erweiterter Ping ist nur im Aktivierungsmodus verfügbar. Beispiel für die Befehlsausgabe:

Router_1#show run interface vlan 10 Building configuration... Current configuration : 141 bytes ! interface Vlan10 ip address 192.168.10.1 255.255.255.0 standby 110 ip 192.168.10.100 standby 110 priority 110 standby 110 preempt end Router_2#show run interface vlan 10 Building configuration... Current configuration : 120 bytes ! interface Vlan10 ip address 192.168.10.2 255.255.255.0 standby 110 ip 192.168.10.100 standby 110 priority 109 end Router_1#ping 192.168.10.2 repeat 1500 Type escape sequence to abort. Sending 1500, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/9 ms

Senden Sie den Ping von jedem HSRP-Router an seine Peers, um den Ort des Verbindungsfehlers zu bestimmen.

4. Überprüfen Sie die unidirektionale Verbindung

Überprüfen Sie den Switch auf unidirektionale Links zwischen HSRP-Peers. Ein unidirektionaler Link liegt vor, wenn zwar der von einem lokalen Gerät über einen Link übertragene Datenverkehr vom benachbarten Gerät empfangen wird, der vom benachbarten Gerät übertragene Datenverkehr umgekehrt jedoch nicht vom lokalen Gerät empfangen wird. Diese Funktion wird als aggressiver UDLD-Modus (UniDirectional Link Detection) bezeichnet. Die Verwendung von UDLD ist nur möglich, wenn beide Seiten der Verbindung die Funktion unterstützen. Der aggressive UDLD-Modus ermittelt auf L2, ob ein Link ordnungsgemäß verbunden ist und ob der Datenverkehr bidirektional zwischen den richtigen Nachbarn fließt. Beispiele für die Befehlsausgaben:

> **Hinweis**: Navigieren Sie zum nächsten Link, um die UDLD-Funktion zu verstehen und zu konfigurieren. Dies hängt von der verwendeten Plattform ab.

Eine weitere Option zur Verifizierung einer unidirektionalen Verbindung, wenn UDLD nicht verfügbar ist, bietet das Cisco Discovery Protocol (CDP). Die Aktivierung von CDP ist eine weitere Möglichkeit, zu erkennen, ob ein unidirektionaler Link vorliegt. Wenn nur eine Seite eines Links das Nachbargerät sehen kann, tauschen Sie das Kabel zwischen den Geräten aus, und überprüfen Sie es auf fehlerhafte Schnittstellen.

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 mcpre 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. Weitere Fehlerbehebungsreferenzen für die physische Schicht

Weitere Informationen finden Sie in diesen Dokumenten:

- Konfiguration und Fehlerbehebung für die automatische Ethernet-10/100/1000-Mb-Halb-/Vollduplex-Aushandlung
- Wiederherstellen Errdisable Port State auf Cisco IOS-Plattformen
- Behebung von Kompatibilitätsproblemen zwischen Cisco Catalyst Switches und NICs
- Abschnitt mit Informationen zu Daten-Link-Fehlern unter Beheben von Kompatibilitätsproblemen zwischen Cisco Catalyst Switches und NICs
- Fehlerbehebung bei Switchport- und Schnittstellenproblemen

D. Layer-3-HSRP-Debugging

Wenn sich der HSRP-Status häufig ändert, verwenden Sie die HSRP-Debug-Befehle (im Aktivierungsmodus) auf dem Router, um die HSRP-Aktivität zu überwachen. Anhand dieser Informationen können Sie feststellen, welche HSRP-Pakete vom Router empfangen und gesendet werden. Sammeln Sie diese Informationen, wenn Sie eine Serviceanfrage beim technischen Support von Cisco erstellen. Die Debug-Ausgabe zeigt auch HSRP-Statusinformationen mit detaillierten Angaben zu HSRP-Hello-Paketen.

1. Standard-HSRP-Debugging

Aktivieren Sie in Cisco IOS die HSRP-Debug-Funktion mit dem Befehl **debug standby**. Diese Informationen sind nützlich, wenn Probleme nur sporadisch auftreten und nur wenige Schnittstellen betreffen. Mit dem Debug-Befehl können Sie ermitteln, ob der betreffende HSRP-Router HSRP-Hello-Pakete in bestimmten Intervallen empfängt und sendet. Wenn der Router keine Hello-Pakete empfängt, können Sie daraus schließen, dass entweder der Peer die Hello-Pakete nicht überträgt oder das Netzwerk die Pakete verwirft.

Command	Zweck
debug standby	Aktiviert das HSRP-Debugging

Beispiel für die Befehlsausgabe:

Router_1#debug standby HSRP debugging is on Jul 29 16:12:16.889: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100 Jul 29 16:12:16.996: HSRP: Vl11 Grp 111 Hello in 192.168.11.2 Standby pri 109 vIP 192.168.11.100 Jul 29 16:12:17.183: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100 Jul 29 16:12:17.366: HSRP: Vl11 Grp 111 Hello out 192.168.11.1 Active pri 110 vIP 192.168.11.100 Jul 29 16:12:18.736: HSRP: Vl10 Interface adv in, Passive, active 0, passive 1, from 192.168.10.2 Jul 29 16:12:19.622: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100

2. Bedingtes HSRP-Debugging (Beschränkung der Ausgabe auf Basis einer Standby-Gruppe und/oder eines VLAN)

Mit Cisco IOS-Software Version 12.0(3) wurde eine Debug-Bedingung eingeführt, die es ermöglicht, die Ausgabe des Befehls **debug standby** basierend auf der Schnittstellen- und Gruppennummer zu filtern. Bei diesem Befehl wird das Debug-Bedingungsparadigma verwendet, das mit Cisco IOS-Software Version 12.0 eingeführt wurde.

Command	Zweck
debug condition standby <Schnittstelle> <Gruppe>	Aktiviert das bedingte HSRP-Debugging der Gruppe (0–255).

Die Schnittstelle muss eine gültige Schnittstelle sein, die HSRP unterstützen kann. Die Gruppe kann eine beliebige Gruppe zwischen 0 und 255 sein. Für nicht vorhandene Gruppen kann eine Debug-Bedingung festgelegt werden. Dadurch können Debugs während der Initialisierung einer neuen Gruppe erfasst werden. Die Debug-Standby-Funktion muss aktiviert sein, damit Debug-Ausgaben erzeugt werden können. Wenn keine Standby-Debug-Bedingungen vorhanden sind, wird die Debug-Ausgabe für alle Gruppen an allen Schnittstellen erzeugt. Wenn mindestens eine Standby-Debug-Bedingung erfüllt ist, wird die Standby-Debug-Ausgabe basierend auf allen Standby-Debug-Bedingungen gefiltert. Beispiel für die Befehlsausgabe:

```
Router_1#debug condition standby vlan 10 110
Condition 1 set
Router_1#
Jul 29 16:16:20.284: Vl10 HSRP110 Debug: Condition 1, hsrp Vl10 HSRP110 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
Jul 29 16:16:44.797: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:45.381: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:16:47.231: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:48.248: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
```

3. Verbessertes HSRP-Debugging

Seit Cisco IOS-Software Version 12.1(1) ist erweitertes HSRP-Debugging verfügbar. Damit die relevanten Informationen leichter zu finden sind, begrenzt das erweiterte HSRP-Debugging das Grundrauschen der regelmäßigen Hello-Nachrichten und liefert zusätzliche Statusinformationen. Diese Informationen sind besonders nützlich, wenn Sie beim Erstellen einer Serviceanfrage mit einem Mitarbeiter des technischen Supports von Cisco zusammenarbeiten.

Command	Zweck
debug standby	Gibt alle HSRP-Fehler, -Ereignisse und -Pakete zur
debug standby errors	Gibt HSRP-Fehler zurück.
debug standby events [[all] | [hsrp | redundancy | track]] [detail]	Gibt HSRP-Ereignisse zurück.
debug standby packets [[all | terse] | [advertise | coup | hello | resign]] [detail]	Gibt HSRP-Pakete zurück.
debug standby terse	Anzeige eines begrenzten Bereichs von HSRP-Feh Ereignissen und -Paketen

Beispiel für die Befehlsausgabe:

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: Vl10 Grp 110 Resign in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Standby: i/Resign rcvd (110/192.168.10.1) *Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Active router is local, was 192.168.10.1 *Jul 29 16:49:35.416: HSRP: Vl10 Nbr 192.168.10.1 no longer active for group 110 (Standby) *Jul 29 16:49:35.417: HSRP: Vl10 Nbr 192.168.10.1 Was active or standby - start passive holddown *Jul 29 16:49:35.417: HSRP: Vl10 Grp 110 Standby router is unknown, was local *Jul 29 16:49:35.417: HSRP: Vl10 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: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Standby -> Active *Jul 29 16:49:35.419: HSRP: Vl10 Grp 110 Added 192.168.10.100 to ARP (0000.0c07.ac6e) *Jul 29 16:49:35.420: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" standby, local -> unknown *Jul 29 16:49:35.421: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Standby -> Active *Jul 29 16:49:38.422: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Active -> Active

Sie können das bedingte Schnittstellen- und/oder HSRP-Gruppen-Debugging verwenden, um diese Debug-Ausgabe zu filtern.

Command	Zweck
debug condition interface interface	Aktiviert das bedingte Schnittstellen-Debugging.
debug condition standby <Schnittstelle> <Gruppe>	Aktiviert das bedingte HSRP-Debugging.

In diesem Beispiel tritt der Router einer bereits vorhandenen HSRP-Gruppe bei:

Rotuer_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: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:15.122: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:17.737: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:18.880: HSRP: Vl10 Nbr 192.168.10.1 is passive *Jul 29 16:54:20.316: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:20.322: HSRP: Vl10 Grp 110 Coup in 192.168.10.1 Listen pri 110 vIP 192.168.10.100 *Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active: j/Coup rcvd from higher pri router (110/192.168.10.1) *Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active router is 192.168.10.1, was local *Jul 29 16:54:20.323: HSRP: Vl10 Nbr 192.168.10.1 is no longer passive *Jul 29 16:54:20.324: HSRP: Vl10 Nbr 192.168.10.1 active for group 110 *Jul 29 16:54:20.324: HSRP: Vl10 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: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Active -> Speak *Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Removed 192.168.10.100 from ARP *Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Deactivating MAC 0000.0c07.ac6e *Jul 29 16:54:20.327: HSRP: Vl10 Grp 110 Removing 0000.0c07.ac6e from MAC address filter *Jul 29 16:54:20.328: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:20.328: HSRP:

Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:23.104: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:23.226: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:25.825: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:25.952: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:28.427: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:28.772: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Speak: d/Standby timer expired (unknown) *Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Standby router is local *Jul 29 16:54:30.727: HSRP: Vl10 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: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Speak -> Standby *Jul 29 16:54:30.728: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:31.082: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:33.459: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:33.811: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:36.344: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:36.378: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.856: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.876: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.688: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.717: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100

E. Spanning Tree-Fehlerbehebung

STP-Schleifenbedingungen oder Instabilität in einem Netzwerk können die ordnungsgemäße Kommunikation von HSRP-Peers verhindern. Aufgrund dieser fehlerhaften Kommunikation wird jeder Peer zum aktiven Router. STP-Schleifen können Broadcast-Stürme, doppelte Frames und Inkonsistenzen bei MAC-Tabellen verursachen. Alle diese Probleme betreffen das gesamte Netzwerk, insbesondere HSRP. HSRP-Fehlermeldungen können der erste Hinweis auf ein STP-Problem sein.

Bei der STP-Fehlerbehebung *müssen* Sie die STP-Topologie des Netzwerks in jedem VLAN genau kennen. Sie müssen ermitteln, welcher Switch die Root-Bridge ist und welche Ports auf dem Switch blockiert und weitergeleitet werden. Da jedes VLAN eine eigene STP-Topologie hat, sind diese Informationen für jedes VLAN sehr wichtig.

1. Überprüfen der Spanning Tree-Konfiguration

Vergewissern Sie sich, dass STP auf jedem Switch und jedem Bridging-Gerät im Netzwerk konfiguriert ist. Notieren Sie die von den einzelnen Switches vermutete Position der Root-Bridge. Notieren Sie auch die Werte dieser Timer:

- `Root Max Age (Max. Root-Alter)`
- `Hello-Zeit`
- `Forward Delay (Verzögerte Weiterleitung)`

Geben Sie den Befehl **show spanning-tree** ein, um alle Informationen anzuzeigen. Standardmäßig werden diese Informationen für alle VLANs angezeigt. Sie können jedoch auch andere VLAN-Informationen filtern, wenn Sie den Befehl zusammen mit der VLAN-Nummer eingeben. Diese Informationen sind sehr hilfreich beim Beheben von STP-Problemen.

Diese drei Timer, die Sie in der Ausgabe von **show spanning-tree** finden, werden von der Root-Bridge gelernt. Diese Timer müssen nicht mit den Timern übereinstimmen, die auf der jeweiligen Bridge eingestellt sind. Stellen Sie jedoch sicher, dass die Timer mit der Root-Bridge übereinstimmen, falls dieser Switch irgendwann zur Root-Bridge werden sollte. Diese Abstimmung der Timer auf die Root-Bridge sorgt für Kontinuität und einfache Verwaltung. Die Übereinstimmung verhindert auch, dass ein Switch mit falschen Timern das Netzwerk beeinträchtigt.

> **Hinweis**: Aktivieren Sie STP jederzeit für alle VLANs, unabhängig davon, ob im Netzwerk redundante Links vorhanden sind. Wenn Sie STP in nicht redundanten Netzwerken

aktivieren, verhindern Sie Unterbrechungen. Eine Unterbrechung kann auftreten, wenn Switches versehentlich zusammen mit Hubs oder anderen Switches überbrückt werden und so eine physische Schleife entsteht. STP ist auch bei der Isolierung spezifischer Probleme sehr nützlich. Wenn die Aktivierung von STP den Betrieb von Elementen im Netzwerk beeinträchtigt, ist möglicherweise bereits ein Problem vorhanden, das Sie isolieren müssen.

Hier ist ein Beispiel für den Befehl **show spanning-tree**:

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 ist der Root von VLAN 10 und VLAN 11.

2. Spanning Tree-Schleifenbedingungen

Damit eine STP-Schleife auftreten kann, muss im Netzwerk physische L2-Redundanz gegeben sein. Eine STP-Schleife tritt nicht auf, wenn keine physische Schleifenbedingung bestehen kann. Symptome einer STP-Schleifenbedingung:

- Totalausfall des Netzwerks
- Verlust von Netzwerkverbindungen
- Netzwerkgeräte melden eine hohe Prozess- und Systemauslastung

Ein einzelnes VLAN, bei dem eine STP-Schleifenbedingung auftritt, kann einen Link überlasten und die Bandbreite der anderen VLANs verringern. Der Befehl **show interfaces <interface> controller** gibt an, welche Ports eine übermäßig große Anzahl an Paketen übertragen oder empfangen. Übermäßiger Broadcast und Multicast können auf Ports hinweisen, die Teil einer STP-Schleife sind. In der Regel können Sie immer dann eine STP-Schleifenbedingung bei einem Link vermuten, wenn Multicast oder Broadcast die Anzahl der Unicast-Pakete überschreitet.

Hinweis: Der Switch zählt auch STP-BPDUs (Bridge Protocol Data Units), die als Multicast-Frames empfangen und übertragen werden. Ein Port, der sich im STP-Blockierungsstatus befindet, sendet und empfängt dennoch STP-BPDUs.

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. Benachrichtigung über Topologieänderung

Ein weiterer für die Diagnose von STP-Problemen wichtiger Befehl ist der Befehl **show spanning-tree detail**. Mit diesem Befehl werden TCNs (Topology Change Notifications, Benachrichtigungen zu Topologieänderungen) zum Ausgangspunkt zurückverfolgt. Diese Nachrichten, die als spezielle BPDUs zwischen Switches versendet werden, zeigen an, dass eine Topologieänderung auf einem Switch stattgefunden hat. Dieser Switch sendet eine TCN über seinen Root-Port. Die TCN wird upstream zur Root-Bridge weitergeleitet. Die Root-Bridge sendet dann zur Bestätigung eine weitere spezielle BPDU, ein TCA (Topology Change Acknowledgement), über alle ihre Ports. Die Root-Bridge legt das TCN-Bit in der Konfigurations-BPDU fest. Dies führt dazu, dass alle Nicht-Root-Bridges ihren Alterungs-Timer für die MAC-Adresstabelle auf die STP-Weiterleitungsverzögerung der Konfiguration setzen.

Um dieses Problem zu isolieren, greifen Sie für jedes VLAN auf die Root-Bridge zu, und geben Sie den Befehl **show spanning-tree <interface> detail (Spanning-Tree-Details anzeigen)** für die mit dem Switch verbundenen Ports ein. Die `letzte Änderung` im Eintrag gibt die Zeit an, zu der die letzte TCN empfangen wurde. In dieser Situation ist es zu spät, um zu sehen, wer die TCNs ausgestellt hat, die die mögliche STP-Schleife verursacht haben könnten. Der Eintrag `Number of topology changes` (Anzahl der Topologieänderungen) vermittelt eine Vorstellung der Anzahl der auftretenden TCNs. Solange eine STP-Schleife vorliegt, wird dieser Zähler unter Umständen einmal pro Minute erhöht. Weitere Informationen finden Sie unter STP-Probleme und zugehörige Überlegungen zum Design.

Weitere nützliche Informationen sind:

- Port der letzten TCN
- Zeitpunkt der letzten TCN
- Aktuelle Anzahl der TCNs

Beispiel für die Befehlsausgabe:

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 BPDU: sent 6067, received 0

Diese Ausgabe zeigt, dass die letzte Topologieänderung beim Gerät stattgefunden hat, das über die GigabitEthernet1/0/35-Schnittstelle angeschlossen ist. Führen Sie als Nächstes den gleichen Befehl **show spanning-tree detail** von diesem Gerät aus, um das Problem zu verfolgen. Wenn dieser Switch, der die TCNs generiert, nur an PCs oder Endgeräte angeschlossen ist, stellen Sie sicher, dass STP PortFast auf diesen Ports aktiviert ist. STP PortFast unterdrückt STP-TCNs, wenn ein Port den Status wechselt.

In diesen Dokumenten finden Sie Informationen zu STP und zur Fehlerbehebung bei Link-Übergängen, die Netzwerkschnittstellenkarten (NICs) zugeordnet sind:

- Verwenden von PortFast und anderen Befehlen zum Beheben von Verzögerungen bei der Workstation-Startverbindung
- Kennenlernen des Rapid Spanning Tree Protocol (802.1w)
- STP-Probleme und zugehörige Überlegungen zum Design

4. Getrennte blockierte Ports

Aufgrund des Load Balancing bei Fast EtherChannel (FEC) (Port-Channeling) können FEC-Probleme sowohl HSRP- als auch STP-Probleme verschlimmern. Wenn Sie eine Fehlerbehebung für STP oder HSRP durchführen, können Sie die Konfiguration für alle FEC-Verbindungen entfernen. Nachdem die Konfigurationsänderungen vorgenommen wurden, führen Sie den Befehl **show spanning-tree blockedports** auf beiden Switches aus. Vergewissern Sie sich, dass mindestens einer der Ports auf einer Seite der Verbindung zu blockieren beginnt.

Informationen zu Fast EtherChannel finden Sie in diesen Dokumenten:

- besseres Verständnis von EtherChannel-Lastenausgleich und -Redundanz bei Catalyst-

Switches
- Konfigurieren von EtherChannels

5. Unterdrückung von Broadcasts

Aktivieren Sie die Broadcast-Unterdrückung, um die Auswirkungen eines Broadcast-Sturms zu verringern. Ein Broadcast-Sturm ist eine der gängigsten Auswirkungen einer STP-Schleife. Beispiel für die Befehlsausgabe:

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. Konsolen- und Telnet-Zugriff

Solange eine STP-Schleife besteht, ist der Konsolen- oder Telnet-Datenverkehr zum Switch oft zu langsam, um ein fehlerhaftes Gerät nachverfolgen zu können. Um die sofortige Wiederherstellung des Netzwerks zu erzwingen, entfernen Sie alle redundanten physischen Links. Nachdem die Rekonvergenz von STP in der neuen nicht redundanten Topologie zugelassen wurde, verbinden Sie die redundanten Links einzeln neu. Wenn die STP-Schleife erneut auftritt, nachdem Sie ein bestimmtes Segment hinzugefügt haben, haben Sie die fehlerhaften Geräte gefunden.

7. Spanning Tree-Funktionen: PortFast, UplinkFast und BackboneFast

Überprüfen Sie, ob PortFast, UplinkFast und BackboneFast ordnungsgemäß konfiguriert sind. Um STP-Probleme beheben zu können, deaktivieren Sie alle erweiterten STP-Funktionen (UplinkFast und BackboneFast). Stellen Sie außerdem sicher, dass STP PortFast nur an Ports aktiviert ist, die direkt mit Nicht-Bridging-Hosts verbunden sind. Nicht-Bridging-Hosts sind u. a. Benutzer-Workstations und Router ohne Bridge-Gruppen. Aktivieren Sie PortFast nicht an Ports, die mit Hubs oder anderen Switches verbunden sind. Im Folgenden finden Sie einige Dokumente, die Ihnen das Verständnis und die Konfiguration dieser Funktionen erleichtern:

Konfigurieren von Spanning Tree PortFast, BPDU Guard, BPDU-Filter, UplinkFast, BackboneFast und Loop Guard

Cisco UplinkFast-Funktion verstehen und konfigurieren

8. BPDU-Guard

Wenn Sie PortFast BPDU Guard aktivieren, wird ein PortFast-fähiger Nicht-Trunk-Port bei Empfang einer BPDU an diesem Port in den Status „errdisable“ (wegen Fehler deaktiviert) versetzt. Diese Funktion hilft Ihnen, Ports zu finden, die falsch für PortFast konfiguriert sind. Die Funktion erkennt außerdem, wo Geräte Pakete reflektieren oder STP-BPDUs in das Netzwerk einschleusen. Wenn Sie STP-Probleme beheben, können Sie diese Funktion aktivieren, um das STP-Problem zu isolieren.

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-Beschneiden

Wenn die VTP-Bereinigung im Netzwerk aktiviert ist, können die Geräte einer HSRP-Gruppe aktiv werden. Dies führt zu IP-Konflikten zwischen den Gateways und zu Datenverkehrsproblemen. Stellen Sie sicher, dass das VLAN einer HSRP-Gruppe nicht durch VTP im Netzwerk entfernt wird.

F. Teilen und Erobern

Wenn alle anderen Versuche, HSRP zu isolieren oder aufzulösen, fehlschlagen, ist das Teile-und-herrsche-Verfahren der nächste Ansatz. Diese Methode trägt dazu bei, das Netzwerk selbst und die Komponenten, aus denen es besteht, zu isolieren. Die Richtlinien aus folgender Liste passen zum Teile-und-herrsche-Verfahren:

> **Hinweis**: Diese Liste wiederholt einige Richtlinien aus anderen Abschnitten dieses Dokuments.

- Erstellen Sie ein Test-VLAN für HSRP und ein isoliertes VLAN für den Switch mit HSRP-Routern.
- Trennen Sie alle redundanten Ports.
- Teilen Sie FEC-Ports in einzelne verbundene Ports auf.
- Reduzieren Sie die Mitglieder der HSRP-Gruppe auf nur zwei Mitglieder.
- Entfernen Sie Trunk-Ports so, dass nur die erforderlichen VLANs über diese Ports übertragen werden.
- Trennen Sie die verbundenen Switches im Netzwerk, bis die Probleme behoben sind.

Bekannte Probleme

HSRP-State-Flapping/Unstable bei Verwendung von Cisco 2620/2621, Cisco 3600 mit Fast Ethernet

Dieses Problem kann bei Fast Ethernet-Schnittstellen bei Unterbrechung der Netzwerkverbindung oder beim Hinzufügen eines HSRP-Routers mit höherer Priorität zu einem Netzwerk auftreten. Wenn der HSRP-Status vom aktiven Status zur Kommunikation wechselt, setzt der Router die Schnittstelle zurück, um die HSRP-MAC-Adresse aus dem MAC-Adressfilter der Schnittstelle zu entfernen. Dieses Problem tritt nur bei bestimmter Hardware auf, die an den Fast Ethernet-Schnittstellen für Cisco 2600, 3600 und 7500 verwendet wird. Das Zurücksetzen der Router-Schnittstelle führt zu einer Änderung des Link-Status an Fast Ethernet-Schnittstellen, die dann vom Switch erkannt wird. Wenn auf dem Switch STP ausgeführt wird, führt die Änderung zu einem STP-Übergang. STP benötigt 30 Sekunden, um den Port in den Weiterleitungsstatus zu versetzen. Diese Zeit ist doppelt so lang wie die standardmäßige Weiterleitungsverzögerung um 15 Sekunden. Zur gleichen Zeit wechselt der kommunizierende Router nach 10 Sekunden (entspricht der Haltezeit) in den `Standby-Status`. STP leitet noch nicht weiter, sodass keine HSRP-Hello-Nachrichten vom aktiven Router empfangen werden. Dadurch wird der Standby-Router nach etwa 10 Sekunden aktiv. Nun sind beide Router `aktiv`. Wenn die STP-Ports zur Weiterleitung übergehen, wechselt der Router mit niedrigerer Priorität vom aktiven Status zur Kommunikation,

und der gesamte Prozess wiederholt sich.

Plattform	Beschreibung	Cisco Bug-ID	Beheben	Problemumgehung
Cisco 2620/2621	Flapping der Fast Ethernet-Schnittstelle tritt auf, wenn HSRP konfiguriert und das Kabel abgezogen wird.		Ein Software-Upgrade; Details zur Revision finden Sie im Fehler.	Aktiviert Spanning Tree PortFast am verbundenen Switch-Port.
Cisco 2620/2621	HSRP-Status-Flapping auf 2600 mit Fast Ethernet		Cisco IOS-Software Version 12.1.3	Aktiviert Spanning Tree PortFast am verbundenen Switch-Port.
Cisco 3600 mit NM-1FE-TX[1]	HSRP-Status-Flapping auf 2600 und 3600 mit Fast Ethernet		Cisco IOS-Software Version 12.1.3	Aktiviert Spanning Tree PortFast am verbundenen Switch-Port.
Cisco 4500 mit Fast Ethernet-Schnittstelle	HSRP-Status-Flapping auf 4500 mit Fast Ethernet	Cisco Bug-ID CSCds16055	Cisco IOS-Software Version 12.1.5	Aktiviert Spanning Tree PortFast am verbundenen Switch-Port.

[1]NM-1FE-TX = Fast Ethernet-Netzwerkmodul (10/100BASE-TX-Schnittstelle) mit nur einem Port.

Eine alternative Problemumgehung besteht darin, die HSRP-Timer so anzupassen, dass die STP-Weiterleitungsverzögerung weniger als die Hälfte der standardmäßigen HSRP-Haltezeit beträgt. Die standardmäßige STP-Weiterleitungsverzögerung beträgt 15 Sekunden, die standardmäßige HSRP-Haltezeit 10 Sekunden.

Wenn Sie den Befehl **track** im HSRP-Prozess verwenden, empfiehlt Cisco, einen bestimmten Minderungswert zu verwenden, um das HSRP-Flapping zu vermeiden.

Beispielkonfiguration auf einem aktiven HSRP-Router, wenn Sie den Befehl **track** verwenden:

```
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
```

Dabei ist 15 der Dekrementwert, wenn das Objekt flattert. Um mehr über den Befehl track zu erfahren, navigieren Sie zum Dokument Track Option in HSRPv2 Configuration Example.

Zugehörige Informationen

- Campus LAN Catalyst Switches - Zugriff
- LAN-Switching
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.