Risoluzione dei problemi relativi all'HSRP nelle reti degli switch Catalyst

Sommario

Introduzione

In questo documento vengono descritti i problemi più comuni e le modalità per risolverli.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Come funziona il protocollo HSRP

Premesse

In questo documento vengono discussi i problemi più comuni che influenzano il protocollo HSRP:

- Il router segnala un indirizzo IP di standby HSRP duplicato
- Lo stato HSRP cambia continuamente (attivo, standby, speak)
- Peer HSRP non presenti
- Lo switch genera messaggi di errore relativi al protocollo HSRP
- I pacchetti unicast vengono trasmessi a tutti i nodi della rete (flooding eccessivo) nella configurazione HSRP

> **Nota**: in questo documento viene spiegato in dettaglio come risolvere i problemi relativi all'HSRP negli ambienti degli switch Catalyst. con molti riferimenti alle versioni software e alla topologia della rete. Tuttavia, il suo solo scopo è fornire indicazioni su come risolvere i problemi del protocollo HSRP. Il documento non è stato ideato come una guida alla progettazione né fornisce consigli sul software o le best practice.

Le aziende e gli utenti che usano i servizi intranet e Internet per le comunicazioni mission-critical vogliono e si aspettano che le reti e le applicazioni siano sempre disponibili. Il protocollo HSRP usato in Cisco IOS® Software permette di soddisfare questa esigenza con tempi di attività della rete prossimi al 100 percento. Esclusivo delle piattaforme Cisco, il protocollo HSRP fornisce ridondanza alle reti IP assicurando un ripristino immediato e trasparente del traffico in caso di errore di first-hop nei dispositivi edge o nei circuiti di accesso.

Due o più router possono agire come un unico router virtuale se condividono un indirizzo IP e un indirizzo MAC (Layer 2 [L2]). L'indirizzo è necessario per la ridondanza del gateway predefinito delle postazioni di lavoro host. La maggior parte delle postazioni di lavoro host non contiene tabelle di routing e utilizza solo un indirizzo IP e un indirizzo MAC di next-hop. L'indirizzo è il gateway predefinito. Quando si usa il protocollo HSRP, i membri del gruppo di router virtuali si scambiano continuamente messaggi sullo stato. In caso di interruzioni del collegamento su un router, pianificate o meno, un altro router può assumersi la responsabilità dell'indirizzamento. Gli host sono configurati con un singolo gateway predefinito e continuano a inoltrare i pacchetti IP agli stessi indirizzi IP e MAC. Il passaggio da un router all'altro è trasparente per le postazioni di lavoro finali.

> **Nota**: è possibile configurare workstation host che eseguono il sistema operativo Microsoft per più gateway predefiniti. Tuttavia, i gateway predefiniti multipli non sono dinamici. Il sistema operativo utilizza un solo gateway predefinito alla volta. Il sistema seleziona un altro gateway predefinito configurato al momento di avvio solo se il primo gateway predefinito

configurato non è raggiungibile dal protocollo Internet Control Management Protocol (ICMP).

Funzionamento di base

Il protocollo HSRP permette di far sembrare un gruppo di router come un unico router gateway predefinito nelle comunicazioni con gli host della LAN. Questo gruppo di router è chiamato gruppo HSRP o gruppo di standby. Un singolo router selezionato dal gruppo è responsabile dell'inoltro dei pacchetti inviati dagli host al router virtuale. Questo è il router attivo, mentre un altro router viene scelto come router di standby. In caso di errore sul router attivo, il router di standby provvede all'inoltro dei pacchetti. Sebbene un numero arbitrario di router possa eseguire l'HSRP, solo il router attivo inoltra i pacchetti inviati all'indirizzo IP del router virtuale.

Per ridurre al minimo il traffico di rete, solo i router attivo e in standby, una volta determinati dal protocollo, inviano regolarmente messaggi HSRP. Gli altri router del gruppo HSRP rimangono nello stato `in ascolto`. Se sul router attivo si verifica un errore, il router di standby lo sostituisce, diventando a sua volta attivo. In caso di errore sul router di standby o se il router di standby diventa il router attivo, il protocollo sceglie un altro router come router di standby.

Ogni gruppo di standby emula un singolo router virtuale (gateway predefinito). A ogni gruppo viene assegnato un singolo indirizzo MAC e un singolo indirizzo IP noti. Più gruppi di standby possono coesistere e sovrapporsi su una LAN; i singoli router possono partecipare a più gruppi. In questo caso, il router mantiene uno stato e dei timer separati in ciascun gruppo.

Termini HSRP

Termine	Definizione
Router attivo	Il router che al momento inoltra i pacchetti per il router virtuale
Router di standby	Il router di backup principale
Gruppo di standby	Gruppo di router che partecipano al protocollo HSRP ed emulano un rou virtuale
Frequenza di invio dei messaggi hello	L'intervallo tra i messaggi hello del protocollo HSRP inviati da un router
Tempo di attesa	L'intervallo tra la ricezione di un messaggio hello e la presunzione di erro del router di invio

Indirizzamento del protocollo HSRP

Comunicazioni dei router HSRP

I router con protocollo HSRP si scambiano tra loro le informazioni HSRP inviando pacchetti hello HSRP. Questi pacchetti vengono inviati all'indirizzo IP multicast di destinazione 224.0.0.2 sulla porta UDP (User Datagram Protocol) 1985. L'indirizzo IP multicast 224.0.0.2 è riservato e viene utilizzato per comunicare con tutti i router. Il router attivo genera i pacchetti hello dall'indirizzo IP configurato e dall'indirizzo MAC virtuale HSRP. Il router di standby genera messaggi hello dall'indirizzo IP configurato e dall'indirizzo MAC fisico, o BIA (Burned-In Address). Questo utilizzo dell'indirizzamento di origine è necessario per consentire ai router HSRP di identificarsi correttamente.

Nella maggior parte dei casi, quando si configurano i router di un gruppo HSRP, i router rimangono in ascolto dell'indirizzo MAC HSRP di tale gruppo e del proprio indirizzo BIA. I router

Cisco 2500, 4000 e 4500 costituiscono un'eccezione. Questi router hanno un hardware Ethernet in grado di riconoscere solo un singolo indirizzo MAC. Pertanto, quando diventano router attivi, usano l'indirizzo MAC HSRP e usano l'indirizzo BIA quando sono router di standby.

Comunicazione dell'indirizzo IP di standby HSRP su tutti i supporti ad eccezione del Token Ring

Poiché le postazioni di lavoro host sono configurate con il proprio gateway predefinito come indirizzo IP di standby HSRP, gli host devono comunicare con l'indirizzo MAC associato all'indirizzo IP di standby HSRP. Questo indirizzo MAC è un indirizzo MAC virtuale composto da 0000.0c07.ac**. ** è il numero del gruppo HSRP in formato esadecimale, basato sulla rispettiva interfaccia. Ad esempio, il gruppo 1 dell'HSRP utilizza l'indirizzo MAC virtuale dell'HSRP 0000.0c07.ac01. Gli host sul segmento LAN adiacente usano il normale processo ARP (Address Resolution Protocol) per risolvere gli indirizzi MAC associati.

Messaggi di reindirizzamento ICMP

I router peer HSRP che proteggono una subnet possono fornire accesso a tutte le altre subnet della rete. Questa è una caratteristica fondamentale del protocollo HSRP. Pertanto, quale router diventa il router HSRP attivo è irrilevante. Nelle versioni software di Cisco IOS diverse da Cisco IOS Software Release 12.1(3)T, i reindirizzamenti ICMP vengono disabilitati automaticamente sull'interfaccia che usa il protocollo HSRP. Senza questa configurazione, gli host possono essere reindirizzati dall'indirizzo IP virtuale HSRP all'indirizzo IP e all'indirizzo MAC dell'interfaccia di un singolo router, perdendo così la ridondanza.

Il software Cisco IOS introduce un metodo per consentire i reindirizzamenti ICMP con HSRP. Questo metodo permette di filtrare i messaggi di reindirizzamento ICMP in uscita tramite il protocollo HSRP. L'indirizzo IP di next-hop viene modificato in un indirizzo virtuale HSRP. L'indirizzo IP del gateway nel messaggio di reindirizzamento ICMP in uscita viene confrontato con un elenco di router attivi HSRP presenti sulla rete. Se il router che corrisponde all'indirizzo IP del gateway è un router attivo di un gruppo HSRP, l'indirizzo IP del gateway viene sostituito con l'indirizzo IP virtuale del gruppo. Questa soluzione consente agli host di imparare le route ottimali per raggiungere le reti remote e, al tempo stesso, di mantenere la resilienza tipica del protocollo HSRP.

Matrice delle funzionalità HSRP

Per ulteriori informazioni sulle funzionalità e le versioni di Cisco IOS Software che supportano il protocollo HSRP, fare riferimento alla sezione Matrice delle funzionalità di Cisco IOS Release e HSRP in Funzionalità e caratteristiche del protocollo Hot Standby Router Protocol.

Funzionalità del protocollo HSRP

Per ulteriori informazioni sul protocollo HSRP, fare riferimento a Funzionalità e caratteristiche del protocollo Hot Standby Router Protocol. In questo documento vengono fornite informazioni sulle seguenti funzionalità HSRP:

- Modalità di prelazione
- Tracciamento dell'interfaccia
- Uso di un indirizzo BIA
- Gruppi HSRP molteplici

- Indirizzi MAC configurabili
- Supporto Syslog
- Debug HSRP
- Debug HSRP avanzato
- Autenticazione
- Ridondanza IP
- Protocollo Simple Network Management Protocol (SNMP) MIB
- Protocollo HSRP per Multiprotocol Label Switching (MPLS)

Nota: è possibile utilizzare la funzione Trova del browser per individuare queste sezioni all'interno del documento.

Formato del pacchetto

In questa tabella viene mostrato il formato della porzione dati del frame UDP HSRP:

Version	**Op Code**	**State**	**Hellotime**
Holdtime	Priority	Group	Reserved
Authentication Data			
Authentication Data			
Virtual IP Address			

In questa tabella viene descritto ciascuno dei campi del pacchetto HSRP:

Campo del pacchetto	Descrizione
Op Code (1 ottetto)	Il codice operativo descrive il tipo di messaggio contenuto nel pacchetto. I valori possibili sono: 0 - ciao, 1 - colpo di stato e 2 - dimissioni. I messaggi hello vengono inviati per segnalare che un router usa il protocollo HSRP e può diventare il router attivo. I messaggi coup vengono inviati quando un router desidera diventare il router attivo. I messaggi resign vengono inviati quando un router non desidera più essere il router attivo.
State (1 ottetto)	Ogni router del gruppo di standby implementa una macchina a stati finiti. Il campo dello stato descrive lo stato corrente del router che invia il messaggio. Questi sono dettagli sui singoli stati: 0 - iniziale, 1 - apprendere, 2 - ascoltare, 4 - parlare, 8 - standby e 16 - attivo.
Hellotime (1 ottetto)	Questo campo è significativo solo per i messaggi hello e specifica l'intervallo approssimativ tra i messaggi hello inviati dal router. Il tempo è espresso in secondi.
Holdtime (1 ottetto)	Questo campo è significativo solo per i messaggi hello e specifica il periodo di tempo durante cui i router attendono un messaggio hello prima di avviare una modifica dello stato
Priority (1 ottetto)	Questo campo viene utilizzato per scegliere il router attivo e il router di standby. Le priorità dei due router vengono messe a confronto e il router con il valore di priorità più alto viene scelto come router attivo. Il router con l'indirizzo IP più alto è quindi il tie breaker.
Group (1 ottetto)	Questo campo identifica il gruppo di standby.
Authentication Data (8 ottetti)	Questo campo contiene una password in chiaro di otto caratteri.
Virtual IP Address (4 ottetti)	Se l'indirizzo IP virtuale non è configurato su un router, l'indirizzo può essere appreso dal messaggio hello del router attivo. Un indirizzo viene appreso solo se non è stato configurat alcun indirizzo IP di standby HSRP e il messaggio hello è stato autenticato (se l'autenticazione è stata configurata).

Stati HSRP

State	Definizione
`Initial`	Lo stato del router all'inizio. Questo stato indica che il protocollo HSRP non è eseguito e viene immesso con una modifica alla configurazione o quando un'interfaccia diventa disponibile per la p volta.
`Learn`	Il router non ha stabilito l'indirizzo IP virtuale e non ha ancora visualizzato un messaggio hello autenticato dal router attivo. In questo stato, il router attende ancora di essere ascoltato dal router attivo.
`Listen`	Il router conosce l'indirizzo IP virtuale, ma non è né il router attivo né il router di standby. Il router rimane in ascolto dei messaggi hello provenienti dagli altri router.
`Speak`	Il router invia messaggi hello a intervalli regolari e partecipa attivamente alla scelta del router attiv di standby. Un router non può passare nello stato `speak` finché non ha acquisito l'indirizzo IP virtua
`Standby`	Il router è un candidato per diventare il successivo router attivo e invia messaggi hello a intervalli regolari. A parte i momenti di transizione, un solo router del gruppo può essere nello stato `standby`
`Active`	Il router che al momento inoltra i pacchetti inviati all'indirizzo MAC virtuale del gruppo. Il router inv messaggi hello a intervalli regolari. A parte i momenti di transizione, un solo router del gruppo può essere nello stato `attivo`.

Timer HSRP

Ogni router utilizza solo tre timer nel protocollo HSRP. I timer misurano la durata dei messaggi hello. Quando si verifica un errore, il protocollo HSRP converge in base ai timer hello e di attesa. Per impostazione predefinita, i timer sono impostati rispettivamente a 3 e 10 secondi, ossia un pacchetto hello viene scambiato tra i dispositivi del gruppo di standby HSRP ogni 3 secondi e il dispositivo di standby diventa attivo se non riceve un pacchetto hello per 10 secondi. È possibile ridurre queste impostazioni del timer per velocizzare il failover o l'interruzione per diritti di priorità, ma, per evitare un maggiore utilizzo della CPU e il flap dello stato di standby non necessario, non impostare il timer di attesa su un valore inferiore a un (1) secondo o a 4 secondi. Notare che se si usa il meccanismo di tracciamento HSRP e il collegamento tracciato viene interrotto, il sistema passa subito al failover o alla prelazione, a prescindere dai timer impostati per la frequenza di invio dei messaggi hello e il tempo di attesa. Quando un timer scade, il router passa a un nuovo stato HSRP. I timer possono essere modificati con questo comando: **standby [group-number] timer hellottime holdtime**. Ad esempio, **standby 1 timers 5 15**.

In questa tabella vengono fornite ulteriori informazioni sui timer:

Timer	Descrizione
Timer attivo	Questo timer viene usato per monitorare il router attivo. Il timer si avvia ogni volta che un router attivo riceve un pacchetto hello. Il timer scade in base al valore impostato per il tempo di attesa n relativo campo del messaggio hello HSRP.
Timer di standby	Questo timer viene utilizzato per monitorare il router di standby. Il timer si avvia ogni volta che il router di standby riceve un pacchetto hello. Il timer scade in base al valore impostato per il tempo di attesa nel rispettivo pacchetto hello.
Timer hello	Questo timer viene utilizzato per sincronizzare i pacchetti hello. Tutti i router HSRP in qualsiasi stato HSRP generano un pacchetto hello alla scadenza del timer hello.

Eventi HSRP

In questa tabella vengono riepilogati gli eventi della macchina a stati finiti HSRP:

Chiave	Eventi
1	HSRP è configurato su un'interfaccia abilitata.
2	HSRP è disabilitato su un'interfaccia o l'interfaccia è disabilitata.

3	Scadenza del timer attivo: il timer attivo è impostato sul tempo di attesa quando l'ultimo messaggi hello viene visualizzato dal router attivo.
4	Scadenza del timer standby: il timer di standby è impostato sul tempo di attesa quando l'ultimo messaggio hello viene visualizzato dal router di standby.
5	Scadenza del timer hello: il timer periodico per l'invio dei messaggi hello è scaduto.
6	Ricezione di un messaggio hello con priorità più alta da un router nello stato `speak`
7	Ricezione di un messaggio hello con priorità più alta dal router attivo
8	Ricezione di un messaggio hello con priorità più bassa dal router attivo
9	Ricezione di un messaggio resign dal router attivo
10	Ricezione di un messaggio coup da un router con priorità più alta
11	Ricezione di un messaggio hello con priorità più alta dal router di standby
12	Ricezione di un messaggio hello con priorità più bassa dal router di standby

Azioni HSRP

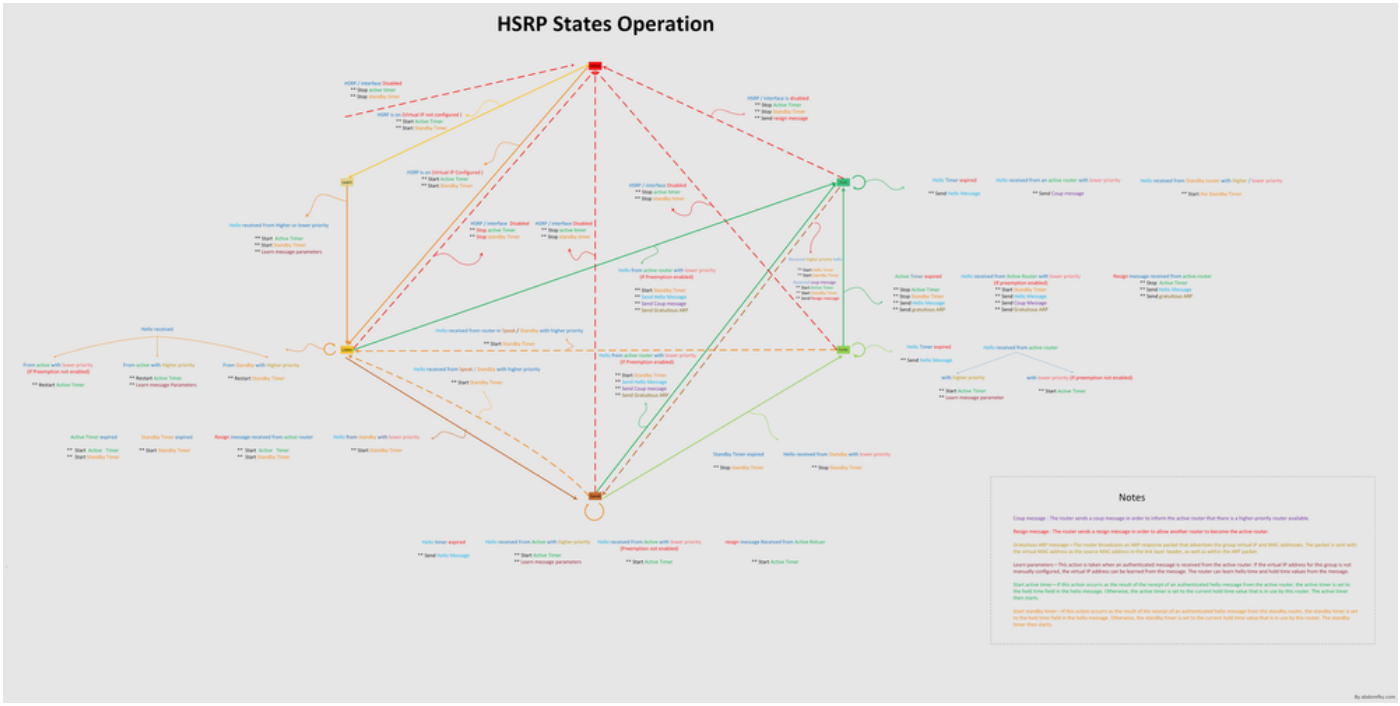
In questa tabella vengono riportate le azioni da eseguire come parte della macchina a stati finiti:

Lettera	Azione
A	Avvia timer attivo: se questa azione si verifica in seguito alla ricezione di un messaggio hello autenticato dal router attivo, il timer attivo viene impostato sul campo del tempo di attesa nel messaggio hello. In caso contrario, il timer attivo viene impostato al valore del tempo di attesa cor utilizzato da questo router. Quindi, il timer attivo viene avviato.
B	Timer di avvio in standby: se questa azione si verifica in seguito alla ricezione di un messaggio di saluto autenticato dal router di standby, il timer di standby viene impostato sul campo del tempo d attesa nel messaggio di saluto. In caso contrario, il timer di standby viene impostato al valore del t di attesa corrente utilizzato da questo router. Quindi, il timer di standby viene avviato.
C	Arresta il timer attivo: il timer attivo viene arrestato.
D	Arresta timer di standby: il timer di standby viene arrestato.
S	Apprendi parametri: questa azione viene eseguita quando si riceve un messaggio autenticato dal router attivo. Se l'indirizzo IP virtuale del gruppo non è stato configurato manualmente, può essere appreso dal messaggio. Il router può ricavare i valori della frequenza di invio dei messaggi hello e tempo di attesa dal messaggio.
F	Invia messaggio hello: il router invia un messaggio hello con lo stato corrente, la frequenza di invi messaggi hello e il tempo di attesa.
G	Invia messaggio coup: il router invia un messaggio coup per informare il router attivo che è dispor un router con priorità più alta.
H	Invia messaggio resign: il router invia un messaggio resign per consentire a un altro router di dive il router attivo.
I	Invia messaggio ARP gratuito: il router trasmette un pacchetto di risposta ARP che annuncia gli indirizzi IP e MAC virtuali del gruppo. Il pacchetto viene inviato con l'indirizzo MAC virtuale come indirizzo MAC di origine nell'intestazione del layer di collegamento e all'interno del pacchetto ARP

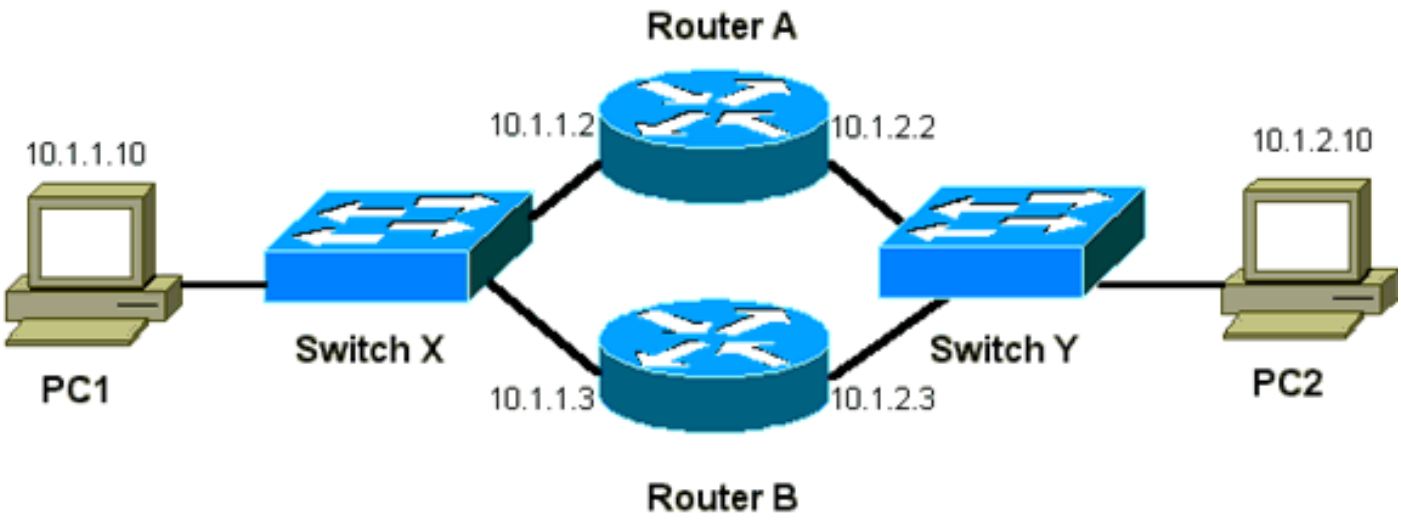
Tabella degli stati del protocollo HSRP

Il diagramma di questa sezione mostra i cambi di stato di una macchina a stati finiti HSRP. Ogni volta che si verifica un evento, viene eseguita l'azione associata e il router passa allo stato HSRP successivo. Nel diagramma, i numeri indicano gli eventi e le lettere indicano l'azione associata. Nella tabella della sezione Eventi HSRP viene spiegato a cosa corrisponde ciascun numero; nella tabella della sezione Azioni HSRP viene spiegato a cosa corrisponde ciascuna lettera. Il diagramma viene riportato a solo scopo esemplificativo Il diagramma è dettagliato e non è necessario per scopi generici di risoluzione dei problemi.

Per un'immagine ad alta risoluzione del diagramma, vedere Descrizione degli stati HSRP.



Flusso dei pacchetti



Sul dispositivo bootflash o slot0:	Indirizzo MAC	Indirizzo IP	Subnet mask	Gateway predefinito
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

Configurazione del router A (router attivo)

```
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
```

Configurazione del router B (router di standby)

```
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
```

> **Nota**: in questi esempi gli indirizzi MAC statici vengono configurati solo a scopo illustrativo. Non configurare indirizzi MAC statici a meno che non sia richiesto.

Quando si ottengono tracce dello sniffer per risolvere i problemi relativi a HSRP, è necessario comprendere il concetto alla base del flusso di pacchetto. Il router A utilizza la priorità 200 e diventa il router attivo su entrambe le interfacce. Nell'esempio di questa sezione, l'indirizzo MAC di origine dei pacchetti del router destinati a una postazione di lavoro host corrisponde all'indirizzo MAC fisico (BIA) del router. L'indirizzo MAC di destinazione dei pacchetti provenienti dai computer host e destinati all'indirizzo IP HSRP coincide con l'indirizzo MAC virtuale HSRP. Tenere presente che gli indirizzi MAC non sono gli stessi per ogni flusso di dati scambiati tra il router e l'host.

Nella tabella vengono mostrate le informazioni dell'indirizzo MAC e dell'indirizzo IP per flusso sulla base di una traccia sniffer ricavata dallo switch X.

Flusso dei pacchetti	MAC di origine	MAC di destinazione	IP di origine	IP di destinazio
Pacchetti provenienti da PC1 e destinati a PC2	PC1 (0000.0c00.0001)	Indirizzo MAC virtuale HSRP dell'interfaccia Ethernet 0 del router A (0000.0c07.ac01)	10.1.1.10	10.1.2.10
Pacchetti di ritorno tramite il router A provenienti da PC2 e destinati a PC1	Router A Ethernet 0 BIA (4000.0000.0010)	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.10
Pacchetti provenienti da PC1 e destinati all'indirizzo IP di standby HSRP (ICMP, Telnet)	PC1 (0000.0c00.0001)	Indirizzo MAC virtuale HSRP dell'interfaccia Ethernet 0 del router A (0000.0c07.ac01)	10.1.1.10	10.1.1.1
Pacchetti destinati all'indirizzo IP effettivo del router attivo (ICMP, Telnet)	PC1 (0000.0c00.0001)	Router A Ethernet 0 BIA (4000.0000.0010)	10.1.1.10	10.1.1.2
Pacchetti destinati all'indirizzo IP effettivo del router di standby (ICMP, Telnet)	PC1 (0000.0c00.0001)	Router B Ethernet 0 BIA (4000.0000.0020)	10.1.1.10	10.1.1.3

Risoluzione dei problemi HSRP - Case study

Caso di studio n. 1: l'indirizzo IP di standby HSRP è segnalato come indirizzo IP duplicato

Possono comparire i messaggi di errore:

```
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
```

Questi messaggi di errore non indicano necessariamente un problema del protocollo HSRP. Al contrario, indicano un possibile loop nel protocollo Spanning Tree Protocol (STP) o un problema di configurazione del router o dello switch. Questi messaggi di errore sono solo il sintomo di un altro problema.

Inoltre, questi messaggi di errore non impediscono il corretto funzionamento del protocollo HSRP. Il pacchetto HSRP duplicato viene ignorato. I messaggi di errore vengono generati a intervalli di 30 secondi. Tuttavia, l'instabilità della rete che causa i messaggi di errore `STANDBY-3-DUPADDR` dell'indirizzo HSRP può dar luogo a prestazioni rallentate o alla perdita di pacchetti.

Questi messaggi indicano in modo specifico che il router ha ricevuto un pacchetto di dati originato dall'indirizzo IP dell'HSRP sulla VLAN 25 con gli indirizzi MAC 000.0c07.ac19. Poiché l'indirizzo MAC dell'HSRP è 0000.0c07.ac19, il router in questione ha ricevuto il proprio pacchetto o entrambi i router del gruppo HSRP sono entrati nello stato `attivo`. Poiché il router ha ricevuto il proprio pacchetto, molto probabilmente il problema riguarda la rete anziché il router. Le cause di questo comportamento possono essere diverse. Questi sono alcuni dei problemi di rete che causano i messaggi di errore:

- Loop STP momentanei
- Problemi di configurazione di EtherChannel
- Frame duplicati

Per la risoluzione dei problemi relativi a questi messaggi di errore, consultare la sezione Risoluzione dei problemi di HSRP sugli switch Catalyst in questo documento. Tutti i moduli di risoluzione dei problemi sono applicabili a questa sezione, che include i moduli sulla configurazione. Inoltre, prendere nota di eventuali errori nel log dello switch e, se necessario, fare riferimento ad altri case study.

Èpossibile utilizzare un elenco degli accessi per impedire al router attivo di ricevere il proprio pacchetto hello multicast. Tuttavia, questa è solo una soluzione alternativa e in realtà non fa che nascondere il sintomo senza risolvere il problema. La soluzione alternativa consiste nell'applicare un elenco degli accessi in entrata esteso alle interfacce HSRP. L'elenco degli accessi blocca tutto il traffico proveniente dall'indirizzo IP fisico e destinato a tutti i router con indirizzo multicast 224.0.0.2.

```
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
```

Caso di studio n. 2: lo stato HSRP cambia continuamente (Attivo, Standby, Speak)

o %HSRP-6-STATECHANGE

Possono comparire i messaggi di errore:

```
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

Questi messaggi di errore descrivono una situazione in cui un router HSRP di standby non riceve tre pacchetti hello HSRP consecutivi dal proprio peer HSRP. L'output mostra che il router di standby passa dallo stato `standby` allo stato `attivo`. Poco dopo, il router torna allo stato `standby`. A meno che il messaggio di errore non si verifichi durante l'installazione iniziale, la causa non è probabilmente un problema del protocollo HSRP. I messaggi di errore indicano la perdita di messaggi hello HSRP tra i peer. Per risolvere questo problema, verificare la comunicazione tra i peer HSRP. La causa più comune di questi messaggi è una perdita di comunicazione dati casuale e momentanea. Il cambio di stato HSRP è spesso dovuto a un utilizzo elevato della CPU. Se il messaggio di errore è dovuto a un elevato utilizzo della CPU, inserire uno sniffer sulla rete e tracciare il sistema che lo sta causando.

La perdita di pacchetti HSRP tra i peer può avere diverse cause. I problemi più comuni sono problemi sul layer fisico, traffico di rete eccessivo causato da problemi del protocollo STP o traffico eccessivo causato da ciascuna VLAN. Come nel caso di studio n. 1, tutti i moduli di risoluzione dei problemi sono applicabili alla risoluzione delle modifiche dello stato HSRP, in particolare il debug HSRP di layer 3.

Se la perdita di pacchetti HSRP tra i peer è dovuta al traffico eccessivo di ciascuna VLAN, è possibile ottimizzare o aumentare le dimensioni SPD e della coda di attesa per evitare che i pacchetti nella coda di entrata vengano scartati.

Per aumentare le dimensioni dell'SPD (Selective Packet Discard), accedere alla modalità di configurazione ed eseguire questi comandi sugli switch Cat6500:

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

!--- Hidden Command

(config)#ip spd queue min-threshold 500

!--- Hidden Command
```

Per aumentare le dimensioni della coda di attesa, passare alla modalità di interfaccia VLAN ed eseguire questo comando:

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

Dopo aver aumentato le dimensioni della coda SPD e della coda di attesa, è possibile cancellare i contatori di interfaccia se si esegue il comando **`clear counter interface`**.

Caso di studio n. 3: HSRP non riconosce il peer

L'output del router in questa sezione mostra un router configurato per HSRP che non riconosce gli altri peer HSRP. Il mancato riconoscimento avviene perché il router non riceve i messaggi hello HSRP dal router adiacente. Per risolvere questo problema, vedere la sezione Verifica della connettività del layer fisico e la sezione Verifica della configurazione del router HSRP in questo documento. Se la connettività del layer fisico è corretta, controllare che le modalità VTP corrispondano.

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

Caso di studio n. 4: Cambiamenti di stato HSRP e segnalazione dello switch SYS-4-P2_WARN: sfasamento di 1/host <indirizzo_mac> tra porta <porta_1> e porta <porta_2> in Syslog

Possono comparire i messaggi di errore:

```
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

Negli switch Catalyst, lo switch segnala un indirizzo MAC host che si sposta se l'indirizzo MAC host viene spostato due volte entro 15 secondi. Una possibile causa è un loop STP. Lo switch ignora i pacchetti provenienti da questo host per circa 15 secondi nel tentativo di ridurre al minimo le conseguenze di un loop STP. Se l'indirizzo MAC instabile è l'indirizzo MAC virtuale HSRP, probabilmente l'errore è causato dal passaggio allo stato `attivo` di entrambi i router HSRP.

Se l'errore riguarda un indirizzo MAC diverso, la causa potrebbe essere un loop, un pacchetto duplicato o riflesso nella rete. Queste condizioni possono contribuire ai problemi HSRP. Le cause più comuni di questo tipo di errore sono problemi del protocollo STP o problemi del layer fisico.

Quando si risolve questo messaggio di errore, attenersi alla seguente procedura:

> **Nota**: completare anche i passaggi descritti nella sezione Risoluzione dei problemi relativi all'HSRP sugli switch Catalyst in questo documento.

1. Determinare l'origine (porta) corretta dell'indirizzo MAC host.

2. Disconnettere la porta che non deve avere come origine l'indirizzo MAC dell'host.
3. Controllare la topologia STP di ciascuna VLAN e verificare che non vi siano errori STP.
4. Verificare la configurazione del port-channel.Una configurazione errata del port-channel può comportare messaggi di errore di instabilità generati dall'indirizzo MAC host. Ciò è dovuto alla natura di bilanciamento del carico del port-channel.

Caso di studio n. 5: Routing asimmetrico e HSRP (sovraccarico del traffico unicast nella rete con router con HSRP)

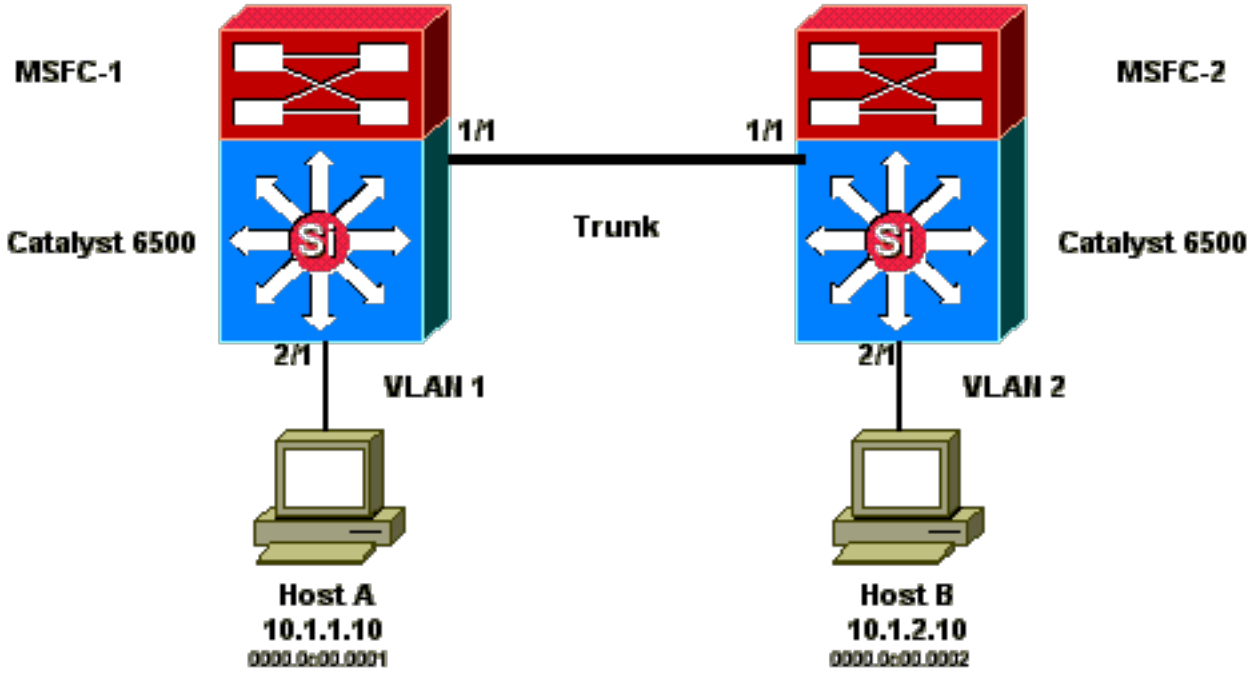
Con il routing asimmetrico, i pacchetti di trasmissione e ricezione utilizzano percorsi diversi tra un host e il peer con cui comunicano. Questo flusso di pacchetto è il risultato della configurazione del bilanciamento del carico tra i router HSRP, basato sulla priorità HSRP, che imposta l'HSRP su attivo o in standby. Questo tipo di flusso di pacchetti in un ambiente di switching può causare un invio eccessivo di pacchetti unknown unicast a tutte le porte (flooding). Inoltre, le voci Multilayer Switching (MLS) possono essere assenti. Questa condizione si verifica quando lo switch inoltra un pacchetto unicast a tutte le porte. Lo switch esegue il flooding del pacchetto perché non trova l'indirizzo MAC di destinazione. Questo comportamento non interrompe la connettività perché i pacchetti vengono comunque inoltrati, ma tiene conto dei pacchetti extra inviati alle porte host. In questa sezione viene analizzato il comportamento del routing asimmetrico e perché la conseguenza è il flooding unicast.

I sintomi del routing asimmetrico includono:

- Flooding eccessivo di pacchetti unicast
- Voce MLS assente nei flussi
- Traccia sniffer che segnala come i pacchetti sulla porta host non siano destinati all'host
- Maggiore latenza di rete con i motori che reindirizzano gli URL dei pacchetti L2 (rewrite engine), come i bilanciatori del carico dei server, i dispositivi di cache Web e le appliance di reteGli esempi includono Cisco LocalDirector e Cisco Cache Engine.
- Pacchetti eliminati sulle postazioni di lavoro e gli host connessi che non sono in grado di gestire il carico extra del flooding di pacchetti unicast

  Nota: il tempo di permanenza predefinito della cache ARP su un router è di quattro ore. La durata predefinita della voce Content-Addressable Memory (CAM) dello switch è cinque minuti. Il tempo di aging ARP delle workstation host non è significativo per questa discussione. Tuttavia, nell'esempio il tempo di aging ARP viene impostato su quattro ore.

Questo diagramma illustra il problema. Nella topologia dell'esempio, vengono usati Catalyst 6500 con MSFC (Multilayer Switch Feature Card), ma è possibile usare qualsiasi router al posto dell'MSFC. I router utilizzabili includono il Route Switch Module (RSM), il Gigabit Switch Router (GSR) e Cisco 7500. Gli host sono collegati direttamente alle porte dello switch. Gli switch sono interconnessi tramite un trunk che trasporta il traffico per la VLAN 1 e la VLAN 2.



Questi output sono estratti del comando **show standby** su ciascuna MSFC.

MSFC1

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

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

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

MSFC2

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

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

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

Nota: sull'MSFC1, la VLAN 1 è nello stato `attivo` dell'HSRP e la VLAN 2 nello stato di `standby` dell'HSRP. Sulla MSFC2, la VLAN 2 è nello stato HSRP `attivo`, la VLAN 1 è nello stato HSRP di `standby`. Il gateway predefinito di ciascun host corrisponde all'indirizzo IP di standby.

1. Inizialmente, tutte le cache sono vuote. L'host A utilizza la scheda MSFC1 come gateway predefinito. L'host B utilizza la scheda MSFC2.**Tabelle degli indirizzi ARP e MAC prima dell'avvio del ping Nota**: per brevità, l'indirizzo MAC dello switch 1 per il router HSRP e l'indirizzo MAC non sono inclusi nelle altre tabelle visualizzate in questa sezione.
2. L'host A esegue il ping sull'host B, ovvero l'host A invia un pacchetto echo ICMP. Poiché ciascun host risiede su una VLAN separata, l'host A inoltra i pacchetti destinati all'host B al gateway predefinito. Affinché il processo si verifichi, l'host A deve inviare una richiesta ARP per risolvere l'indirizzo MAC del gateway predefinito, 10.1.1.1.**Tabelle degli indirizzi ARP e MAC dopo che l'host A ha inviato una richiesta ARP per il gateway predefinito**
3. MSFC1 riceve il pacchetto, lo riscrive e lo inoltra all'host B. Per riscrivere il pacchetto, MSFC1 invia una richiesta ARP per l'host B perché l'host non risiede su un'interfaccia connessa direttamente. MSFC2 non ha ancora ricevuto alcun pacchetto in questo flusso. Quando MSFC1 riceve la risposta ARP dall'host B, entrambi gli switch apprendono la porta di origine associata all'host B.**Tabelle degli indirizzi ARP e MAC dopo che l'host A ha inviato il pacchetto al gateway predefinito e MSFC1 ha inviato la richiesta ARP per l'host B**
4. L'host B riceve il pacchetto echo dall'host A tramite MSFC1. L'host B deve ora inviare una risposta echo all'host A. Poiché l'host A risiede su una VLAN diversa, l'host B inoltra la

risposta tramite il gateway predefinito, MSFC2. Per inoltrare il pacchetto tramite MSFC2, l'host B deve inviare un ARP per l'indirizzo IP del gateway predefinito, 10.1.2.1.**Tabelle degli indirizzi ARP e MAC dopo che l'host B ha inviato la richiesta ARP per il gateway predefinito**

5. L'host B inoltra ora il pacchetto di risposta echo all'MSFC2. L'MSFC2 invia una richiesta ARP per l'host A perché è connesso direttamente alla VLAN 1. Lo switch 2 popola la relativa tabella degli indirizzi MAC con l'indirizzo MAC dell'host B.**Tabelle degli indirizzi ARP e MAC dopo che l'host A ha ricevuto il pacchetto echo**
6. La risposta echo raggiunge l'host A e il flusso è completo.

Conseguenze del routing asimmetrico

Si consideri il caso del ping continuo sull'host B da parte dell'host A. Tenere presente che l'host A invia il pacchetto echo a MSFC1 e l'host B invia la risposta echo a MSFC2, che si trova in uno stato di routing asimmetrico. L'unica volta in cui lo switch 1 viene a conoscenza dell'indirizzo MAC di origine dell'host B è quando l'host B risponde a una richiesta ARP di MSFC1. Infatti l'host B utilizza MSFC2 come gateway predefinito e non invia pacchetti all'MSFC1 e, di conseguenza, allo switch 1. Poiché il timeout ARP è di quattro ore per impostazione predefinita, lo switch 1 esegue il conteggio dell'indirizzo MAC dell'host B dopo cinque minuti per impostazione predefinita. Lo switch 2 esegue l'hosting A dopo cinque minuti. Di conseguenza, lo switch 1 deve considerare i pacchetti con indirizzo MAC di destinazione dell'host B come pacchetti unknown unicast. Lo switch invia il pacchetto proveniente dall'host A e destinato all'host B a tutte le porte (flooding). Inoltre, poiché nello switch 1 non è presente alcun indirizzo MAC dell'host B, non sono presenti neanche voci MLS.

Tabelle degli indirizzi ARP e MAC dopo 5 minuti di ping continuo tra l'host B e l'host A

Tabella ARP dell'host A	Tabella degli indirizzi MAC dello switch 1, porta VLAN MAC	Tabella ARP MSFC1	Tabella ARP MSFC2	Tabella degli indirizzi MAC dello switch 2, porta VLAN MAC	Tabella ARP dell'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 : 0003.6bf1.2a01 10.1.2.1 : 0000.0c07.ac01

I pacchetti di risposta echo provenienti dall'host B hanno lo stesso problema dopo l'invio della voce dell'indirizzo MAC dell'host A sullo switch 2. L'host B inoltra la risposta echo all'MSFC2, che a sua volta instrada il pacchetto e lo invia sulla VLAN 1. Lo switch non ha una voce host A nella tabella degli indirizzi MAC e deve instradare il pacchetto su tutte le porte della VLAN 1.

I problemi di routing asimmetrici non interrompono la connettività. Tuttavia, il routing asimmetrico può causare l'invio dei pacchetti unicast a tutte le porte e problemi di voci MLS mancanti. Per rimediare a questa situazione, è possibile apportare tre modifiche alla configurazione:

- Impostare la durata dell'indirizzo MAC sui rispettivi switch a 14.400 secondi (quattro ore) o su un periodo più lungo.
- Modificare il timeout ARP sui router a cinque minuti (300 secondi).
- Modificare la durata dell'indirizzo MAC e il timeout ARP allo stesso valore di timeout.

Il metodo preferibile è modificare la durata dell'indirizzo MAC a 14.400 secondi. Ecco le linee guida per la configurazione:

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

Caso di studio n. 6: l'indirizzo IP virtuale HSRP viene segnalato come un indirizzo IP diverso

Il messaggio di errore `STANDBY-3-DIFFVIP1` si verifica quando la presenza di loop di bridging nello switch causa perdite di dati nelle VLAN.

Se viene visualizzato questo messaggio di errore e si verificano delle perdite di dati nelle VLAN a causa di un loop di bridging nello switch, attenersi alla seguente procedura:

1. Identificare il percorso dei pacchetti tra i nodi finali.Se sul percorso è presente un router, completare questi passaggi:Risolvere i problemi relativi al percorso tra il primo switch e il router.Risolvere i problemi relativi al percorso tra il router e il secondo switch.
2. Connettersi a ogni switch sul percorso e verificare lo stato delle porte utilizzate sul percorso tra i nodi finali.

Caso di studio n. 7: HSRP causa una violazione MAC su una porta protetta

La funzionalità di sicurezza configurata sulle porte dello switch connesse ai router con protocollo HSRP causa una violazione dell'indirizzo MAC, in quanto non è possibile avere lo stesso indirizzo MAC sicuro su più di un'interfaccia. La violazione della sicurezza su una porta sicura si può verificare in una di queste situazioni:

- Alla tabella degli indirizzi è stato aggiunto il numero massimo di indirizzi MAC sicuri e una postazione il cui indirizzo MAC non è presente nella tabella cerca di accedere all'interfaccia.
- L'indirizzo appreso o configurato su un'interfaccia sicura viene visualizzato su un'altra interfaccia sicura nella stessa VLAN.

Per impostazione predefinita, la violazione della sicurezza di una porta causa il passaggio allo stato error-disabled dell'interfaccia dello switch e la sua disattivazione immediata. I messaggi sullo stato HSRP scambiati tra i router vengono bloccati.

Soluzione alternativa

- Usare il comando **standby use-bia** sui router. In questo modo i router useranno un indirizzo BIA (Burned-In Addess) per il protocollo HSRP anziché l'indirizzo MAC virtuale.
- Disabilitare la funzionalità di sicurezza sulle porte dello switch che si connettono ai router che usano il protocollo HSRP.

Caso di studio n. 9: %Interface Hardware Cannot Support Multiple Groups (L'hardware dell'interfaccia non supporta più gruppi)

Se sull'interfaccia vengono creati più gruppi HSRP, viene visualizzato questo messaggio di errore:

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

Questo messaggio di errore viene ricevuto a causa della limitazione hardware presente su alcuni router o switch. Non è possibile superare questa limitazione con il software. Il problema è che ogni gruppo HSRP utilizza un solo indirizzo MAC aggiuntivo sull'interfaccia, quindi il chip MAC Ethernet deve supportare più indirizzi MAC programmabili per supportare più gruppi HSRP.

Per risolvere il problema temporaneamente, usare il comando di configurazione interfaccia **standby use-bia** in modo da usare l'indirizzo BIA (Burned-In Address) dell'interfaccia come indirizzo MAC virtuale anziché l'indirizzo MAC preassegnato.

Risoluzione dei problemi di HSRP sugli switch Catalyst

A. Verifica della configurazione del router HSRP

1. Verifica dell'indirizzo IP univoco dell'interfaccia del router

Verificare che ogni router HSRP abbia un indirizzo IP univoco per ogni subnet di ogni singola interfaccia. Inoltre, verificare che il protocollo di linea dell'interfaccia sia `up`. Per verificare rapidamente lo stato corrente di ciascuna interfaccia, usare il comando **show ip interface brief**. Di seguito è riportato un esempio:

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. Verifica degli indirizzi IP di standby (HSRP) e dei numeri dei gruppi di standby

Verificare che gli indirizzi IP di standby (HSRP) configurati e i numeri dei gruppi di standby corrispondano in ciascun router che appartiene al gruppo HSRP. Una mancata corrispondenza dei gruppi di standby o degli indirizzi di standby HSRP può causare errori. Il comando **show standby** mostra in dettaglio la configurazione del gruppo di standby e dell'indirizzo IP di standby di ciascuna interfaccia. Di seguito è riportato un esempio:

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. Verifica dell'indirizzo IP di standby (HSRP) univoco per ogni interfaccia

Verificare che l'indirizzo IP di standby (HSRP) sia diverso dall'indirizzo IP configurato su ogni interfaccia. Il comando **show standby** permette di verificare rapidamente queste informazioni. Di seguito è riportato un esempio:

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. Uso del comando standy use-bia

A meno che il protocollo HSRP non sia configurato su un'interfaccia Token Ring, usare il comando **standby use-bia** solo in circostanze speciali. Questo comando dice al router di usare il proprio indirizzo BIA anziché l'indirizzo MAC HSRP virtuale del gruppo HSRP. Su una rete Token Ring, se si usa la tecnica SRB (Source-Route Bridging), il comando **standby use-bia** permette al nuovo router attivo di aggiornare la cache Routing Information Field (RIF) dell'host con un ARP gratuito. Tuttavia, non tutte le implementazioni dell'host gestiscono correttamente l'ARP gratuito. Il comando **standby use-bia** presenta un altro problema, che riguarda il proxy ARP. Un router in standby non può recuperare il database del proxy ARP perso in seguito a un errore sul router attivo.

5. Verifica della configurazione dell'elenco degli accessi

Verificare che gli elenchi degli accessi configurati su tutti i peer HSRP non filtrino gli indirizzi HSRP configurati sulle rispettive interfacce. In particolare, verificare l'indirizzo multicast utilizzato per inviare il traffico a tutti i router di una subnet (**224.0.0.2**). Inoltre, verificare che il traffico UDP destinato alla porta HSRP **1985** non sia filtrato. Il protocollo HSRP usa questo indirizzo e questa porta per inviare pacchetti hello tra i peer. Usare il comando **show access-lists** per verificare rapidamente gli elenchi degli accessi configurati sul router. Di seguito è riportato un esempio:

```
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. Verifica della configurazione di trunking e di Catalyst Fast EtherChannel

1. Verifica della configurazione di trunking

Se si utilizza un trunk per connettere i router HSRP, verificare le configurazioni di trunking sui router e sugli switch. Le modalità di trunking sono cinque:

- on
- desirable
- auto
- Disattivato
- nonegotiate

Verificare che le modalità di trunking configurate forniscano il metodo di trunking desiderato.

Usare la modalità `desirable` per le connessioni tra switch quando si risolvono i problemi HSRP. Questa configurazione può isolare i problemi in cui le porte dello switch non sono in grado di stabilire correttamente i trunk. Impostare una configurazione tra router e switch come nonegotiate in quanto la maggior parte dei router Cisco IOS non supporta la negoziazione di un trunk.

Per la modalità trunking IEEE 802.1Q (dot1q), verificare che entrambi i lati del trunk siano configurati per utilizzare la stessa VLAN nativa e lo stesso incapsulamento. Poiché i prodotti Cisco non contrassegnano la VLAN nativa per impostazione predefinita, una mancata corrispondenza delle configurazioni VLAN native comporterà assenza di connessione sulle VLAN non corrispondenti. Infine, verificare che il trunk sia configurato in modo da trasportare le VLAN configurate sul router e verificare che le VLAN non siano in modalità pruning e nello stato STP sulle porte connesse al router. Utilizzare il comando **show interfaces <interface> trunk** per ottenere un riferimento rapido con queste informazioni. Di seguito è riportato un esempio:

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. Verifica della configurazione di Fast EtherChannel (port-channel)

Se si usa un port-channel per connettere i router HSRP, verificare la configurazione di EtherChannel sui router e sugli switch. Configurare un port-channel tra switch come desirable su almeno un lato. L'altro lato può essere in una di queste modalità:

- on
- desirable
- auto

Tuttavia, nell'esempio riportato, le interfacce non sono membri di un canale porta:

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. Esame della tabella di inoltro degli indirizzi MAC dello switch

Verificare che la tabella degli indirizzi MAC dello switch abbia le voci corrette per i router HSRP, per l'indirizzo MAC virtuale HSRP e per gli indirizzi BIA fisici. Il comando **show standby** sul router

restituisce l'indirizzo MAC virtuale. Il comando **show interface** fornisce l'indirizzo BIA fisico. Ecco alcuni esempi di output:

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

Accertarsi di controllare la durata CAM per stabilire con quale rapidità scadranno le voci. Se la durata è uguale al valore configurato per il ritardo di inoltro STP, ossia 15 secondi per impostazione predefinita, è molto probabile che ci sia un loop STP nella rete. Ecco un output di esempio del comando:

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. Verifica della connettività del layer fisico

Se più di un router del gruppo HSRP diventa attivo, tali router non ricevono in modo coerente i pacchetti hello dai peer HSRP. I problemi di layer fisico possono impedire la trasmissione coerente del traffico tra i peer e causare questo scenario. Accertarsi di verificare la connettività fisica e la connettività IP tra i peer HSRP quando si esegue la risoluzione dei problemi del protocollo HSRP. Per verificare la connettività, usare il comando **show standby**. Di seguito è riportato un esempio:

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. Controllo dello stato dell'interfaccia

Controllare le interfacce. Verificare che tutte le interfacce con HSRP siano `up/up`, come mostrato nell'esempio:

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

Se una delle interfacce è `down/down`, accedere in modalità di configurazione sul router e immettere il comando **no shutdown** per l'interfaccia specifica. Di seguito è riportato un esempio:

```
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

Se le interfacce sono `down/down` o `up/down`, riesaminare il log e cercare eventuali avvisi di modifica. Sugli switch Cisco IOS Software, in situazioni `up/down` vengono visualizzati i seguenti messaggi:

```
%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
```

Ispezionare le porte, i cavi e tutti i ricetrasmettitori o altri dispositivi che si trovano tra i peer HSRP. Sono tutti presenti e collegati correttamente? Ci sono interfacce su cui il collegamento viene perso ripetutamente? Sono stati utilizzati i tipi di cavo corretti? Verificare la presenza di eventuali errori nelle interfacce, come illustrato nell'esempio seguente:

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. Modifica del collegamento ed errori delle porte

Controllare se vi sono modifiche al collegamento delle porte dello switch o se si sono verificati altri errori. Immettere questi comandi ed esaminare l'output:

- **show logging (visualizza registri)**
- **show interfaces <interface>, contatori**
- **show interfaces <interface> status**

Questi comandi consentono di determinare se esiste un problema di connettività tra gli switch e altri dispositivi.

In situazioni in cui il collegamento è `up/down`, la visualizzazione di questi messaggi è normale:

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

Per determinare lo stato generale di una porta, usare il comando **show interfaces <interface>status**. Di seguito è riportato un esempio:

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

Lo stato dell'interfaccia è `connected` (connesso), `notconnect` (non connesso) o `errdisable`? Se lo stato è `notconnect`, controllare che il cavo sia collegato su entrambi i lati. Verificare che sia stato utilizzato il cavo corretto. Se lo stato è `errdisable`, verificare che il valore misurato dai contatori sia corretto. Per ulteriori informazioni, fare riferimento a Ripristino di una porta disabilitata a causa di un errore sulle piattaforme Cisco IOS.

Per quale VLAN è stata configurata questa porta? Accertarsi che l'altro lato della connessione sia configurato per la stessa VLAN. Se il collegamento è configurato in modalità trunk, assicurarsi che il traffico delle VLAN sia trasmesso su entrambi i lati del trunk.

Come sono configurati la velocità e il duplex? Se l'impostazione è preceduta da a-, la velocità e il duplex vengono negoziati automaticamente sulla porta. In caso contrario, la configurazione è stata eseguita dall'amministratore di rete. Per configurare la velocità e il duplex di un collegamento, le impostazioni devono essere uguali su entrambi i lati del collegamento. Se una porta dello switch è stata configurata per la negoziazione automatica, lo stesso deve essere configurato anche sull'altro lato del collegamento. Se su un lato velocità e duplex sono hardcoded, altrettanto deve essere specificato sull'altro lato. Se si lascia la negoziazione automatica su un lato mentre l'altro lato è hardcoded, il processo di negoziazione automatica si interrompe.

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**

Gli errori `Align-Err`, `FCS-Err` o `Runts` sono numerosi? Questi errori indicano che la velocità e il duplex tra la porta e il dispositivo connesso non corrispondono. Modificare le impostazioni di

velocità e duplex della porta interessata per correggere questi errori.

Usare il comando **show mac** per verificare che la porta trasmetta il traffico. Le colonne `In` e `Out` indicano il numero di pacchetti unicast, multicast e broadcast che vengono ricevuti e trasmessi su una particolare porta. I contatori in basso rivelano il numero di pacchetti scartati o persi e se questi pacchetti fanno parte del traffico in entrata o in uscita. `Le opzioni Lrn-Discrd`, `In-Lost` e `Out-Lost` contano il numero di pacchetti che sono stati inoltrati o scartati erroneamente a causa di buffer non sufficienti.

`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. Verifica della connettività IP

Verificare la connettività IP. Eseguire un ping IP tra il router associato e il dispositivo HSRP remoto. Ciò aiuta a capire se ci sono problemi di perdita momentanea di connettività. Un ping esteso è disponibile solo in modalità enable. Ecco un output di esempio del comando:

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

Eseguire il ping tra ciascun router HSRP e i relativi peer per determinare dove si verifica l'errore di connettività.

4. Controllo della presenza di collegamenti unidirezionali

Controllare se tra lo switch e i peer HSRP si verificano collegamenti unidirezionali. Un collegamento unidirezionale si verifica ogni volta che il traffico proveniente da un dispositivo locale su un collegamento viene ricevuto dal nodo vicino, ma il traffico proveniente dal nodo vicino non viene ricevuto dal dispositivo locale. Questa funzionalità è nota come modalità UDLD (UniDirectional Link Detection) aggressiva. L'uso della funzionalità UDLD è possibile solo se supportata su entrambi i lati della connessione. La modalità UDLD aggressiva agisce sul Layer 2 per determinare se il collegamento è stata stabilito correttamente e se il traffico scorre in entrambe le direzioni tra i router vicini corretti. Ecco alcuni esempi di output dei comandi:

> **Nota**: passare al collegamento successivo per Comprendere e configurare le funzionalità UDLD. Dipende dalla piattaforma in uso.

Un'altra opzione che consente di verificare un collegamento unidirezionale se il protocollo UDLD

non è disponibile è tramite il protocollo CDP (Cisco Discovery Protocol). Il protocollo CDP, quando abilitato, offre un metodo alternativo per rilevare la presenza di un collegamento unidirezionale. Se solo un lato del collegamento può vedere il dispositivo adiacente, sostituire il cavo tra i dispositivi e verificare che non vi siano interfacce difettose.

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. Ulteriori riferimenti per la risoluzione dei problemi del layer fisico

Fare riferimento a questi documenti:

- Configurazione e risoluzione dei problemi Ethernet 10/100/1000Mb Half/Full Duplex Auto-Negotiation
- Ripristino di una porta disabilitata a causa di un errore sulle piattaforme Cisco IOS
- Risoluzione dei problemi di compatibilità NIC degli switch Cisco Catalyst
- Sezione Descrizione degli errori del collegamento dati nel documento Risoluzione dei problemi di compatibilità NIC degli switch Cisco Catalyst
- Risoluzione dei problemi relativi alle porte e alle interfacce dello switch

D. Debug HSRP sul Layer 3

Se le modifiche dello stato dell'HSRP sono frequenti, utilizzare i comandi di debug dell'HSRP (in modalità abilitazione) sul router per monitorare l'attività dell'HSRP. Queste informazioni permettono di determinare quali sono i pacchetti HSRP ricevuti e inviati dal router e devono essere riportati al supporto tecnico Cisco in caso si sia richiesto un intervento di assistenza. L'output del debug mostra anche le informazioni sullo stato HSRP, insieme agli account dettagliati dei pacchetti hello HSRP.

1. Debug HSRP standard

In Cisco IOS, abilitare la funzionalità di debug HSRP con il comando **debug standby**. Queste informazioni sono utili quando i problemi sono intermittenti e interessano solo alcune interfacce. Il debug permette di determinare se il router HSRP in questione riceve e trasmette i pacchetti hello HSRP a intervalli specifici. Se il router non riceve i pacchetti hello, il peer non trasmette i pacchetti hello oppure i pacchetti vengono scartati dalla rete.

Comando	Scopo
debug standby	Abilita il debug per il protocollo HSRP

Ecco un output di esempio del comando:

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. Debug HSRP condizionato (output limitato in base al gruppo di standby e/o alla VLAN)

In Cisco IOS Software Release 12.0(3), è stata introdotta l'opzione di debug per poter filtrare l'output del comando **debug standby** in base all'interfaccia e al numero del gruppo. Il comando usa il paradigma della condizione di debug introdotto in Cisco IOS Software Release 12.0.

Comando	Scopo
debug condition standby <interfaccia> <gruppo>	Abilita il debug condizionato per il protocollo HSRP del grup (0–255)

L'interfaccia deve essere un'interfaccia valida in grado di supportare il protocollo HSRP. Il gruppo può essere qualsiasi gruppo, da 0 a 255. È possibile impostare una condizione di debug per i gruppi che non esistono. Ciò consente di acquisire i debug durante l'inizializzazione di un nuovo gruppo. Il debug di standby deve essere abilitato per produrre un output. Se non esistono condizioni di debug di standby, viene prodotto l'output di debug di tutti i gruppi su tutte le interfacce. Se esiste almeno una condizione di debug di standby, l'output del debug di standby viene filtrato in base a tutte le condizioni di debug di standby. Ecco un output di esempio del comando:

```
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. Debug HSRP avanzato

In Cisco IOS Software Release 12.1(1) è stato aggiunto il debug HSRP avanzato. Per trovare informazioni utili, il debug HSRP avanzato limita il rumore nei messaggi hello inviati a intervalli regolari e include ulteriori informazioni sullo stato. Queste informazioni sono particolarmente utili quando è stata inviata una richiesta di assistenza e si deve illustrare il problema al tecnico del supporto Cisco.

Comando	Scopo
debug standby	Visualizza tutti gli errori, gli eventi e i pacchet HSRP
debug standby errors	Visualizza gli errori HSRP
debug standby events [[all] | [hsrp | redundancy | track]] [detail]	Visualizza gli eventi HSRP
debug standby packets [[all | terse] | [advertise | coup | hello | resign]] [detail]	Visualizza i pacchetti HSRP
debug standby	Visualizza un intervallo limitato di errori, ever pacchetti HSRP

Ecco un output di esempio del comando:

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

Èpossibile usare il debug condizionato dell'interfaccia e/o del gruppo HSRP per filtrare questo output di debug.

Comando	Scopo
debug condition interface interface	Abilita il debug condizionato dell'interfaccia
debug condition standby <interfaccia> <gruppo>	Abilita il debug condizionato del protocollo HSRP

Nell'esempio, il router si collega a un gruppo HSRP preesistente:

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. Risoluzione dei problemi del protocollo Spanning Tree (STP)

I loop STP o l'instabilità in una rete possono impedire la corretta comunicazione tra i peer HSRP.

A causa di questi problemi di comunicazione, ogni peer diventa un router attivo. I loop STP possono causare tempeste di trasmissione (broadcast storm), frame duplicati e incoerenze nella tabella MAC. Tutti questi problemi riguardano l'intera rete e in particolare il protocollo HSRP. I messaggi di errore HSRP possono essere il primo segnale di un problema STP.

Quando si risolvono i problemi del protocollo STP, è *necessario* conoscere la topologia STP della rete su ciascuna VLAN. È necessario stabilire quale switch è il bridge root e quali porte dello switch sono in fase di blocco o di inoltro. Poiché ogni VLAN ha una propria topologia STP, queste informazioni sono molto importanti.

1. Verifica della configurazione del protocollo Spanning Tree (STP)

Accertarsi che il protocollo STP sia configurato su ogni switch e dispositivo di bridging della rete. Prendere nota di dove ogni switch ritiene che si trovi il bridge root. Inoltre, prendere nota dei valori di questi timer:

- Durata massima root
- Frequenza di invio dei messaggi hello
- Ritardo di inoltro

Usare il comando **show spanning-tree** per visualizzare tutte queste informazioni. Per impostazione predefinita, il comando visualizza queste informazioni per tutte le VLAN. Tuttavia, è possibile filtrare altre informazioni sulla VLAN anche se si fornisce il numero di VLAN con il comando. Queste informazioni sono molto utili quando si risolvono i problemi del protocollo STP.

I tre timer menzionati nell'output **show spanning-tree** vengono appresi dal bridge radice. Questi timer non devono corrispondere ai timer impostati sul bridge specifico. Tuttavia, accertarsi che i timer corrispondano alle impostazioni del bridge root nel caso in cui, in qualsiasi momento, questo switch diventi il bridge root. Se i timer corrispondono alle impostazioni del bridge root, sarà più facile continuare a gestire la rete. Inoltre, sarà impossibile per uno switch con i timer non corrispondenti bloccare la rete.

> **Nota**: abilitare l'opzione STP per tutte le VLAN in qualsiasi momento, indipendentemente dal fatto che la rete contenga collegamenti ridondanti. Se si abilita il protocollo STP nelle reti non ridondanti, si impedisce che il collegamento venga interrotto. Un'interruzione può verificarsi se qualcuno collega gli switch con hub o altri switch e crea accidentalmente un loop fisico. Il protocollo STP è molto utile anche per isolare problemi specifici. Se l'abilitazione del protocollo STP disturba il funzionamento di un altro componente della rete, potrebbe essersi verificato un problema che deve essere isolato.

Di seguito è riportato un output di esempio del comando **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

Lo switch L2Switch_1 è la radice della VLAN 10 e della VLAN 11.

2. Condizioni di loop STP

Affinché si verifichi un loop STP, è necessario che sia presente una ridondanza fisica L2 nella rete. Un protocollo STP non funziona se non esiste la possibilità di una condizione di loop fisico. I sintomi di una condizione di loop STP sono:

- Interruzioni della rete totale
- Perdita di connettività
- Report del dispositivo di rete con elevato utilizzo di processi e sistemi

Una singola VLAN che presenta un loop STP può creare una congestione sul collegamento e ridurre la larghezza di banda delle altre VLAN. Il comando **show interfaces <interface>controller** rileva le porte che trasmettono o ricevono un numero eccessivo di pacchetti. Un numero eccessivo di pacchetti broadcast e multicast su una porta può essere il segnale di un loop STP. In genere, sospettare la presenza di un loop sul collegamento ogni volta che il numero di pacchetti multicast o broadcast supera il numero di pacchetti unicast.

> **Nota**: lo switch conta anche le BPDU (Bridge Protocol Data Unit) STP ricevute e trasmesse come frame multicast. Una porta che si trova nello stato di blocco STP trasmette e riceve ancora unità BPDU STP.

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. Notifica di cambio della topologia

Un altro comando fondamentale per la diagnosi dei problemi dell'STP è il comando **show spanning-tree detail**. Questo comando traccia i messaggi TCN (Topology Change Notification) fino a risalire all'origine. Questi messaggi, inviati come BPDU speciali tra switch, segnalano la presenza di una modifica alla topologia in uno switch. Lo switch interessato dalla modifica invia un messaggio TCN alla porta root. Il messaggio TCN risale in alto nella topologia fino al bridge root. Il bridge root invia quindi un altro BPDU speciale, un'unità TCA (Topology Change Acknowledgement), su tutte le sue porte. Il bridge root imposta il bit TCN nella configurazione BPDU. Questo fa sì che tutti i bridge non root impostino il timer di durata della tabella degli indirizzi MAC sul ritardo di inoltro STP di configurazione.

Per isolare il problema, accedere al bridge radice per ciascuna VLAN e usare il comando **show spanning-tree <interface>detail** per le porte connesse allo switch. La voce `Ultima modifica` indica l'ora in cui è stato ricevuto l'ultimo TCN. In questa situazione, è troppo tardi per vedere chi ha inviato i TCN responsabili del loop STP. La voce `Numero di modifiche alla topologia` fornisce un'idea sul numero di TCN che si verificano. Durante un loop STP, questo contatore può aumentare ogni minuto. Per ulteriori informazioni, vedere Considerazioni sul protocollo Spanning Tree e sulla progettazione correlata.

Altre informazioni utili sono:

- Porta dell'ultimo TCN
- Ora dell'ultimo TCN
- Conteggio corrente dei TCN

Ecco un output di esempio del comando:

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

Questo output mostra che l'ultima modifica della topologia è stata apportata da un dispositivo connesso tramite l'interfaccia Gigabit Ethernet 1/0/35. Quindi, usare lo stesso comando **show spanning-tree detail** da questo dispositivo per cercare di tenere traccia del problema. Se lo switch che genera i TCN è collegato solo a PC o a endpoint, verificare che STP PortFast sia abilitato su queste porte. Il protocollo STP PortFast elimina le notifiche TCN STP quando una porta cambia stato.

Per informazioni sul protocollo STP e su come risolvere i problemi relativi ai cambi di stato del collegamento associati alle schede di interfaccia di rete, o NIC (Network Interface Cards), fare riferimento a questi documenti:

- Utilizzo di PortFast e di altri comandi per correggere i ritardi di connettività all'avvio della postazione di lavoro
- Comprendere il protocollo 802.1w (Rapid Spanning Tree Protocol)
- Considerazioni sulla progettazione del protocollo STP e relativi problemi

4. Disconnessione delle porte bloccate

Poiché la funzionalità Fast EtherChannel (FEC) (port-channel) esegue il bilanciamento del carico, potrebbe contribuire a causare problemi nel protocollo HSRP o nel protocollo STP. Quando si esegue la risoluzione dei problemi con STP o HSRP, è possibile rimuovere la configurazione per qualsiasi connessione FEC. Dopo aver apportato le modifiche alla configurazione, usare il comando **show spanning-tree blockedports** su entrambi gli switch. Accertarsi che almeno una delle porte venga bloccata su entrambi i lati della connessione.

Per informazioni sul Fast EtherChannel, fare riferimento a questi documenti:

- Comprensione del bilanciamento del carico e della ridondanza EtherChannel sugli switch Catalyst
- Configurazione di EtherChannel

5. Interruzione dei pacchetti broadcast

Abilitare l'interruzione dei pacchetti broadcast per mitigare l'impatto di una tempesta di trasmissioni. La tempesta di trasmissioni è uno dei principali effetti collaterali di un loop STP. Ecco un output di esempio del comando:

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. Accesso dalla console e in modalità Telnet

Il traffico della console o in modalità Telnet e destinato allo switch spesso diventa troppo lento per risalire correttamente al dispositivo che ha creato il loop STP. Per forzare il ripristino immediato

della rete, rimuovere tutti i collegamenti fisici ridondanti. Dopo che il protocollo STP si è riallineato alla nuova topologia non ridondante, ricollegare i collegamenti ridondanti uno alla volta. Il verificarsi del loop STP all'aggiunta di un particolare segmento permette di identificare subito i dispositivi che hanno causato il problema.

7. Funzioni Spanning Tree: Portfast, UplinkFast e BackboneFast

Verificare che le funzionalità PortFast, UplinkFast e BackboneFast siano configurate correttamente. Quando si risolvono i problemi STP, disabilitare tutti le funzionalità STP avanzate (UplinkFast e BackboneFast). Inoltre, verificare che la funzionalità STP PortFast sia abilitata solo sulle porte connesse direttamente agli host non bridging. Gli host non bridging includono postazioni di lavoro degli utenti e router che non hanno gruppi di bridge. Non abilitare PortFast sulle porte che sono connesse ad hub o altri switch. Di seguito sono riportati alcuni documenti che consentono di comprendere e configurare queste funzionalità:

Configurazione di Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast e Loop Guard

Comprendere e configurare la funzione Cisco UplinkFast

8. BPDU Guard

Quando si abilita la funzionalità PortFast BPDU Guard, lo stato di una porta PortFast non trunking diventa errdisable al ricevimento di una BPDU. Questa funzione consente di individuare le porte configurate in modo errato per PortFast. La funzione rileva anche il punto in cui i dispositivi riflettono i pacchetti o inseriscono BPDU STP nella rete. Quando si risolvono i problemi STP, è possibile abilitare questa funzione per isolare il problema STP.

```
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. PVTP Pruning

Quando la funzionalità VTP Pruning è abilitata nella rete, i dispositivi di un gruppo HSRP possono attivarsi. Ciò provoca conflitti IP tra i gateway e causa problemi di traffico. Accertarsi che la VLAN di un gruppo HSRP non sia in modalità VTP Pruning.

F. Divide and Conquer

Se tutti gli altri tentativi di isolare o risolvere i problemi HSRP non hanno esito positivo, usare il metodo "divide et impera". Questo metodo consiste nell'isolare la rete e i componenti che la compongono. Per isolare la rete, fare riferimento alle linee guida di questo elenco:

> **Nota**: questo elenco ripete alcune linee guida tratte da altre sezioni del presente documento.

- Creare una VLAN di prova per il protocollo HSRP e una VLAN isolata per lo switch con i router HSRP.
- Disconnettere tutte le porte ridondanti.

- Scomporre le porte FEC in singole porte connesse.
- Ridurre i membri del gruppo HSRP a soli due membri.
- Restringere il traffico sulle porte trunk con la modalità VTP Pruning in modo che solo le VLAN necessarie si propaghino su tali porte.
- Scollegare gli switch connessi nella rete fino a quando i problemi non si verificano più.

Problemi noti

Stato HSRP flapping/instabile quando si utilizzano Cisco 2620/2621, Cisco 3600 con Fast Ethernet

Questo problema può verificarsi con le interfacce Fast Ethernet a seguito di un'interruzione della connettività di rete o dell'aggiunta di un router HSRP con priorità più elevata. Quando il protocollo HSRP cambia stato da attivo a speak, il router reimposta l'interfaccia in modo da rimuovere l'indirizzo MAC HSRP dal filtro degli indirizzi MAC delle interfacce. Il problema si verifica solo sui dispositivi specifici che vengono utilizzati sulle interfacce Fast Ethernet per i Cisco 2600, 3600 e 7500. Il ripristino dell'interfaccia del router provoca un cambio di stato del collegamento sulle interfacce Fast Ethernet e lo switch rileva tale cambio. Se lo switch esegue il protocollo STP, il cambio di stato provoca una transizione STP. Il protocollo STP impiega 30 secondi per far passare la porta allo stato forwarding. Questo tempo corrisponde al doppio del ritardo di inoltro predefinito di 15 secondi. Allo stesso tempo, il router speaking passa allo stato di `standby` dopo 10 secondi, ossia dopo il tempo di attesa impostato per il protocollo HSRP. Il protocollo STP non sta inoltrando i pacchetti, quindi nessun messaggio hello HSRP viene ricevuto dal router attivo. In questo modo il router di standby diventa attivo dopo circa 10 secondi. Entrambi i router sono ora `attivi`. Quando le porte STP passano allo stato forwarding, il router con priorità più bassa passa da attivo a speak e l'intero processo si ripete.

Piattaforma	Descrizione	ID bug Cisco	Fix	Soluzione alternativa
Cisco 2620/2621	L'interfaccia Fast Ethernet inizia a diventare instabile quando è configurato il protocollo HSRP e il cavo è scollegato.		Un aggiornamento del software; fare riferimento al bug per i dettagli della revisione.	Abilita il protocollo Spanning Tree PortFas sulla porta dello switch connesso.
Cisco 2620/2621	Lo stato HSRP è instabile sui Cisco 2600 con Fast Ethernet.		Cisco IOS Software Release 12.1.3	Abilita il protocollo Spanning Tree PortFas sulla porta dello switch connesso.
Cisco 3600 con NM-1FE-TX[1]	Lo stato HSRP è instabile sull'interfaccia Fast Ethernet 2600 e 3600.		Cisco IOS Software Release 12.1.3	Abilita il protocollo Spanning Tree PortFas sulla porta dello switch connesso.
Cisco 4500 con interfaccia Fast Ethernet	Lo stato HSRP è instabile sull'interfaccia Fast Ethernet 4500.	ID bug Cisco CSCds1605	Cisco IOS Software Release 12.1.5	Abilita il protocollo Spanning Tree PortFas sulla porta dello switch connesso.

[1]NM-1FE-TX = modulo di rete Fast Ethernet (interfaccia 10/100BASE-TX) su una porta

In alternativa, è possibile regolare i timer HSRP in modo che il ritardo di inoltro STP sia inferiore

alla metà del tempo di attesa HSRP predefinito. Il ritardo di inoltro STP predefinito è 15 secondi e il tempo di attesa HSRP predefinito è 10 secondi.

Quando si usa il comando **track** nel processo HSRP, Cisco consiglia di ridurre il ritardo di inoltro di un valore prestabilito per evitare instabilità.

Ecco una configurazione di esempio in un router HSRP attivo quando si usa il comando **track**:

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

Dove 15 è il valore di decremento quando l'oggetto flap. Per ulteriori informazioni sul comando track, passare all'opzione Track del documento nell'esempio di configurazione HSRPv2.

Informazioni correlate

- Switch Catalyst LAN per campus - Accesso
- Switching per LAN
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).