

Resolución de Problemas de HSRP en las Redes de Switch Catalyst

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Introducción a HSRP](#)

[Antecedentes](#)

[Operación básica](#)

[Términos de HSRP](#)

[Direccionamiento HSRP](#)

[Configuración del router HSRP](#)

[Comunicación de dirección IP en espera HSRP en todos los medios, excepto Token Ring](#)

[Mensajes de redirección ICMP](#)

[Matriz de funcionalidad HSRP](#)

[Funciones de HSRP](#)

[Formato de paquetes](#)

[Estados de HSRP](#)

[Temporizadores HSRP](#)

[Eventos HSRP](#)

[Acciones de HSRP](#)

[Tabla de estado de HSRP](#)

[Flujo de paquetes](#)

[Configuración del router A \(router activo\)](#)

[Configuración del router B \(router en espera\)](#)

[Estudios de casos para la resolución de problemas de HSRP](#)

[Caso práctico #1: La dirección IP en espera de HSRP se informa como una dirección IP duplicada](#)

[Caso práctico #2: Cambios continuos en el estado de HSRP \(activo, en espera, en voz alta\) o %HSRP-6-STATECHANGE](#)

[Caso práctico #3: HSRP no reconoce a sus iguales](#)

[Caso práctico #4: Cambios de estado de HSRP e informes de switch SYS-4-P2 WARN: 1/EI host está inestable entre el puerto y el puerto en Syslog](#)

[Caso práctico #5: Ruteo asimétrico y HSRP \(Inundación excesiva de tráfico unidifusión en la red con routers que ejecutan HSRP\)](#)

[MSFC1](#)

[MSFC2](#)

[Consecuencias del enrutamiento asimétrico](#)

[Caso práctico #6: La dirección IP virtual de HSRP se informa como una dirección IP diferente](#)

[Caso práctico #7: HSRP provoca una violación de MAC en un puerto seguro](#)

[Caso práctico #9: %Interface Hardware no admite varios grupos](#)

[Resolución de Problemas de HSRP en Switches Catalyst](#)

[A. Verificar la configuración del router HSRP](#)

- [1. Verifique la dirección IP de la interfaz única del router](#)
- [2. Verifique las direcciones IP y los números de grupo en espera \(HSRP\)](#)
- [3. Compruebe que la dirección IP en espera \(HSRP\) es diferente para cada interfaz](#)
- [4. Cuándo Utilizar el Comando standby use-bia](#)
- [5. Verificar la configuración de la lista de acceso](#)

[B. Verificar la Configuración de Catalyst Fast EtherChannel y Trunking](#)

- [1. Verifique la configuración de troncal](#)
- [2. Verifique la configuración de Fast EtherChannel \(Port Channel\)](#)
- [3. Investigue la tabla de reenvío de direcciones MAC del switch](#)

[C. Verifique la conectividad de la capa física](#)

- [1. Compruebe el estado de la interfaz](#)
- [2. Errores de cambio de link y de puerto](#)
- [3. Verifique la conectividad IP](#)
- [4. Compruebe si hay un link unidireccional](#)
- [5. Referencias adicionales de resolución de problemas de capa física](#)

[D. Depuración de HSRP de capa 3](#)

- [1. Depuración HSRP estándar](#)
- [2. Depuración HSRP condicional \(limitación de la salida basada en el grupo en espera y/o VLAN\)](#)
- [3. Depuración HSRP mejorada](#)

[E. Solución de problemas de árbol de expansión](#)

- [1. Verifique la configuración del árbol de expansión](#)
- [2. Condiciones del loop del árbol de expansión](#)
- [3. Notificación de cambio de topología](#)
- [4. Puertos bloqueados desconectados](#)
- [5. Supresión de la difusión](#)
- [6. Acceso Telnet y de consola](#)
- [7. Funciones del árbol de expansión: Portfast, UplinkFast y BackboneFast](#)
- [8. Protección BPDU](#)
- [9. Poda VTP](#)

[F. Dividir y conquistar](#)

[Problemas conocidos](#)

[Inestabilidad/inestabilidad del estado de HSRP al utilizar Cisco 2620/2621, Cisco 3600 con Fast Ethernet](#)

[Información Relacionada](#)

Introducción

Este documento describe problemas comunes y maneras de resolver problemas de Hot Standby Router Protocol (HSRP).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.


La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Introducción a HSRP

Antecedentes

Este documento cubre los siguientes problemas más comunes relacionados con HSRP:


- El router informa que hay una dirección IP en espera HSRP duplicada
- Cambios de estado del HSRP constantes (activo, en espera, hablar)
- Peers HSRP no presentes
- Mensajes de error del switch relacionados con HSRP
- Unidifusión de red excesiva inundando la configuración HSRP

 Nota: Este documento detalla cómo resolver problemas de HSRP en entornos de switch Catalyst. El documento contiene muchas referencias a versiones de software y diseño de topología de red. Sin embargo, el único propósito de este documento es facilitar y guiar a los ingenieros a través de la solución de problemas del HSRP. Este documento no se diseñó para servir como guía de diseño, documento de recomendación de software ni como documento de mejores prácticas.

Las empresas y los consumidores que confían en servicios de intranet e Internet para sus comunicaciones de misión crítica necesitan y esperan que sus redes y aplicaciones estén disponibles en todo momento. Los clientes pueden satisfacer sus demandas de un tiempo de actividad de la red de cerca del 100 por ciento si aprovechan el HSRP en el software Cisco IOS®. El HSRP, que es exclusivo de las plataformas Cisco, proporciona redundancia de red para redes IP de una manera que asegura que el tráfico de usuarios se recupere inmediata y transparentemente de errores en los primeros saltos en dispositivos de borde de red o circuitos de acceso.

Dos o más routers pueden funcionar como un solo router virtual al compartir una dirección IP y una dirección MAC (Capa 2 [L2]). La dirección es necesaria para la redundancia de la gateway predeterminada de la estación de trabajo host. La mayoría de las estaciones de trabajo host no contienen tablas de enrutamiento y sólo utilizan una dirección IP y MAC de salto siguiente (next hop). Esta dirección se conoce como gateway predeterminada. Con HSRP, los miembros del

grupo del router virtual intercambian mensajes de estado en forma continua. Un router puede asumir la responsabilidad de enrutamiento de otro, en el caso de que éste haya quedado fuera de servicio, ya sea por razones planificadas o no planificadas. Los host se configuran con una única gateway predeterminada y continúan reenviando paquetes IP a una dirección IP y MAC coherente. El cambio de dispositivos que realizan el enrutamiento es transparente para las estaciones de trabajo finales.

 Nota: Puede configurar estaciones de trabajo host que ejecuten el sistema operativo de Microsoft para varias puertas de enlace predeterminadas. Sin embargo, los distintos gateways predeterminados no son dinámicos. El OS utiliza sólo una gateway predeterminada a la vez. El sistema sólo selecciona otra gateway predeterminada configurada durante el inicio si el Protocolo de control de mensajes de Internet (ICMP) determina que no puede alcanzar la primera gateway predeterminada configurada.

Operación básica

Un conjunto de routers que ejecutan HSRP trabaja conjuntamente para dar la impresión a los host de la LAN de que son un único router de gateway predeterminado. Este conjunto de routers se conoce como grupo HSRP o grupo en espera. Un único router que se selecciona del grupo es responsable de reenviar los paquetes que los hosts envían al router virtual. Este router se denomina Router activo. Se elige otro router como router en espera. Si el router activo falla, el router en espera asume las tareas de reenvío de paquetes. Aunque un número arbitrario de routers puede ejecutar HSRP, sólo el router activo reenvía los paquetes que se envían a la dirección IP del router virtual.

Para minimizar el tráfico de la red, sólo los routers activo y en espera envían mensajes de HSRP periódicos una vez que el protocolo ha completado el proceso de elección. Los routers adicionales del grupo HSRP permanecerán en el estado *Escuchar*. Si el router activo falla, el router en espera desempeña las funciones de éste. Si el router en espera falla o se convierte en el router activo, entonces se selecciona otro router como router en espera.

Cada grupo en espera emula un único router virtual (gateway predeterminada). Para cada grupo, se asigna una sola dirección MAC e IP conocida a ese grupo. Varios grupos en espera pueden coexistir y superponerse en una LAN y los routers individuales pueden participar en varios grupos. En este caso, el router mantiene estados y temporizadores separados para cada grupo.

Términos de HSRP

Término	Definición
Router activo	El router que actualmente reenvía paquetes al router virtual
Router en reserva	El router de respaldo primario
Grupo de reserva	El grupo de routers que participan en HSRP y emulan conjuntamente un router virtual
Tiempo de saludo	El intervalo entre mensajes sucesivos de saludo de HSRP desde un router dado

Tiempo de espera	El intervalo entre la recepción de un mensaje de saludo y la presunción de que el router de envío ha fallado.
------------------	---

Direccionamiento HSRP

Configuración del router HSRP

Los routers que ejecutan HSRP se comunican la información de HSRP entre ellos mediante los paquetes de saludo de HSRP. Estos paquetes se envían a la dirección IP de multidifusión de destino 224.0.0.2 en el puerto 1985 del Protocolo de datagramas de usuario (UDP). La dirección IP de multidifusión 224.0.0.2 es una dirección de multidifusión reservada que se utiliza para comunicarse con todos los routers. El router activo genera paquetes de saludo desde su dirección IP configurada y la dirección MAC virtual de HSRP. El router en espera genera saludos desde su dirección IP configurada y la dirección MAC programada de fábrica (BIA). El uso de direccionamiento de origen es necesario para que los routers HSRP puedan identificarse entre ellos de forma correcta.

En la mayoría de los casos cuando se configuran routers para que formen parte de un grupo HSRP, éstos están a la escucha de la dirección MAC de HSRP para ese grupo y también intentan detectar su propia BIA. La única excepción a este comportamiento es para los routers 2500, 4000 y 4500 de Cisco. Estos routers disponen de hardware Ethernet que sólo reconoce una sola dirección MAC. Por lo tanto, estos routers utilizan la dirección MAC de HSRP cuando ejercen la función de router activo. Los routers utilizan su BIA cuando ejercen la función de router en espera.

Comunicación de dirección IP en espera HSRP en todos los medios, excepto Token Ring

Dado que las estaciones de trabajo host se configuran con su gateway predeterminada como dirección IP en espera HSRP, los host deben comunicarse con la dirección MAC asociada a la dirección IP en espera HSRP. Esta dirección MAC es una dirección MAC virtual que se compone de 0000.0c07.ac**. ** es el número de grupo HSRP en hexadecimales en base a la interfaz respectiva. Por ejemplo, el grupo 1 de HSRP utiliza la dirección MAC virtual del HSRP 0000.0c07.ac01. Los host en el segmento LAN contiguo utilizan el proceso normal del Protocolo de resolución de direcciones (ARP) para resolver las direcciones MAC asociadas.

Mensajes de redirección ICMP

Los peer routers HSRP que protegen una subred pueden proporcionar acceso a todas las demás subredes de la red. Ésta es la base de HSRP. En consecuencia, es irrelevante qué router se convierte en el router HSRP activo. En las versiones del software Cisco IOS anteriores a la versión 12.1(3)T del software Cisco IOS, los redireccionamientos de ICMP se inhabilitan de manera automática en una interfaz si se utiliza HSRP en ella. Sin esta configuración, los host se pueden redirigir desde la dirección IP virtual de HSRP a una interfaz IP y dirección MAC de un único router. Se pierde la redundancia.

El software Cisco IOS introduce un método para permitir redirecciones ICMP con HSRP. Este método filtra los mensajes salientes de redireccionamiento de ICMP mediante HSRP. La dirección IP de salto siguiente (next hop) se cambia a una dirección virtual HSRP. La dirección IP de la

puerta de enlace en el mensaje saliente de redireccionamiento de ICMP se compara con una lista de routers HSRP activos de esa red. Si el router que corresponde a la dirección IP de la gateway es un router activo para un grupo HSRP, se sustituye la dirección IP de la gateway por la dirección IP virtual de ese grupo. Esta solución permite a los host aprender rutas óptimas hacia redes remotas y, al mismo tiempo, mantener la elasticidad que proporciona HSRP.


Matriz de funcionalidad HSRP

Consulte la sección [Cisco IOS Release and HSRP Functionality Matrix \(Versión de Cisco IOS y matriz de funcionalidad de HSRP\)](#) del documento [Hot Standby Router Protocol Features and Functionality \(Funciones y características del protocolo HSRP\)](#) para conocer las funciones y las versiones del software Cisco IOS que admiten HSRP.

Funciones de HSRP

Consulte [Hot Standby Router Protocol Features and Functionality \(Funciones y características del protocolo HSRP\)](#) para obtener más información sobre las funciones principales de HSRP. Este documento ofrece información sobre las siguientes funciones de HSRP:

- Prioritario
- Seguimiento de interfaz
- Uso de una BIA
- grupos HSRP múltiples
- Direcciones MAC configurables
- Soporte syslog
- Depuración de HSRP
- Depuración HSRP mejorada
- Autenticación
- Redundancia IP
- MIB del protocolo de administración de red simple (SNMP)
- HSRP para Multiprotocol Label Switching (MPLS)

 Nota: Puede utilizar la función Buscar del navegador para localizar estas secciones dentro del documento.

Formato de paquetes

La siguiente tabla muestra el formato de la porción de datos de la trama HSRP UDP:

Versión	Código op	Estado	Hellotime
Tiempo en espera	Prioridad	Grupo	Reservado
Datos de autenticación			
Datos de autenticación			
Dirección IP virtual			

La siguiente tabla describe cada uno de los campos del paquete HSRP:

Campo del paquete	Descripción
Código Op (1 octeto)	El código Op describe el tipo de mensaje que contiene el paquete. Los valores posibles son: 0 - hola, 1 - golpe, y 2 - dimitir. Los mensajes de saludo se envían para indicar que un router ejecuta HSRP y es capaz de convertirse en el router activo. Los mensajes de golpe se envían cuando el router desea pasar a ser el router activo. Los mensajes de retiro se envían cuando un router ya no desea funcionar como router activo.
Estado (1 octeto)	Cada router en el grupo de espera implementa una máquina de estado. El campo de estado describe el estado actual del router que envía el mensaje. Estos son detalles sobre los estados individuales: 0 - inicial, 1 - aprender, 2 - escuchar, 4 - hablar, 8 - en espera y 16 - activo.
Tiempo de saludo (1 octeto)	Este campo sólo tiene sentido en mensajes hello (saludo). Contiene el período aproximado entre los mensajes de saludo que envía el router. El tiempo se expresa en segundos.
Tiempo de espera (1 octeto)	Este campo sólo tiene sentido en mensajes hello (saludo). En él se define cuánto tiempo deben esperar los routers para recibir un mensaje de saludo antes de iniciar un cambio de estado.
Prioridad (1 octeto)	Este campo se utiliza para seleccionar los routers activos y en espera. Si se compara la prioridad de los dos routers, el router de mayor valor pasa a ser el router activo. El ganador es el router con la dirección IP más alta.
Grupo (1 octeto)	Este campo identifica el grupo de espera.
Datos de autenticación (8 octetos)	Este campo contiene una contraseña de texto sin cifrar de ocho caracteres.
Dirección IP virtual (4 octetos)	Si la dirección IP virtual no está configurada en un router, se puede aprender a partir del mensaje de saludo del router activo. Sólo se aprende una dirección si no se configuró una dirección IP en espera HSRP y si el mensaje de saludo se ha autenticado (si la autenticación está configurada).

Estados de HSRP

Estado	Definición
Inicial	Se trata del estado de inicio. Este estado indica que HSRP no se ejecuta. Este estado se ingresa a través de un cambio de configuración o cuando una interfaz está disponible

	por primera vez.
Learn	El router no ha determinado la dirección IP virtual y aún no ha detectado ningún mensaje de saludo autenticado proveniente del router activo. En este estado, el router aún espera recibir noticias del router activo.
Escuchar	El router conoce la dirección IP virtual, pero el router no es el router activo ni el router de reserva. Escucha los mensajes de saludo provenientes de esos routers.
Hablar	El router envía mensajes de saludo periódicos y participa activamente en la elección de un router activo y/o de reserva. Un router no puede pasar al estado de <code>pico</code> a menos que tenga una dirección IP virtual.
Standby	El router es candidato a convertirse en el próximo router activo y envía mensajes de saludo periódicos. Si se excluyen las condiciones pasajeras, hay, como máximo, un router en el grupo, en estado de <code>espera</code> .
Activo	El router actualmente reenvía paquetes que son enviados a la dirección MAC virtual del grupo. El router envía mensajes de saludo periódicos. Si se excluyen las condiciones pasajeras, hay, como máximo, un router en el grupo, en estado <code>activo</code> .

Temporizadores HSRP

Cada router únicamente utiliza tres temporizadores en HSRP. Los temporizadores programan los mensajes de saludo. El HSRP converge, cuando ocurre una falla, según cómo se configuran los temporizadores de saludo y espera del HSRP. De manera predeterminada, estos temporizadores están configurados en 3 y 10 segundos, respectivamente. Esto significa que se envía un paquete de saludo entre los dispositivos del grupo en espera de HSRP cada 3 segundos, y el dispositivo en espera se activa cuando no se recibe un paquete de saludo durante 10 segundos. Puede reducir estos ajustes del temporizador para acelerar la conmutación por error o la preferencia, pero, para evitar un aumento del uso de la CPU y la inestabilidad innecesaria del estado de espera, no establezca el temporizador de saludo en menos de un (1) segundo o el temporizador de espera en menos de 4 segundos. Tenga en cuenta que, si utiliza el mecanismo de seguimiento de HSRP y el enlace de seguimiento falla, la conmutación por error o la preferencia se produce inmediatamente, independientemente de los temporizadores de saludo y de espera. Cuando un temporizador vence, el router pasa a un estado de HSRP nuevo. Los temporizadores se pueden cambiar con este comando: `standby [group-number] timers hellotime holdtime`. Por ejemplo, `standby 1 timers 5 15`.

La siguiente tabla aporta más información acerca de estos temporizadores:

Temporizador	Descripción
Temporizador activo	Este temporizador se utiliza para supervisar el router activo. Este temporizador se inicia en cualquier momento en que un router activo recibe un paquete de saludo. El temporizador vence de acuerdo con el valor del tiempo de espera que se ha fijado en el campo correspondiente del mensaje de saludo HSRP.
Temporizador en espera	Este temporizador se utiliza para supervisar el router en espera. Este temporizador se inicia en cualquier momento en que un router en espera recibe un paquete de saludo. El temporizador vence de acuerdo con el valor del tiempo de espera que se ha fijado en el paquete de saludo correspondiente.
Temporizador hello (saludo)	Este temporizador se utiliza para temporizar los paquetes de saludo. Todos los routers HSRP en cualquier estado de HSRP generan un paquete de saludo

	cuando vence este temporizador de saludo.
--	---

Eventos HSRP

La siguiente tabla proporciona los eventos en la máquina de estado finito HSRP:

Clave	Events
1	HSRP se ha configurado en una interfaz habilitada.
2	HSRP está inhabilitado en una interfaz o la interfaz está inhabilitada.
3	Vencimiento del temporizador activo El temporizador activo se establece en el valor de tiempo de espera cuando se detecta el último mensaje de saludo del router activo.
4	Vencimiento del temporizador en espera El temporizador en espera se establece en el valor de tiempo de espera cuando se detecta el último mensaje de saludo del router en espera.
5	Vencimiento del temporizador de saludo El temporizador periódico para enviar mensajes de saludo ha vencido.
6	Recepción de un mensaje de saludo de mayor prioridad desde un router es estado hablar
7	Recepción de un mensaje de saludo de mayor prioridad desde el router activo
8	Recepción de un mensaje de saludo de menor prioridad desde el router activo
9	Recepción de un mensaje de retiro del router activo
10	Recepción de un mensaje de golpe desde un router de mayor prioridad
11	Recepción de un mensaje de saludo de mayor prioridad desde el router en espera
12	Recepción de un mensaje de saludo de menor prioridad desde el router en espera

Acciones de HSRP

La siguiente tabla especifica las acciones que se deben llevar a cabo como parte de la máquina de estado:

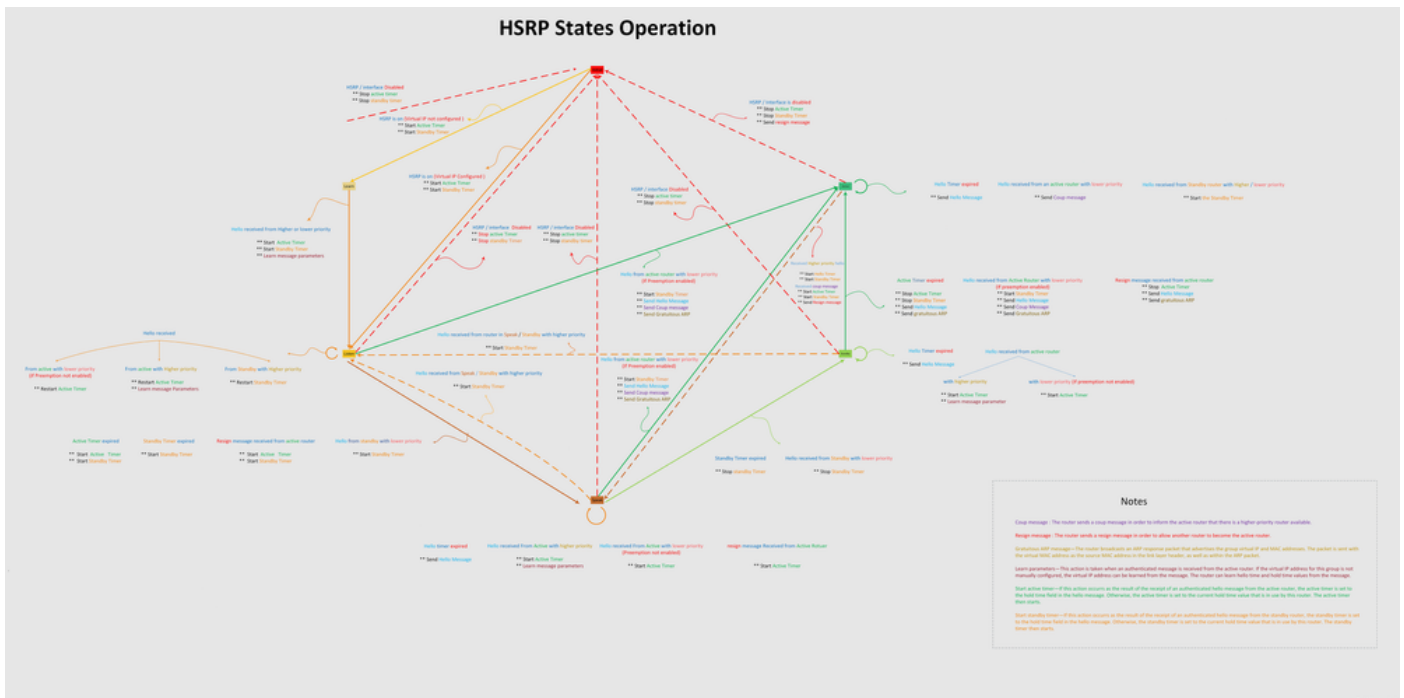
Carta	Acción
R	Iniciar temporizador activo: Si esta acción ocurre como resultado de la recepción de un mensaje de saludo autenticado del router activo, el temporizador activo se establece en el campo de tiempo en espera en el mensaje de saludo. De lo contrario, el temporizador activo utiliza el valor de tiempo de espera actual usado por ese router. A continuación, el temporizador activo se inicia.
B	Iniciar temporizador en espera: Si esta acción ocurre como resultado de la recepción de un mensaje de saludo autenticado del router en espera, el temporizador en espera se establece en el campo de tiempo en espera en el mensaje de saludo. De lo contrario, el temporizador en espera utiliza el valor de tiempo de espera actual usado por ese router. A continuación, el temporizador en espera se inicia.
C	Detener el temporizador activo: El temporizador activo se detiene.
D	Detener el temporizador en espera: El temporizador en espera se detiene.
E	Parámetros de aprendizaje: esta acción se realiza cuando se recibe un mensaje autenticado desde el router activo. Si la dirección IP virtual para este grupo no se configuró manualmente, la dirección IP virtual se puede obtener del mensaje. El router puede

	aprender del mensaje los valores de tiempo de saludo y de tiempo de espera.
F	Enviar mensaje de saludo: El router envía un mensaje de saludo con su estado actual, el tiempo de saludo y el tiempo en espera.
G	Enviar mensaje de impacto: El router envía un mensaje de impacto para informar al router activo que hay un router de mayor prioridad disponible.
H	Enviar mensaje de retiro: El router envía un mensaje de retiro para permitir que otro router se convierta en el router activo.
I	Enviar mensaje ARP gratuito: El router transmite un paquete de respuesta ARP que anuncia la dirección IP virtual y la dirección MAC del grupo. El paquete se envía con la dirección MAC virtual como la dirección MAC de origen en el encabezado de la capa de enlace, así como dentro del paquete ARP.

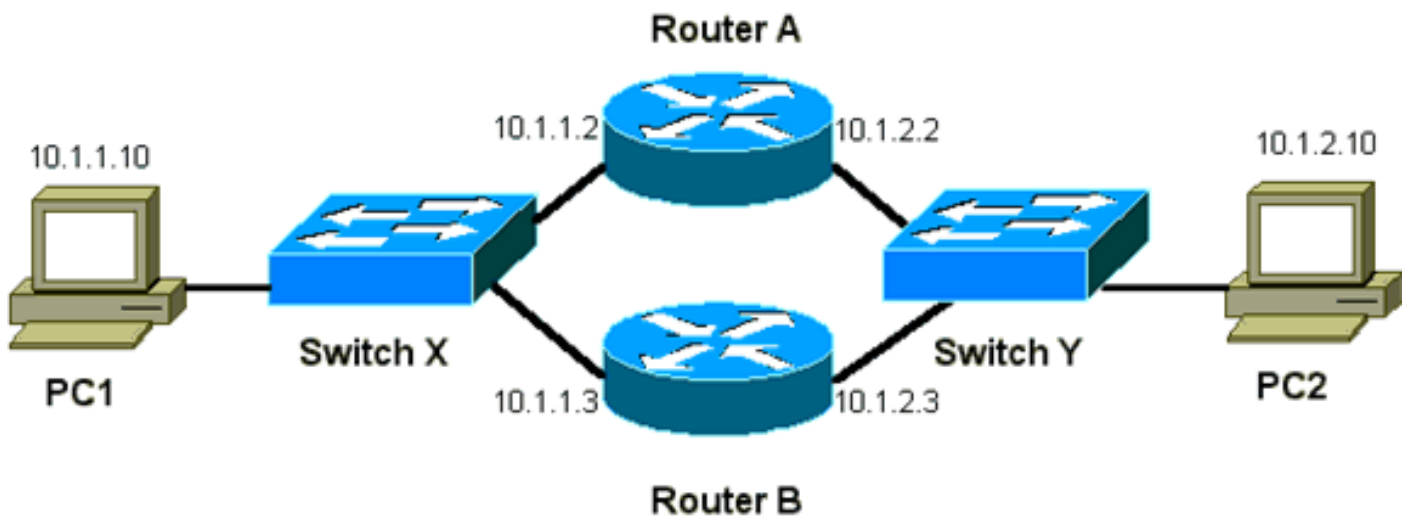
Tabla de estado de HSRP

El diagrama de esta sección muestra los cambios de estado de la máquina de estados de HSRP. Cada vez que ocurre un evento, la acción asociada se lleva a cabo y el router pasa al siguiente estado de HSRP. En el diagrama, los números designan eventos y las letras las acciones asociadas. La tabla de la sección [Eventos del HSRP define los números](#), y la tabla de la sección [Acciones del HSRP define las letras](#). Utilice este diagrama sólo como referencia. El diagrama es detallado y no es necesario para la resolución general de problemas.

Para obtener una imagen de alta resolución del diagrama, [consulte HSRP States Operation](#) (Funcionamiento de los estados del HSRP).



Flujo de paquetes



Dispositivo	Dirección MAC	IP Address	Máscara de subnet	Gateway predeterminado
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

Configuración del router A (router activo)

```
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
```

Configuración del router B (router en espera)

```
interface GigabitEthernet 0/0
ip address 10.1.1.3 255.255.255.0
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: Estos ejemplos configuran direcciones MAC estáticas sólo a título ilustrativo. No configure direcciones MAC estáticas a menos que sea necesario.

Debe entender el concepto detrás del flujo de paquetes cuando obtiene rastros de sabueso para resolver problemas de HSRP. El router A utiliza la prioridad de 200 y se convierte en el router activo de ambas interfaces. En el ejemplo de esta sección, los paquetes provenientes del router destinados a una estación de trabajo host tienen la dirección MAC de origen de la dirección MAC física (BIA) del router. Los paquetes provenientes de las máquinas host destinados a la dirección IP HSRP tienen la dirección MAC de destino de la dirección MAC virtual HSRP. Tenga en cuenta que las direcciones MAC no son las mismas para cada flujo entre el router y el host.

La siguiente tabla muestra la información de las direcciones IP y MAC correspondientes por flujo basándose en un rastro del sabueso tomado del switch X.

Flujo de paquetes	MAC de origen	MAC de destino	IP de origen	IP de destino
Paquetes del PC1 destinados al PC2	PC1 (0000.0c00.0001)	Dirección MAC virtual HSRP de la interfaz Ethernet0 (0000.0c07.ac01) del router A	10.1.1.10	10.1.2.10
Los paquetes que vuelven a través del router A provenientes del PC2 y destinados al PC1	Router A Ethernet 0 BIA (4000.0000.0010)	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.10
Paquetes del PC1 destinados a la dirección IP en espera HSRP (ICMP, Telnet)	PC1 (0000.0c00.0001)	Dirección MAC virtual HSRP de la interfaz Ethernet0 (0000.0c07.ac01) del router A	10.1.1.10	10.1.1.1
Paquetes destinados a la dirección IP real del router activo (ICMP, Telnet)	PC1 (0000.0c00.0001)	Router A Ethernet 0 BIA (4000.0000.0010)	10.1.1.10	10.1.1.2
Paquetes destinados a la dirección IP real del router en espera (ICMP, Telnet)	PC1 (0000.0c00.0001)	Router B Ethernet 0 BIA (4000.0000.0020)	10.1.1.10	10.1.1.3

Estudios de casos para la resolución de problemas de HSRP

Caso práctico #1: La dirección IP en espera de HSRP se informa como una dirección IP duplicada

Estos mensajes de error pueden aparecer:

```
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
```

Estos mensajes de error no necesariamente indican un problema HSRP. Por el contrario, los mensajes de error indican un posible loop del Spanning Tree Protocol (STP) o problema de configuración del router/switch. Los mensajes de error son sólo síntomas de otro problema.

Además, estos mensajes de error no impiden que HSRP funcione correctamente. El paquete HSRP duplicado se ignora. Estos mensajes de error se regulan en intervalos de 30 segundos. Sin embargo, se puede observar un desempeño de la red lento y una pérdida de paquetes como resultado de la inestabilidad de la red que provocan los mensajes de error STANDBY-3-DUPADDR de la dirección HSRP.

Estos mensajes indican específicamente que el router recibió un paquete de datos originado en la dirección IP del HSRP, en la VLAN 25, con las direcciones MAC 0000.0c07.ac19. Dado que la dirección HSRP MAC es 0000.0c07.ac19, el router en cuestión recibió su propio paquete de vuelta o ambos routers en el grupo HSRP ingresaron al estado activo. Dado que el router recibió su propio paquete, es más probable que el problema tenga que ver con la red y no con el router. Hay distintos problemas que pueden provocar este comportamiento. Entre los posibles problemas de red que pueden provocar los mensajes de error encontramos:

- Bucles STP momentáneos
- Problemas de configuración de EtherChannel
- Tramas duplicadas

Cuando resuelva estos mensajes de error, vea los pasos para resolver problemas en la sección [Troubleshooting de HSRP en Switches Catalyst](#) de este documento. Todos los módulos de solución de problemas son aplicables a esta sección, que incluye módulos sobre la configuración. Además, observe los errores en el registro del switch e indique estudios de casos adicionales según corresponda.

Puede utilizar una lista de acceso para evitar que el router activo reciba su propio paquete de saludo multidifusión. Sin embargo, únicamente se trata de una solución alternativa a los mensajes de error y realmente esconde el síntoma del problema. La solución alternativa consiste en aplicar una lista de acceso de entrada extendida a las interfaces HSRP. La lista de acceso bloquea todo el tráfico que proviene de la dirección IP física y destinado a la dirección de multidifusión 224.0.0.2 de todos los routers.

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

```
interface GigabitEthernet 0/0
ip address 172.16.12.3 255.255.255.0
standby 1 ip 172.16.12.1
ip access-group 101 in
```

Caso práctico #2: Cambios continuos en el estado de HSRP (activo, en espera, en voz alta) o %HSRP-6-STATECHANGE

Estos mensajes de error pueden aparecer:

```
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
```

Estos mensajes de error describen una situación en la que un router en espera HSRP no recibió tres paquetes de saludo HSRP sucesivos de su par HSRP. El resultado muestra que el router en espera pasa del estado en espera al estado activo. A partir de allí, el router regresa al estado de reserva inmediatamente. Salvo en el caso de que este error se produzca durante la instalación inicial, es posible que no sea un problema de HSRP el que provoque este mensaje de error. Los mensajes de error indican la pérdida de saludos HSRP entre los pares. Al solucionar este problema, debe verificar la comunicación entre los pares HSRP. El problema más común que provoca estos mensajes es una pérdida aleatoria y momentánea de comunicación de datos entre entidades pares. Los cambios de estado del HSRP a menudo se deben a un alto uso de la CPU. Si el mensaje de error se debe a un uso elevado de la CPU, coloque un analizador de protocolos en la red y rastree el sistema que provoca el uso elevado de la CPU.

Existen varias causas posibles por las que los paquetes HSRP se pierden entre los pares. Los problemas más comunes son [problemas de la capa física](#), tráfico de red excesivo provocado por [problemas del árbol de expansión o tráfico excesivo provocado por cada VLAN](#). Al igual que con el [Caso Práctico n.º 1](#), todos los módulos de solución de problemas son aplicables a la resolución de los cambios de estado de HSRP, en particular la [Depuración de HSRP de Capa 3](#).

Si la pérdida de paquetes HSRP entre pares se debe a un tráfico excesivo causado por cada VLAN, como se mencionó, puede ajustar o aumentar el SPD y mantener el tamaño de la cola para superar el problema de descarte de la cola de entrada.

Para aumentar el tamaño del Descarte selectivo de paquetes (SPD), vaya al modo de configuración y ejecute estos comandos en los switches Cat6500:

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

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

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

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

Para aumentar el tamaño de la cola de espera, vaya al modo de interfaz de VLAN y ejecute este comando:

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

Después de aumentar el tamaño de la cola SPD y hold, puede borrar los contadores de interfaz si ejecuta el comando `clear counter interface`.

Caso práctico #3: HSRP no reconoce a sus iguales

El resultado del router de esta sección muestra un router configurado para HSRP que no reconoce a sus pares HSRP. Para que esto ocurra, el router debe fallar al recibir mensajes de saludo HSRP del router vecino. Para solucionar este problema, consulte la sección [Verify Physical Layer Connectivity \(Verificar la conectividad de la capa física\)](#) y [Verify HSRP Router Configuration \(Verificar la configuración del router HSRP\)](#) de este documento. Si la conectividad de la capa física es correcta, revise los modos de VTP no coincidentes.

```
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 práctico #4: Cambios de estado de HSRP e informes de switch SYS-4-P2_WARN: 1/Host <mac_address> está inestable entre el puerto <port_1> y el puerto <port_2> en Syslog

Estos mensajes de error pueden aparecer:


```
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
```

En los switches Catalyst, el switch informa una dirección MAC del host que se mueve si la dirección MAC del host se mueve dos veces en 15 segundos. Una causa posible es un loop STP. El switch descarta paquetes del host por unos 15 segundos en un esfuerzo por reducir el impacto de un loop STP. Si la dirección MAC que se registra como fluctuante entre dos puertos es la dirección MAC virtual HSRP, probablemente el problema se produce cuando los dos routers HSRP pasan al estado activo .

Si la dirección MAC que se registra no es la dirección MAC virtual HSRP, el problema puede indicar el bucle, duplicación o reflexión de los paquetes en la red. Estos tipos de condiciones pueden contribuir a los problemas de HSRP. Las causas más comunes de los movimientos de las direcciones MAC son los [problemas del árbol de expansión o los problemas de la capa física](#).

Cuando resuelva este mensaje de error, siga los pasos siguientes:

 Nota: Además, complete los pasos de la sección [Troubleshooting de HSRP en Switches Catalyst](#) de este documento.

1. Determine el origen (puerto) correcto de la dirección MAC del host.
2. Desconecte el puerto que no debe originar la dirección MAC del host.
3. Documente la topología STP a nivel VLAN y compruebe si hay fallos de STP.
4. Verifique la configuración de canalización de puerto.
 1. Una configuración de canal de puerto incorrecta puede provocar mensajes de error lanzados por la dirección MAC del host. Esto se debe a la naturaleza de balance de cargas del canal del puerto.

Caso práctico #5: Ruteo asimétrico y HSRP (Inundación excesiva de tráfico unidifusión en la red con routers que ejecutan HSRP)


Con el ruteo asimétrico, los paquetes de transmisión y recepción utilizan diferentes trayectos entre un host y el par con el que se comunica. Este flujo de paquetes es el resultado de la configuración del balanceo de carga entre routers HSRP, basado en la prioridad HSRP, que establece el HSRP en activo o en espera. Este tipo de flujo de paquetes en un entorno de conmutación puede llegar a un flujo excesivo de unidifusión desconocido. Además, se pueden perder entradas de conmutación multicapa (MLS). La saturación de unidifusión desconocida ocurre cuando el switch inunda con un paquete de unidifusión a todos los puertos. El switch inunda con el paquete porque no hay una entrada para la dirección MAC de destino. Este comportamiento no interrumpe la conectividad porque los paquetes siguen reenviándose. Sin embargo, el comportamiento sí es responsable del envío de paquetes adicionales por saturación en los puertos host. Este caso estudia el comportamiento del enrutamiento asimétrico y el motivo de la saturación de unidifusión.

Entre los síntomas de enrutamiento asimétrico se encuentran los siguientes:

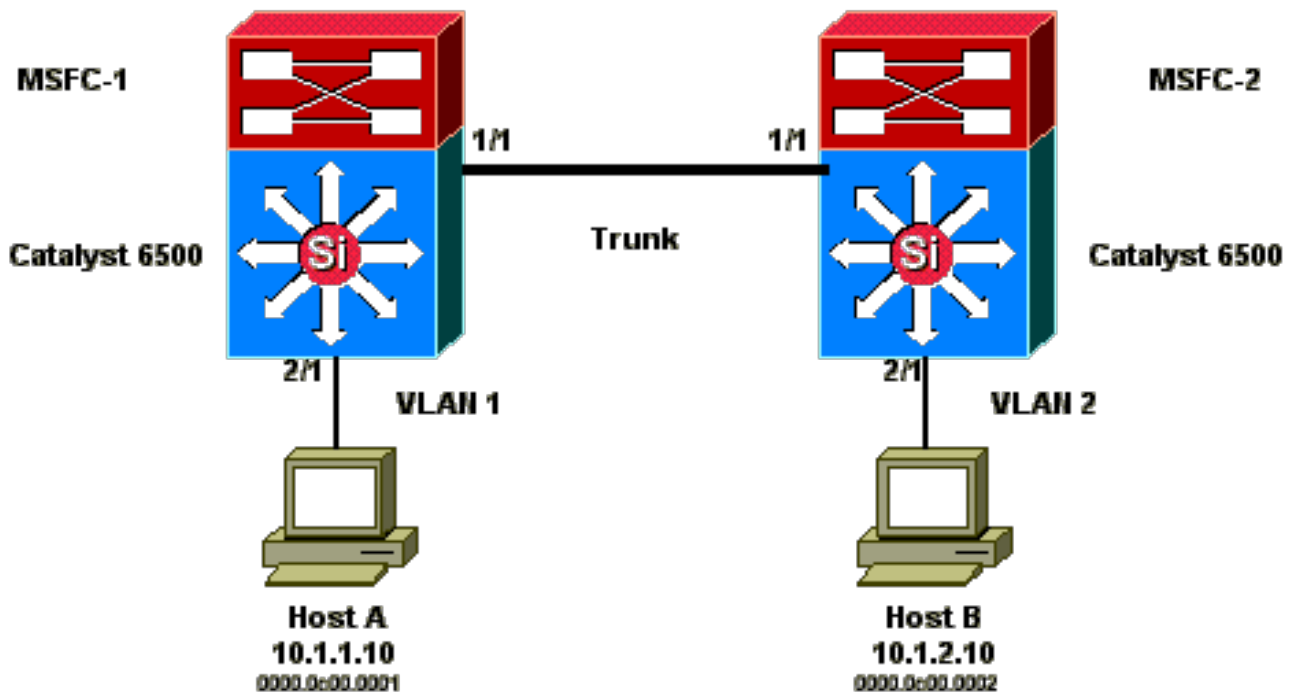
- Flujo excesivo de paquetes de unidifusión
- Falta la entrada de MLS para los flujos
- Un rastro del sabueso (sniffer) que muestra que los paquetes en el puerto del host no van dirigidos al host.
- Latencia de red aumentada con motores de reescritura de los paquetes basados en L2, tales como los mecanismos de balance de cargas de los servidores, los dispositivos de caché de la Web y los dispositivos de red.

Entre los ejemplos están el Cisco LocalDirector y Cisco Cache Engine.

- Paquetes perdidos en los host y estaciones de trabajo conectados que no pueden gestionar la carga adicional de tráfico por saturación de unidifusión

 Nota: El tiempo de envejecimiento predeterminado de la memoria caché ARP en un router es de cuatro horas. El tiempo de vencimiento predeterminado de la entrada de la memoria direccionable por contenido (CAM) del switch es de 5 minutos. El tiempo de envejecimiento ARP de las estaciones de trabajo host no es significativo para esta discusión. pero, el ejemplo establece el tiempo de envejecimiento ARP en cuatro horas.

Este diagrama ilustra este tema. Este ejemplo de topología incluye un Catalyst 6500 con tarjetas de función del switch multicapa (MSFC) en cada switch. Aunque este ejemplo utiliza MSFC, puede utilizar cualquier otro router en lugar de MSFC. Los routers que puede utilizar son, por ejemplo, el Módulo de switch de ruta (RSM), Router de switch Gigabit (GSR) o Cisco 7500. Los hosts están conectados de forma directa a los puertos del switch. Los switches están interconectados a través de un tronco que lleva el tráfico para redes VLAN 1 y VLAN 2.



Los resultados siguientes son fragmentos de la configuración del comando show standby de cada 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: En MSFC1, la VLAN 1 está en el estado activo de HSRP y la VLAN 2 está en el estado de espera de HSRP. En MSFC2, VLAN 2 está en el estado de HSRP activo, y VLAN 1, en el estado de HSRP en espera. El gateway predeterminado de cada host es la respectiva dirección IP en espera.

1. Inicialmente, todas las memorias caché están vacías. El host A utiliza MSFC1 como puerta de enlace predeterminada. El host B utiliza MSFC2.

Tablas ARP y de direcciones MAC antes de iniciar ping

Tabla ARP del	Tabla de direcciones MAC del switch 1- Puerto	Tabla ARP	Tabla ARP	Tabla de direcciones MAC del switch 2- Puerto	Tabla ARP del
---------------	---	-----------	-----------	---	---------------

host A	VLAN de MAC	MSFC1	MSFC2	VLAN de MAC	host B
	0003.6bf1.2a01 1 15/1			0003.6bf1.2a02 1 15/1	
	0003.6bf1.2a01 2 15/1			0003.6bf1.2a02 2 15/1	
	0000.0c07.ac01 1 15/1			0000.0c07.ac01 1 1/1	
	0000.0c07.ac02 2 1/1			0000.0c07.ac02 2 15/1	
	0003.6bf1.2a02 1 1/1			0003.6bf1.2a01 1 1/1	
	0003.6bf1.2a02 2 1/1			0003.6bf1.2a01 2 1/1	

 Nota: Para mayor brevedad, la dirección MAC del switch 1 para el router HSRP y la dirección MAC no se incluyen en las otras tablas que aparecen en esta sección.

2. El host A hace ping al host B, lo que significa que el host A envía un paquete de eco ICMP. Debido a que cada host reside en una VLAN independiente, el host A reenvía sus paquetes destinados al host B a su gateway predeterminada. Para que ocurra ese proceso, el host A debe enviar un ARP para resolver la dirección MAC de su gateway predeterminada, 10.1.1.1.

Tablas de direcciones ARP y MAC luego de que el host A envía un ARP para la puerta de enlace predeterminada

Tabla ARP del host A	Tabla de direcciones MAC del switch 1- Puerto VLAN de MAC	Tabla ARP MSFC1	Tabla ARP MSFC2	Tabla de direcciones MAC del switch 2- Puerto VLAN de MAC	Tabla ARP del host B
10.1.1.1: 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001			

3. MSFC1 recibe el paquete, lo reescribe y lo reenvía al host B. Para reescribir el paquete, MSFC1 envía una solicitud ARP para el host B porque el host reside en una interfaz conectada directamente. MSFC2 aún debe recibir los paquetes en este flujo. Cuando MSFC1 recibe la respuesta ARP del host B, ambos switches aprenden el puerto de origen asociado al host B.

Tablas ARP y de direcciones MAC luego de que el host A envía un paquete a la gateway predeterminada y MSFC1 envía ARP al host B

Tabla ARP del host A	Tabla de direcciones MAC del switch 1- Puerto VLAN de MAC	Tabla ARP MSFC1	Tabla ARP MSFC2	Tabla de direcciones MAC del switch 2- Puerto VLAN de MAC	Tabla ARP del host B
10.1.1.1: 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001		0000.0c00.0002 2 2/1	10.1.2.2: 0003.6bf1.2a01
	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0002			

4. El host B recibe el paquete de eco del host A, a través de MSFC1. El host B ahora debe enviar una respuesta de eco al host A. Dado que el host A reside en una VLAN diferente, el host B reenvía la respuesta a través de su puerta de enlace predeterminada, MSFC2. Para poder reenviar el paquete por medio de MSFC2, el host B debe enviar un ARP para su dirección IP de puerta de enlace predeterminada, 10.1.2.1.

Tablas de direcciones ARP y MAC luego de que el host A envía un ARP para la puerta de enlace predeterminada

Tabla ARP del host A	Tabla de direcciones MAC del switch 1- Puerto VLAN de MAC	Tabla ARP MSFC1	Tabla ARP MSFC2	Tabla de direcciones MAC del switch 2- Puerto VLAN de MAC	Tabla ARP del host B
10.1.1.1: 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 (0003.6bf1.2a01)
	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0001			10.1.2.1 (0000.0c07.ac02)

5. El host B ahora reenvía el paquete de respuesta de eco a MSFC2. MSFC2 envía una solicitud ARP para el host A porque está conectado directamente en la VLAN 1. El switch 2 completa su tabla de direcciones MAC con la dirección MAC del host B.

Tablas de ARP y direcciones MAC luego de que el host A recibe el paquete de eco

Tabla ARP del host A	Tabla de direcciones MAC del switch 1- Puerto VLAN de MAC	Tabla ARP MSFC1	Tabla ARP MSFC2	Tabla de direcciones MAC del switch 2- Puerto VLAN de MAC	Tabla ARP del host B
10.1.1.1: 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 (0003.6bf1.2a00)
10.1.1.3: 0003.6bf1.2a0	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001	0000.0c00.00001 1 1/1	10.1.2.1 (0000.0c07.ac00)

6. La respuesta de eco llega al host A y el flujo está completo.

Consecuencias del enrutamiento asimétrico

Considere el caso de un ping continuo al host B por parte del host A. Recuerde que el host A envía el paquete de eco a MSFC1 y que el host B envía la respuesta de eco a MSFC2, lo cual es un estado de enrutamiento asimétrico. El único momento en que el switch 1 obtendrá la MAC de origen del host B será cuando el host B conteste el pedido ARP del MSFC1. Esto se debe a que el host B utiliza MSFC2 como puerta de enlace predeterminada y no envía paquetes a MSFC1 y, por lo tanto, al switch 1. Dado que el tiempo de espera de ARP es de cuatro horas de manera predeterminada, el switch 1 desactualiza la dirección MAC del host B después de cinco minutos de manera predeterminada. El Switch 2 envejece el host A después de cinco minutos. Como consecuencia, el switch 1 debe tratar cualquier paquete con una MAC de destino del host B como

una unidifusión desconocida. El switch inunda todos los puertos con el paquete que llega del host A con destino al host B. Además, puesto que no hay una entrada de dirección MAC del host B en el switch 1, tampoco hay una entrada MLS.

Tablas ARP y de direcciones MAC luego de transcurridos 5 minutos de que el host A realice ping continuos del host B

Tabla ARP del host A	Tabla de direcciones MAC del switch 1- Puerto VLAN de MAC	Tabla ARP MSFC1	Tabla ARP MSFC2	Tabla de direcciones MAC del switch 2- Puerto VLAN de MAC	Tabla ARP del host B
10.1.1.1: 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2: 0003.6bf1.2a01
10.1.1.3: 0003.6bf1.2a0		10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001		10.1.2.1: 0000.0c07.ac01

Los paquetes de respuesta de eco que provienen del host B experimentan el mismo problema después de que la entrada de dirección MAC para el host A caduque en el switch 2. El host B reenvía la respuesta de eco a MSFC2, que a su vez rutea el paquete y lo envía a la VLAN 1. El switch no tiene un host de entrada A en la tabla de direcciones MAC y debe saturar el paquete por todos los puertos en la VLAN 1.

Los problemas de enrutamiento asimétrico no interrumpen la conectividad. Sin embargo, el enrutamiento asimétrico puede causar un flujo excesivo de unidifusión y la falta de entradas MLS. Hay tres cambios de configuración que pueden remediar esta situación:

- Ajuste del plazo de vencimiento de las direcciones MAC en los respectivos conmutadores en 14.400 segundos (cuatro horas) o más.
- Cambie el tiempo de espera de ARP en los routers a 5 minutos (300 segundos).
- Cambie el plazo de vencimiento de las direcciones MAC y el tiempo de espera de ARP al mismo valor de tiempo de espera.

El método preferible es cambiar el plazo de vencimiento de las MAC a 14.400 segundos. A continuación, se enumeran las pautas para la configuración:

- Software Cisco IOS:

```
mac address-table aging-time <seconds> vlan <vlan_id>
```

Caso práctico #6: La dirección IP virtual de HSRP se informa como una dirección IP diferente

El mensaje de error STANDBY-3-DIFFVIP1 se genera cuando hay una pérdida en la InterVLAN debido a la presencia de bucles de conexión en puente en el switch.

Si aparece este mensaje de error y hay una pérdida en la InterVLAN debido a bucles de conexión en puente en el switch, siga estos pasos para resolver el error:

1. Identifique la trayectoria que toman los paquetes entre los nodos extremos.

Si hay un router en este trayecto, siga los pasos siguientes:

- a. Solucione los problemas del trayecto desde el primer switch hasta el router.
- b. Solucione los problemas del trayecto desde el router al segundo switch.

2. Conéctese a cada uno de los switches del trayecto y compruebe el estado de los puertos que se utilizan en el trayecto entre los nodos extremos.

Caso práctico #7: HSRP provoca una violación de MAC en un puerto seguro

Cuando se configura la seguridad de puertos en los puertos de switch que están conectados a los routers habilitados para HSRP, se produce una violación de MAC, ya que no se puede tener la misma dirección MAC segura en más de una interfaz. La violación a la seguridad ocurre en un puerto seguro en una de estas situaciones:

- Se agrega la cantidad máxima de direcciones MAC seguras en la tabla de direcciones, y una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz.
- Una dirección obtenida o configurada en una interfaz segura se ve en otra interfaz segura en la misma VLAN.

De manera predeterminada, una violación de seguridad de puerto hace que la interfaz de switch se deshabilite y se desactive inmediatamente, lo que bloquea los mensajes de estado de HSRP entre los routers.

Solución Alternativa

- Ejecute el comando `standby use-BIA` en los routers. Esto obliga a los routers a utilizar una dirección grabada para HSRP en lugar de la dirección MAC virtual.
- Deshabilite la seguridad de puertos en los puertos de switch que se conectan a los routers habilitados para HSRP.

Caso práctico #9: %Interface Hardware no admite varios grupos

Si se crean varios grupos de HSRP en la interfaz, se recibe este mensaje de error:

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

Este mensaje de error se recibe debido a la limitación de hardware en algunos routers o switches.

No es posible superar la limitación mediante ningún método de software. El problema es que cada grupo de HSRP utiliza una dirección MAC adicional en la interfaz, por lo que el chip MAC de Ethernet debe admitir varias direcciones MAC programables para habilitar varios grupos de HSRP.

La solución alternativa es utilizar el comando de configuración de la interfaz `standby use-bia`, que utiliza la dirección grabada (BIA) de la interfaz como su dirección MAC virtual, en lugar de la dirección MAC preasignada.

Resolución de Problemas de HSRP en Switches Catalyst

A. Verificar la configuración del router HSRP

1. Verifique la dirección IP de la interfaz única del router

Verifique que cada router HSRP tiene una dirección IP única para cada subred en base a la interfaz. Además, verifique que cada interfaz tenga el protocolo de línea `up`. Para verificar con rapidez el estado actual de cada interfaz, ejecute el comando `show ip interface brief`. Aquí tiene un ejemplo:

```
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. Verifique las direcciones IP y los números de grupo en espera (HSRP)

Verifique que las direcciones IP en espera (HSRP) configuradas y que los números del grupo en espera coinciden con cada router que participa en HSRP. Una discrepancia de los grupos en espera o de las direcciones HSRP en espera puede provocar problemas de HSRP. El comando `show standby` detalla la configuración del grupo en espera y la dirección IP en espera de cada interfaz. Aquí tiene un ejemplo:

```
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-V110-110" (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-V111-111" (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-V110-110" (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-V111-111" (default)
FLAGS: 0/1
```

3. Compruebe que la dirección IP en espera (HSRP) es diferente para cada interfaz

Verifique que la dirección IP (HSRP) en espera sea una sola desde la dirección IP configurada de cada interfaz. El comando show standby es una referencia rápida para ver esta información. Aquí tiene un ejemplo:

```
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-V110-110" (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-V111-111" (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-V110-110" (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-V111-111" (default)
FLAGS: 0/1
```

4. Cuándo Utilizar el Comando standby use-bia

Salvo que HSRP esté configurado en una interfaz Token Ring, solo utilice el comando standby use-bia en circunstancias excepcionales. Este comando indica al router que debe utilizar su BIA en lugar de la dirección MAC virtual HSRP para el grupo HSRP. En una red Token Ring, si se usa el Puente de enrutamiento fuente (SRB), el comando standby use-bia le permite al router activo nuevo actualizar el caché del Campo de información de enrutamiento (RIF) del host con un ARP gratuito. Sin embargo, no todas las implementaciones de host administran el ARP gratuito de manera correcta. Otra advertencia que debe tenerse en cuenta en el comando standby use-bia involucra al proxy ARP. Un router en reserva no puede suplir la pérdida de la base de datos ARP de representación del router activo fallido.

5. Verificar la configuración de la lista de acceso

Verifique que las listas de acceso configuradas en todos los pares HSRP no filtran las direcciones HSRP configuradas en sus interfaces. En concreto, verifique la dirección de multidifusión que se utiliza para enviar tráfico a todos los routers de una subred (224.0.0.2). Asimismo, verifique que el tráfico UDP destinado al puerto HSRP 1985 no esté filtrado. HSRP utiliza esta dirección y puerto para enviar paquetes de saludo entre los pares. Ejecute el comando show access-lists para obtener una referencia rápida sobre las listas de acceso configuradas en el router. Aquí tiene un ejemplo:

```
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. Verificar la Configuración de Catalyst Fast EtherChannel y Trunking

1. Verifique la configuración de troncal

Si se utiliza una conexión troncal para conectar los routers HSRP, verifique las configuraciones de

la conexión troncal en los routers y switches. Existen cinco modos de conexión troncal posibles:

- encendido
- deseable
- Auto
- desactivado
- ausencia de negociación

Verifique que los modos de la conexión troncal configurados proporcionan el método de conexión troncal deseado.

Utilice la configuración recomendada para las conexiones entre switches al momento de resolver problemas del HSRP. Esta configuración puede aislar los problemas de los puertos de los switches para establecer conexiones troncales de forma correcta. Establezca una configuración de router a switch de no negociación, ya que la mayoría de los routers de Cisco IOS no soportan la negociación de la conexión troncal.

Para el modo de trunking IEEE 802.1Q (dot1q), verifique que ambos lados del trunk estén configurados para utilizar la misma VLAN nativa y encapsulación. Dado que, de manera predeterminada, los productos de Cisco no etiquetan la VLAN nativa, una discrepancia de configuraciones de VLAN nativas producirá la falta de conectividad en las VLAN no coincidentes. Por último, verifique que la conexión troncal esté configurada para transportar las VLAN configuradas en el router y que las VLAN no están recortadas en el estado STP para puertos conectados al router. Ejecute el comando `show interfaces <interface> trunk` para obtener una referencia rápida que muestre esta información. Aquí tiene un ejemplo:

```
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
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
```

2. Verifique la configuración de Fast EtherChannel (Port Channel)

Si se utiliza un canal de puerto para conectar los routers HSRP, verifique la configuración EtherChannel en ambos routers y switches. Configure un canal de puerto de switch a switch en modo deseable en un lado, como mínimo. El otro lado puede estar en uno de estos modos:

- encendido
- deseable
- Auto

Sin embargo, en este ejemplo las interfaces no son miembros de un canal de puerto:

```
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. Investigue la tabla de reenvío de direcciones MAC del switch

Verifique que existan las entradas de la tabla de direcciones MAC del switch para los routers HSRP para la dirección MAC virtual HSRP y las BIA físicas. El comando show standby del router proporciona la dirección MAC virtual. El comando show interface proporciona la BIA física. A continuación, se muestran algunos resultados de muestra:

```
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-V110-110" (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-V111-111" (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

```

Asegúrese de verificar el plazo de vencimiento de la CAM a fin de determinar la rapidez en que vencen las entradas. Si el plazo es igual que el valor configurado para el retardo de reenvío STP, que es 15 segundos de forma predeterminada, hay una gran probabilidad de que exista un bucle STP en la red. Esta es una salida del comando de ejemplo:

```

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. Verifique la conectividad de la capa física

Si más de un router en un grupo HSRP pasa a estar activo, implica que esos routers no están recibiendo los paquetes de saludo de los pares HSRP de forma consistente. Los problemas de la capa física pueden impedir que el tráfico pase entre los pares de forma consistente y provocar esta situación. Asegúrese de verificar la conectividad física y la conectividad IP entre los pares HSRP al solucionar problemas de HSRP. Ejecute el comando show standby para verificar la conectividad. Aquí tiene un ejemplo:

```

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-V110-110" (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-V111-111" (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-V110-110" (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-V111-111" (default)
FLAGS: 0/1
```

1. Compruebe el estado de la interfaz

Verifique las interfaces. Verifique que todas las interfases HSRP configuradas estén up/up (activo/activo), como se muestra en este ejemplo:


```
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

Si alguna de las interfaces está, desde el punto de vista administrativo, down/down (inactivo/inactivo), ingrese al modo configuración en el router y ejecute el comando específico de la interfaz no shutdown . Aquí tiene un ejemplo:

```
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

Si cualquiera de las interfaces está down/down (inactivo/inactivo) o up/down (activo/inactivo), revise el registro para consultar cualquier notificación de cambio de interfaz. Para los switches basados en el software Cisco IOS, estos mensajes aparecen en situaciones de enlace activo/inactivo:

```
%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
```

Inspeccione los puertos, cables, transceptores y otros dispositivos que estén entre los pares HSRP. ¿Alguien ha eliminado o aflojado alguna conexión? ¿Hay alguna interfaz que pierda un enlace repetidamente? ¿Se han utilizado los tipos de cables adecuados? Verifique que no hay errores en la interfaz, tal como muestra este ejemplo:

```
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. Errores de cambio de link y de puerto

Verifique las modificaciones de los links de los puertos del switch y otros errores. Ejecute los siguientes comandos y revise el resultado:

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

Estos comandos le ayudarán a determinar si existe un problema de conectividad entre los switches y otros dispositivos.

Estos mensajes son normales en situaciones de enlace up/down (activo/inactivo):

```
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

Ejecute el comando `show interfaces <interface> status` para determinar el estado general de un puerto. Aquí tiene un ejemplo:

```
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

¿El estado de la interfaz es conectado, no conectado o errdisable? Si el estado es notconnect, verifique que el cable esté conectado en ambos lados. Compruebe que se ha utilizado el cable adecuado. Si el estado es errdisable, revise los contadores de errores excesivos. Consulte [Recuperación del Estado de Puerto Errdisable en Plataformas Cisco IOS](#) para obtener más información.

¿Para qué VLAN está configurado este puerto? Asegúrese de que el otro lado de la conexión está

configurado para la misma VLAN. Si se ha configurado el enlace para que sea troncal, asegúrese de que los dos lados del enlace troncal tienen las mismas VLAN.

¿Cuál es la configuración de la velocidad y de dúplex? Si la configuración está precedida por a-, el puerto está configurado para que negocie de manera automática la velocidad y el dúplex. De lo contrario, el administrador de red ha predeterminado esta configuración. Para configurar la velocidad y el dúplex de un enlace, las configuraciones en ambos lados del enlace deben coincidir. Si un puerto del switch está configurado para la negociación automática, el otro lado del enlace también debe estar configurado para la negociación automática. Si un lado está codificado por software en una velocidad y dúplex determinados, el otro lado también debe estar codificado por software. El proceso de negociación automática queda interrumpido, si un lado ha sido configurado para negociar automáticamente pero el otro está fijado a mano.

<#root>

```
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
```

¿Existen muchos errores de alineación, errores FCS o fragmentos diminutos? Estos indican una discrepancia de dúplex o velocidad entre el puerto y el dispositivo de conexión. Cambie la configuración de la velocidad y dúplex de ese puerto para ayudar a corregir estos errores.

Ejecute el comando show mac para verificar que el puerto pasa tráfico. Las columnas In y Out indican el número de paquetes de unidifusión, multidifusión y difusión que se reciben y transmiten en un puerto determinado. Los contadores inferiores revelan la cantidad de paquetes que fueron descartados o perdidos y si eran parte del tráfico entrante o saliente. Lrn-Discrd, In-Lost y Out-Lost cuentan la cantidad de paquetes enviados o descartados erróneamente debido a búfers insuficientes.

```
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. Verifique la conectividad IP

Verifique la conectividad IP. Emita un ping IP desde el router asociado al dispositivo HSRP remoto. Esto ayuda a observar las pérdidas momentáneas de conectividad. El ping extendido sólo

la conectividad.

4. Compruebe si hay un link unidireccional

Compruebe si el switch presenta un enlace unidireccional entre los pares HSRP. Un enlace unidireccional se produce cada vez que el vecino recibe el tráfico que transmite el dispositivo local mediante un enlace, pero el dispositivo local no recibe el tráfico que transmite el vecino. Esta función se conoce como modo agresivo de Detección de enlace unidireccional (UDLD). El uso de UDLD únicamente es posible si los dos lados de la conexión soportan la función. El modo agresivo UDLD funciona en la L2 para determinar si un enlace está correctamente conectado y si el tráfico fluye en ambas direcciones entre los vecinos correctos. A continuación, se muestran los resultados de los comandos de muestra:

 Nota: Vaya al siguiente enlace para [Comprender y Configurar la Función UDLD](#). Depende de la plataforma que se utilice.

Otra opción que puede ayudar a verificar un link unidireccional si el UDLD no está disponible es con el uso de Cisco Discovery Protocol (CDP). La habilitación de CDP es otra manera de detectar si existe un enlace unidireccional. Si sólo un lado de un enlace puede ver su dispositivo vecino, reemplace el cable entre los dispositivos y verifique que no haya interfaces defectuosas.

```
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. Referencias adicionales de resolución de problemas de capa física

Consulte los siguientes documentos:

- [Configuración y resolución de problemas de negociación automática de half/full duplex para Ethernet 10/100/1000 Mb](#)
- [Recuperar el estado de puerto errDisable en plataformas Cisco IOS](#)
- [Troubleshooting de Problemas de Compatibilidad entre Cisco Catalyst Switches y NIC](#)
- Sección [Understanding Data Link Errors \(Comprender errores en el enlace de datos\)](#) de [Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues \(Resolución de problemas de compatibilidad entre los switches Catalyst de Cisco y NIC\)](#)
- [Solución de problemas del puerto del switch y de la interfaz](#)

D. Depuración de HSRP de capa 3

Si los cambios de estado de HSRP son frecuentes, utilice los comandos debug de HSRP (en modo de habilitación) en el router para observar la actividad de HSRP. Esta información le ayudará a determinar qué paquetes HSRP recibe y envía el router. Reúna esta información si crea una solicitud de servicio en el soporte técnico de Cisco. El resultado de la depuración también muestra información sobre el estado de HSRP junto con las cuentas detalladas de los paquetes de saludo de HSRP.

1. Depuración HSRP estándar

En Cisco IOS, habilite la capacidad de depuración HSRP con el comando debug standby. Esta información es útil cuando los problemas son intermitentes y sólo afectan a unas pocas interfaces. La depuración le permite determinar si el router HSRP en cuestión recibe y transmite paquetes de saludo HSRP en intervalos específicos. Si el router no recibe los paquetes de saludo, se puede deducir que o bien el par no transmite los paquetes de saludo o bien la red los descarta.

Comando	Propósito
debug standby	Habilita la depuración HSRP

Esta es una salida del comando de ejemplo:

```
Router_1#debug standby
HSRP debugging is on
Jul 29 16:12:16.889: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
```

```

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

```

2. Depuración HSRP condicional (limitación de la salida basada en el grupo en espera y/o VLAN)

La versión 12.0(3) del software Cisco IOS implementó una condición de depuración para permitir que el resultado del comando `debug standby` se filtrara en función de la interfaz y del número de grupo. El comando utiliza el paradigma de la condición de depuración que se implementó en la versión 12.0 del software Cisco IOS.

Comando	Propósito
<code>debug condition standby <interface> <group></code>	Habilita la depuración condicional HSRP del grupo (0-255)

La interfaz debe ser una interfaz válida capaz de soportar HSRP. El grupo puede ser cualquiera, de 0 a 255. Se puede configurar una condición de depuración para grupos que no existen. Esto permite que se capturen las depuraciones durante la inicialización de un grupo nuevo. Debe habilitar la depuración en espera para generar resultados de depuración. Si no existen condiciones de depuración en espera, se generará el resultado de la depuración para todos los grupos en todas las interfaces. Si existe por lo menos una condición de depuración en espera, el resultado de la depuración en espera se filtra de acuerdo con todas las condiciones de depuración en espera. Esta es una salida del comando de ejemplo:

```

Router_1#debug condition standby v1an 10 110
Condition 1 set
Router_1#
Jul 29 16:16:20.284: V110 HSRP110 Debug: Condition 1, hsrp V110 HSRP110 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
Jul 29 16:16:44.797: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:45.381: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:16:47.231: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:48.248: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100

```

3. Depuración HSRP mejorada

La versión 12.1(1) del software Cisco IOS agregó la depuración HSRP mejorada. Para ayudar a encontrar información útil, la depuración HSRP mejorada limita el ruido de los mensajes de saludo periódicos e incluye información de estado adicional. Esta información resulta particularmente útil si trabaja con un ingeniero del soporte técnico de Cisco al crear una solicitud de servicio.

Comando	Propósito
---------	-----------

debug standby	Muestra todos los errores, eventos y paquetes HSRP
depurar errores standby	Muestra los errores HSRP
debug standby events [[all] [hsrp redundancia track]] [detail]	Muestra los eventos HSRP
debug standby packets [[all terse] [advertise coup Saludo resign]] [detail]	Muestra los paquetes HSRP
debug standby terse	Mostrar un rango limitado de errores, eventos y paquetes HSRP

Esta es una salida del comando de ejemplo:

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

Puede utilizar la depuración condicional del grupo HSRP y/o de interfaz para filtrar el resultado de la depuración.

Comando	Propósito
debug condition interface interface	Habilita la depuración condicional de la interfaz
debug condition standby <interface> <group>	Habilita la depuración condicional de HSRP

En este ejemplo, el router se une a un grupo HSRP preexistente.

```
Router_2#debug condition standby vlan 10 110
Condition 1 set
Router_2#debug condition interface gigabitEthernet 1/0/1 vlan-id 10
Condition 2 set
```

```

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

```

E. Solución de problemas de árbol de expansión

Las condiciones de bucle STP o la inestabilidad en una red pueden impedir una comunicación adecuada de los pares HSRP. Debido a esta comunicación inadecuada, cada par se convierte en un router activo. Los bucles STP pueden provocar tormentas de difusión, tramas duplicadas e inconsistencia en la tabla MAC. Todos estos problemas afectan a toda la red y, en especial, a HSRP. Los mensajes de error HSRP pueden ser la primera indicación de un problema con STP.

Cuando solucione los problemas de STP, debe entender la topología STP de la red en cada

VLAN. Debe determinar qué switch es el bridge raíz y qué puertos del switch están bloqueando y reenviando. Dado que cada VLAN tiene su propia topología STP, esta información resulta muy importante a nivel VLAN.


1. Verifique la configuración del árbol de expansión

Asegúrese de que STP está configurado en todos los switches y dispositivos de conexión en bridge de la red. Tome nota de dónde cada switch cree que se ubica el bridge raíz. Asimismo, anote los valores de los siguientes temporizadores:

- duración máxima de la root
- Tiempo de Hello
- demora de reenvío

Ejecute el comando `show spanning-tree` para ver toda esta información. De forma predeterminada, el comando muestra esta información para todas las VLAN. Sin embargo, también puede filtrar otra información de VLAN si proporciona el número de VLAN con el comando. Esta información resulta muy útil al solucionar problemas de STP.

Estos tres temporizadores que se anotan en el resultado `show spanning-tree` se aprenden del puente raíz. Estos temporizadores no deben coincidir con los temporizadores configurados en ese bridge específico. Sin embargo, asegúrese de que los temporizadores coinciden con el puente de ruta en caso de que el switch se convierta en el puente de ruta en algún momento. Esta coincidencia de los temporizadores con el bridge raíz ayuda a mantener la continuidad y facilidad de administración. Asimismo, esta coincidencia impide que un switch con temporizadores incorrectos paralice la red.

 Nota: Habilite STP para todas las VLAN en todo momento, independientemente de si hay links redundantes en la red. Si habilita STP en redes no redundantes, se evitan pérdidas. Una pérdida puede producirse si alguien conecta en bridge switches con concentradores u otros switches y accidentalmente crea un bucle físico. STP también es muy útil para aislar problemas específicos. Si la habilitación de STP afecta al funcionamiento de la red, podría existir un problema que debe aislarse.

A continuación se muestra un ejemplo de salida 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

El switch L2Switch_1 es la raíz de VLAN 10 y VLAN 11.


2. Condiciones del loop del árbol de expansión

Para que tenga lugar un bucle STP, debe haber redundancia física L2 en la red. Un STP no tiene lugar si no existe la posibilidad de que haya una condición de bucle físico. Los síntomas de una condición de bucle STP son los siguientes:

- Interrupción total de la red
- Pérdida de conectividad
- La notificación por parte de los equipos de la red de la alta utilización del sistema y de los

procesos

Una sola VLAN que experimente una condición de bucle STP puede congestionar un enlace y privar del ancho de banda a las demás VLAN. El comando `show interfaces <interface> controller` indica qué puertos transmiten o reciben un número excesivo de paquetes. Una difusión y multidifusión excesiva puede indicar puertos que son parte de un bucle STP. Como regla general, sospeche que existe un enlace con una condición de bucle STP siempre que la multidifusión o difusión sobrepase la cantidad de paquetes de unidifusión.

 Nota: El switch también cuenta las unidades de datos de protocolo de puente STP (BPDU) que se reciben y transmiten como tramas multicast. Aun así, un puerto que está en el estado de bloqueo STP sigue transmitiendo y recibiendo BPDU de 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 msec AGO

3. Notificación de cambio de topología

Otro comando que es vital para el diagnóstico de los problemas de STP es el comando `show spanning-tree detail`. Este comando sigue los mensajes de la Notificación de cambio de topología

(TCN) hacia su originador. Estos mensajes, enviados como BPDU especiales entre switches, indican que ha habido un cambio de topología en un switch. Ese switch envía un TCN fuera de su puerto raíz. La TCN se mueve de forma ascendente hacia el bridge raíz. El puente de ruta envía otra BPDU especial, un Reconocimiento de cambio de topología (TCA), a todos sus puertos. El bridge raíz establece el bit TCN en la BPDU de configuración. Como consecuencia, todos los bridges que no son raíz establecen su temporizador de vencimiento de la tabla de direcciones MAC de acuerdo con el retardo de reenvío del STP de configuración.

Para aislar este problema, acceda al bridge raíz para cada VLAN y ejecute el comando `show spanning-tree <interface> detail` para los puertos conectados al switch. La entrada `última modificación realizada` indica la hora en que se recibió el último TCN. En esta situación, no tiene tiempo de observar quién emitió las TCN que han podido ser las causas del posible bucle. La entrada `Number of topology changes` le da una idea sobre el número de TCN que ocurren. Durante un bucle STP, este contador puede incrementarse cada minuto. Consulte la sección [Spanning Tree Protocol Problems and Related Design Considerations \(Problemas en el protocolo de árbol de expansión y consideraciones de diseño\)](#) para obtener más información.

Otra información útil incluye:

- Puerto de la última TCN
- Hora de la última TCN
- Conteo de TCN actual

Esta es una salida del comando de ejemplo:

```
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

Este resultado muestra que el último cambio de topología se produjo desde el dispositivo conectado fuera de la interfaz GigabitEthernet1/0/35. A continuación, ejecute el mismo comando `show spanning-tree detail` desde este dispositivo para intentar rastrear el problema. Si este switch que genera las TCNs sólo está conectado a PC o terminales, asegúrese de que STP PortFast esté habilitado en estos puertos. STP PortFast elimina las TCN STP cuando un puerto cambia de estados.

Consulte los documentos siguientes para obtener más información sobre STP y cómo solucionar los problemas de las transiciones de enlaces asociadas a las tarjetas de interfaz de red (NIC):

- [Uso de Portfast y otros comandos para solucionar retrasos al iniciar la conectividad de la estación de trabajo](#)
- [Explicación del Protocolo de árbol de expansión rápida \(802.1w\)](#)
- [Problemas con STP y consideraciones de diseño relacionadas](#)

4. Puertos bloqueados desconectados

Debido a la naturaleza del balance de cargas de Fast EtherChannel (FEC, canalización de puerto), los problemas de FEC pueden contribuir a los problemas de HSRP y STP. Al resolver problemas de STP o HSRP, puede eliminar la configuración de cualquier conexión FEC. Una vez que los cambios de configuración estén en su lugar, ejecute el comando `show spanning-tree blockedports` en ambos switches. Asegúrese de que, como mínimo, uno de los puertos empieza el bloqueo en uno de los lados de la conexión.

Consulte los siguientes documentos para obtener más información sobre Fast EtherChannel:

- [Comprensión del Equilibrio de Carga y Redundancia de EtherChannel en Switches Catalyst](#)
- [Configuración de EtherChannels](#)

5. Supresión de la difusión

Habilite la supresión de la difusión para ayudar a reducir el impacto de una tormenta de difusión. Una tormenta de difusión es uno de los efectos secundarios principales de un bucle STP. Esta es una salida del comando de ejemplo:

```
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. Acceso Telnet y de consola

El tráfico de la consola o de Telnet al switch a veces se ralentiza demasiado como para localizar adecuadamente un dispositivo problemático durante un bucle de STP. Para forzar una recuperación instantánea de la red, elimine todos los enlaces físicos redundantes. Después de permitir que STP vuelva a converger en la nueva topología no redundante, vuelva a conectar un enlace redundante a la vez. Si el bucle STP regresa después de agregar un segmento determinado, significa que ha identificado los dispositivos problemáticos.

7. Funciones del árbol de expansión: Portfast, UplinkFast y BackboneFast

Verifique que PortFast, UplinkFast y BackboneFast están configurados adecuadamente. Al solucionar los problemas de STP, inhabilite todos los STP avanzados (UplinkFast y BackboneFast). Además, verifique que STP PortFast sólo está habilitado en puertos conectados directamente a los host sin conexión en bridge. Los host sin conexión en bridge incluyen estaciones de trabajo de usuario y routers sin grupos de bridge. No habilite PortFast en los puertos conectados a concentradores u otros switches. Estos son algunos documentos para ayudar a comprender y configurar estas funciones:

[Configuración de Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast y Loop Guard](#)

8. Protección BPDU

Cuando habilita la protección PortFast BPDU, un puerto no troncal habilitado para PortFast cambia a estado errdisable en el momento en que se recibe una BPDU en ese puerto. Esta función le ayuda a encontrar puertos configurados incorrectamente para PortFast. La función también detecta dónde los dispositivos reflejan los paquetes o inyectan las BPDU STP en la red. Cuando resuelve problemas de STP, puede habilitar esta función para ayudar a aislar el problema de 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. Poda VTP

Cuando la eliminación de VTP está habilitada en la red, puede hacer que los dispositivos de un grupo de HSRP se activen. Esto da como resultado conflictos de IP entre las puertas de enlace y causa problemas de tráfico. Asegúrese de que la VLAN de cualquier grupo de HSRP no sea eliminada por VTP en la red.

F. Dividir y conquistar

Si todos los demás intentos para aislar o resolver los problemas de HSRP no tienen éxito, el método "dividir y vencer" es el siguiente enfoque. Este método ayuda a aislar la red y los componentes que forman la red. Dividir y vencer incluye cada una de las pautas de esta lista:




Nota: Esta lista repite algunas pautas de otras secciones de este documento.

- Cree una VLAN de prueba para conectar HSRP y la VLAN aislada a routers HSRP.
- Desconecte todos los puertos redundantes.
- Divida los puertos FEC en puertos de conexión única.
- Reduzca los miembros del grupo HSRP a sólo dos miembros.
- Recorte los puertos troncales de modo que sólo las VLAN necesarias se propaguen a través de dichos puertos.
- Desconecte los switches conectados a la red hasta que los problemas desaparezcan.

Problemas conocidos

Inestabilidad/inestabilidad del estado de HSRP al utilizar Cisco 2620/2621, Cisco 3600 con Fast Ethernet

Este problema puede tener lugar con interfaces Fast Ethernet al interrumpir la conectividad de la red o agregar un router HSRP con una prioridad superior en una red. Cuando el estado de HSRP cambia de activo a hablar, el router reinicia la interfaz con el propósito de eliminar la dirección MAC HSRP del filtro de direcciones MAC de interfaces. Únicamente el hardware específico que se utiliza en las interfaces Fast Ethernet para Cisco 2600s, 3600s y 7500s presenta este problema. El reinicio de la interfaz del router provoca que el estado de un enlace cambie en las interfaces Fast Ethernet y que el switch detecte el cambio. Si el switch ejecuta STP, el cambio provoca una transición de STP. El STP tarda 30 segundos en cambiar el puerto al estado de reenvío. Este tiempo es el doble del plazo de retardo de reenvío predeterminado de 15 segundos. Al mismo tiempo, el router en estado de hablar pasa al estado en espera después de 10 segundos, que es el tiempo en espera de HSRP. STP todavía no está en estado de reenvío, por lo que no se reciben mensajes de saludo HSRP desde el router activo. Como consecuencia, el router en espera se convierte en el activo transcurridos unos 10 segundos. Ambos routers ahora están activos. Cuando los puertos STP se ponen en estado de reenvío, el router de menor prioridad cambia de activo a hablar y todo el proceso se repite.

Platform	Descripción	ID de falla de funcionamiento de Cisco	Corregir	Solución Alternativa
Cisco 2620/2621	La interfaz Fast Ethernet comienza a inestabilizarse cuando HSRP está configurado y el cable está desconectado.		Una actualización de software; consulte el bug para obtener detalles de la revisión.	Habilita el árbol de expansión PortFast en el puerto del switch conectado.
Cisco 2620/2621	Estado de HSRP inestable en 2600 con Fast Ethernet.		Versión 12.1.3 del software Cisco IOS	Habilita el árbol de expansión PortFast en el puerto del switch conectado.
Cisco 3600 con NM-1FE-TX ¹	Estado de HSRP inestable en 2600 y 3600 Fast Ethernet.		Versión 12.1.3 del software Cisco IOS	Habilita el árbol de expansión PortFast en el puerto del switch conectado.
Cisco 4500 con interfaz Fast Ethernet	Estado de HSRP inestable en 4500 Fast Ethernet.	ID de bug de Cisco CSCds16055 	Versión 12.1.5 del software Cisco IOS	Habilita el árbol de expansión PortFast en el puerto del switch conectado.

1NM-1FE-TX = módulo de red de un puerto Fast Ethernet (interfaz 10/100BASE-TX).

Una solución alternativa es ajustar los temporizadores HSRP para que el retardo de reenvío de STP sea menos que la mitad del tiempo de espera predeterminado de HSRP. El tiempo de retardo de reenvío predeterminado de STP es de 15 segundos y el tiempo de espera HSRP predeterminado es de 10 segundos.

Cuando utiliza el comando track en el proceso HSRP, Cisco recomienda utilizar un valor de disminución determinado para evitar la intermitencia del HSRP.

Este es un ejemplo de configuración en un router activo de HSRP cuando se utiliza el 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
```

Donde 15 es el valor de disminución cuando el objeto es inestable. Para obtener más información sobre el comando track, navegue hasta el documento [Opción de seguimiento en Ejemplo de configuración de HSRPv2](#).

Información Relacionada

- [Switches Catalyst para redes LAN de campus - Acceso](#)
- [LAN Switching](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).