# Funciones y Funcionalidad de Hot Standby Router Protocol

## Contenido

# Introducción

Este documento describe las características y las funciones de Hot Standby Router Protocol (HSRP).

# prerrequisitos

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

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

## Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

# Operaciones y antecedentes de HSRP

Una forma de lograr que el tiempo de actividad de la red esté cerca del 100 % es utilizar HSRP, que ofrece redundancia de red para las redes IP, asegurando que el tráfico de usuarios se recupere de forma inmediata y transparente de los errores de primer salto en los dispositivos de borde de red o circuitos de acceso.

Al compartir una dirección IP y una dirección MAC (Capa 2), dos o más routers pueden funcionar como un solo router “virtual”. Los miembros del grupo de router virtual continuamente intercambian mensajes de estado. Esta manera, un router puede asumir la responsabilidad por el ruteo de otro, si sale de la comisión para planeado o los motivos no planificados. Los hosts continúan reenviando paquetes IP a una dirección de IP y MAC consistente y el cambio de dispositivos que realizan el ruteo es transparente.

## Mecanismos de detección dinámica de routers

Abajo están las descripciones de los mecanismos de detección dinámica de router que están disponibles para los host. Muchos de estos mecanismos no proporcionan la flexibilidad de la red requerida por los administradores de redes. Esto es porque el protocolo inicialmente no pretendía proporcionar resilencia de red o porque no es factible que cada uno de los hosts de una red ejecuten el protocolo. Además de cuál es mencionado abajo, es importante observar que muchos host permiten solamente que usted configure un gateway predeterminado.

### Protocolo de resolución de direcciones proxy

Algunos host IP utilizan el (ARP) del protocolo proxy address resolution para seleccionar a un router. Cuando un host ejecuta un proxy ARP, envía una solicitud ARP para la dirección IP del

host remoto que desea contactar. Un router, Router A, responde en la red en nombre del host remoto y proporciona su propia dirección MAC. Con proxy ARP, el host se comporta como si el host remoto estuviese conectado al mismo segmento de la red. Si el Router A falla, el host continúa enviando los paquetes destinados al host remoto a la dirección MAC del Router A, aun si estos paquetes no tienen a dónde ir y se pierden. Usted puede o esperar el ARP para adquirir la dirección MAC de otro router, el router B, en el segmento local enviando otro pedido ARP, o reinicie el host para forzarlo para enviar un pedido ARP. En ambos casos, por un periodo prolongado de tiempo, el host no puede comunicar con el host remoto, aunque ha convergido el Routing Protocol, y preparan al router B para transferir los paquetes que pasarían de otra manera a través del router A.

### Protocolo de ruteo dinámico

Algunos host IP funcionan con (o fisgón) un Dynamic Routing Protocol tal como el Routing Information Protocol (RIP) o abren la trayectoria de Shortes primero (OSPF) para descubrir al Routers. La desventaja del uso de RIP es que la adaptación a los cambios en la topología es lenta. Es posible que no sea factible ejecutar un protocolo de ruteo dinámico en todos los hosts por varias razones, entre ellas el encabezado administrativo, el encabezado de procesamiento, los asuntos de seguridad o la falta de la implementación mediante protocolo de algunas plataformas.

### Protocolo de detección del router ICMP

Algún Protocolo de descubrimiento de router ICMP (IRDP) más nuevo del uso de los host IP (RFC 1256 ) para encontrar a un nuevo router cuando una ruta llega a ser inasequible. Un host que ejecuta el IRDP está atentos hola los mensajes de multidifusión de su router configurado y utiliza a un router alterno cuando recibe no más esos mensajes Hello Messages. Los valores del temporizador predeterminados de IRDP significan que no es apto para detectar la falla del primer salto. La frecuencia de anuncio predeterminada es una vez cada 7 a 10 minutos, y la vida útil predeterminada es de 30 minutos.

### Protocolo de configuración de host dinámico

El Protocolo de configuración dinámica de host (DHCP) (RFC 1531 ) proporciona un mecanismo para pasar la información de la configuración a los host en una red TCP/IP. Cuando se inicia en la red, el host que ejecuta un DHCP cliente solicita información de configuración a un servidor DHCP. Esta información de la configuración comprende típicamente una dirección IP y un default gateway. No hay mecanismo para conmutar a un router alternativo si el default gateway falla.

## Operación de HSRP

Una clase grande de instrumentaciones de host de la herencia que no soporten la detección dinámica es capaz de configurar a un router predeterminado. Es posible que no se pueda ejecutar un protocolo de ruteo dinámico en cada host por varias razones, entre ellas el gasto administrativo, el gasto de procesamiento, las cuestiones de seguridad o la falta de la implementación de un protocolo para algunas plataformas. El HSRP proporciona los servicios de la Conmutación por falla a estos host.

Usando el HSRP, un conjunto de routers funciona en el concierto para presentar la ilusión de un solo router virtual a los host en el LAN. Esta serie se conoce como un grupo HSRP o un grupo de espera. Un solo router elegido del grupo es responsable del reenvío de los paquetes de los hosts

envían al router virtual. Este router se denomina Router activo. Se elige otro router como router en espera. En caso de que falle el router activo, el router inactivo asume las tareas de reenvío de paquetes de éste. A pesar de que un número arbitrario de routers pueden ejecutar HSRP, sólo el router Activo reenvía los paquetes enviados al router virtual.

Para minimizar el tráfico de la red, sólo los routers Activo y Stanby envían mensajes de HSRP periódicos una vez que el protocolo ha completado el proceso de elección. Si el router activo falla, el router en espera actúa como router activo. Si el router de espera falla o se convierte en el router activo, entonces se selecciona otro router como router de espera.

En una LAN determinada, pueden coexistir y superponerse varios grupos en reserva activos. Cada grupo en espera emula a un solo router virtual. Los routers individuales pueden participar en varios grupos. En este caso, el router mantiene estados y temporizadores separados para cada grupo.

Cada grupo en espera tiene una dirección MAC única y conocida, así como una dirección IP.

## Direccionamiento HSRP

En la mayoría de los casos cuando configura los routers para que estén separados del un grupo HSRP, los mismos detectan la dirección MAC de HSRP para ese grupo como también su propias direcciones MAC impresas a fuego. La excepción es el Routers cuyos controladores Ethernet reconocen solamente una sola dirección MAC (por ejemplo, el controlador Lance en el Cisco2500 y los Cisco 4500 Router). Este Routers utiliza la dirección MAC del HSRP cuando él es el router activo, y a su dirección impresa a fuego cuando él no es.

El HSRP utiliza la dirección MAC siguiente en todos los media excepto el Token Ring:

```
0000.0c07.ac**   (where ** is the HSRP group number)
```

Las interfaces Token Ring utilizan direcciones funcionales para la dirección MAC de HSRP. Las direcciones funcionales son el único mecanismo de multidifusión general disponible. Hay una cantidad limitada de direcciones funcionales de anillo token disponibles y muchas de ellas están reservadas para otras funciones. Puede utilizar las tres direcciones siguientes con HSRP:

```
c000.0001.0000   (group 0)
c000.0002.0000   (group 1)
c000.0004.0000   (group 2)
```

**Nota:** Cuando los funcionamientos del HSRP en un entorno del (SRB) del Source-Route Bridging de los anillos múltiples y los routers del HSRP residen en diversos timbres, usando las direcciones funcionales puede causar la confusión del (RIF) del campo routing information. Por ejemplo, en un ambiente SRB, es posible que un router HSRP en espera resida en un anillo diferente al router activo. Cuando este router en espera se vuelve activo, las estaciones en el mismo anillo que el anterior router activo necesitan un nuevo RIF a fin de enviar paquetes al nuevo router activo. Sin embargo, dado que el router en espera (activo nuevo) está utilizando la misma dirección funcional que el router activo anterior, las estaciones no advierten que deben enviar exploradores para un nuevo RIF. Por esta razón, se presentó el comando use-bia.

## Versión de IOS de Cisco y matriz de funcionalidad de HSRP

Este documento muestra qué versiones del software del IOS® de Cisco admiten funciones HSRP. Haga clic en una función para ver una descripción detallada. Un número de versión interina indica

en qué versión apareció por primera vez la función o la versión donde cambió.

| Función | 10.0 | 10.2 | 10.3 | 11.0 | 11.1 | 11.2 | 11.3 | 12.0 | 12.0T | 12.1 | 12.1T |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Prioritario | X | X | X | X | X | X | X | X | X | X | X |
| Grupos múltiples (MHSRP) | | | X | X | X | X | X | X | X | X | X |
| Ethernet es 802.10 SDE | | | | | X | X | X | X | X | X | X |
| Seguimiento de interfaz | | | | | X | X | X | X | X | X | X |
| Utilice BIA | | | | | 8.0 | X | X | X | X | X | X |
| Demora de retención | | | | | | X | X | 6.1 | X | X | X |
| LANE Ethernet | | | | | | X | X | X | X | X | X |
| LANE de Token Ring | | | | | | | X | X | X | X | X |
| ISL | | | | | | | X | X | X | X | X |
| soporte syslog | | | | | | | X | X | X | X | X |
| Intervalo de actualización de MAC | | | | | | | | 1.0 | X | X | X |
| SNMP MIB | | | | | | | | | 3.0 | X | X |
| MHSRP y utilice BIA | | | | | | | | | 3.4 | X | X |
| Redundancia IP | | | | | | | | | 3.4 | X | X |
| BVI | | | | | | | | | 6.2 | X | X |
| 802.1Q | | | | | | | | | 8.1 | X | X |
| Depuración HSRP mejorada | | | | | | | | | | 0.2 | X |
| Redirecci | | | | | | | | | | | 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ón HSRP ICMP | | | | | | | | | | | |
| VPN HSRP MPLS | | | | | | | | | | | 3 |

# Imágenes del arranque de sistema y funcionalidad HSRP del Cisco IOS

La funcionalidad HSRP fue incluida en las imágenes del arranque de sistema del Cisco IOS hasta la integración del Id. de bug Cisco CSCec16720 (clientes registrados solamente). El Id. de bug Cisco CSCec16720 quitó el HSRP de las imágenes del arranque de sistema a excepción de:

- c7200-boot-mz
- c7200-kboot-mz
- c10k-eboot-mz
- c4500-boot-mz
- c7200-boot-mz
- c7200-kboot-mz
- c7400-kboot-mz
- ubr7200-boot-mz
- c6400r-boot-mz
- RPM-inicio-mz
- rpmxf-inicio-mz
- Rsp-boot-mz
- URM-wboot-mz
- c5350-boot-mz
- c5400-boot-mz
- c7301-boot-mz
- c5850-boot-mz
- c4gwy-cboot-mz
- ubr910-rboot-mz
- ubr910-rboot-mz
- ubr925-k8boot-mz
- c5850tb-boot-mz

# Funciones de HSRP

## Prioritario

La característica HSRP de prioridad habilita al router con mayor prioridad para que inmediatamente pase a ser el router activo. La prioridad se determina en primer lugar por el valor de prioridad que usted configure y luego por la dirección IP. En cada caso, un valor más alto tiene mayor prioridad.

Cuando un router más prioritario se apropia de un router de menor prioridad, envía un mensaje de golpe. Cuando un router activo de prioridad inferior recibe un mensaje de golpe o un mensaje de

saludo desde un router activo de prioridad superior, cambia al estado hablar y envía un mensaje de renuncia.

### Demora de retención

La función de retraso de la apropiación permite el derecho preferente de compra sea retrasado por un periodo de tiempo configurable, permitiendo que el router pueble su tabla de ruteo antes de sentir bien al router activo.

Antes del Cisco IOS Software Release 12.0(9), el retardo encendido cuando el router recargó. En la versión 12.0(9) del IOS de Cisco, el retraso comienza cuando la prioridad se intenta por primera vez.

**Para configurar la prioridad HSRP, utilice el comando standby [group] [priority number] [preempt [delay [minimum] seconds] [sync seconds.**

Refiera a la documentación HSRP para más información sobre configurar el HSRP.

## Seguimiento de interfaz

El seguimiento de interfaz le permite especificar otra interfaz en el router para que el proceso HSRP monitoree y pueda alterar la prioridad HSRP de un grupo determinado.

Si se interrumpe el funcionamiento del protocolo de línea de la interfaz especificado, se reduce la prioridad de HSRP de este router y se permite la activación de otro router HSRP con prioridad más alta (en caso de tener habilitada la prioridad).

**Para configurar el rastreo de interfaz HSRP, use el comando standby [grupo] track interface [prioridad].**

Cuando varias interfaces rastreadas se encuentran desconectadas, la prioridad se reduce por una cantidad acumulativa. Si establece de manera explícita el valor de disminución, entonces el valor disminuye en la cantidad especificada si la interfaz se encuentra inactiva, y la disminución es acumulativa. Si no establece un valor de disminución explícito, el valor se disminuye en 10 por cada interfaz que se desactiva, y las disminuciones son acumulativas.

El siguiente ejemplo utiliza la configuración siguiente, con el valor de disminución predeterminado de 10.

**Nota:** Cuando no se especifica un número de grupo HSRP, el número de grupo predeterminado es grupo 0.

```
interface ethernet0
     ip address 10.1.1.1 255.255.255.0
     standby ip  10.1.1.3
     standby priority 110
     standby track serial0
     standby track serial1
```

El comportamiento de HSRP con esta configuración es:

- 0 interfaces inactivas = sin disminución (la prioridad es 110)
- 1 interfaz inactiva = disminuye en 10 (la prioridad se vuelve 100)

- 2 interfaz inactiva = disminuye en 10 (la prioridad se vuelve 90)

El comportamiento HSRP anterior es verdadero incluso si los valores decrecientes están configurados explícitamente como sigue:

```
interface ethernet0
     ip address 10.1.1.1 255.255.255.0
     standby ip  10.1.1.3
     standby priority 110
     standby track serial0 10
     standby track serial1 10
```

Antes del Cisco IOS Release 12.1, si usted enciende a un router con una interfaz fuera de servicio, el seguimiento de interfaz del HSRP mira la interfaz como para arriba.

Este defecto tiene ID de falla de funcionamiento Cisco CSCdp32289 (sólo para clientes registrados).

## Use dirección programada en fábrica

El uso de la característica Dirección impresa a fuego (BIA) permite que los grupos HSRP utilicen una dirección MAC impresa a fuego de la interfaz en lugar de una dirección MAC HSRP. El uso de BIA se implementó por primera vez en la versión 11.1(8) del software Cisco IOS. **Para configurar HSRP utilizando el BIA, use el comando standby use-bia [scope interface].**

El comando use-bia se implementó para superar las limitaciones de la utilización de una dirección funcional para la dirección de HSRP MAC en interfaces Token Ring.

**Nota:** Cuando HSRP funciona en un entorno de conexión en puente con ruteo de origen de anillos múltiples y los routers HSRP residen en diferentes anillos, el uso de direcciones funcionales puede ocasionar confusión de Campo de información de ruteo (RIF). Por esta razón, se presentó el comando use-bia.

La función use-bia también habilita el uso de DECnet, Xerox Network Systems (XNS) y HSRP en el mismo router al permitir que la dirección MAC DECnet (el BIA) se utilice como la dirección MAC HSRP. **El comando use-bia** es también útil en las situaciones de la conexión en red en donde el BIA de un dispositivo se ha configurado en los otros dispositivos en el LAN.

Sin embargo, el comando use-bia presenta varias desventajas:

- Cuando un router hace activo, mueven a la dirección IP virtual a una diversa dirección MAC. El nuevo router activo envía una respuesta de ARP gratuito, pero no todas las implementaciones de host gestionan ARP gratuito de manera adecuada.
- Proxy ARP se interrumpe al configurar use-bia. Un router inactivo no puede cubrir para la base de datos ARP de representación perdida de un router defectuoso.
- Antes de la versión 12.0(3.4)T del IOS de Cisco, se permite sólo un grupo HSRP si use-bia está configurado.

Cuando usted configura el **comando use-bia** en una subinterfaz, aparece realmente en la interfaz principal y se aplica a todas las subinterfaces. En IOS de Cisco versión 12.0(6.2) o posterior, el comando use-bia se amplía con las palabras clave opcionales de la interfaz de alcance para poder aplicarlo a una subinterfaz única.

Este defecto tiene Id. de bug Cisco CSCdm25468 (clientes registrados solamente).

## grupos HSRP múltiples

La característica de los grupos de HSRP múltiples (MHSRP) fue agregada a la Versión 10.3 del IOS de Cisco. Esta característica permite mayor redundancia y carga compartida dentro de las redes también permite routers de redundancia para ser usado completamente. Mientras que un router reenvía tráfico de manera activa para un grupo HSRP, puede estar en espera o en estado de escucha para otro grupo.

A partir del Cisco IOS Release 12.0(3.4)T, usted puede utilizar el **comando use-bia** con los grupos HSRP múltiples habilitados.

Refiera a la carga a compartir con el HSRP para configurar el HSRP para aprovecharse de los trayectos múltiples.

## Dirección MAC configurable

Usted utiliza normalmente el HSRP para ayudar a las estaciones terminales para localizar el primer gateway del salto para el Routing IP. Las estaciones terminales se configuran con un default gateway. No obstante, HSRP puede proporcionar la primera redundancia de salto para otros protocolos. Algunos protocolos, como el de Interconexión par a par avanzado (APPN), utilizan la dirección MAC para identificar el primer salto a los efectos del ruteo.

En este caso, es por lo general necesario poder especificar la dirección MAC virtual mediante el comando standby mac-address. La dirección IP virtual no es importante para estos protocolos. La sintaxis real del comando es standby [group] mac-address mac-address.

**Nota:** Usted no puede utilizar este comando en una interfaz Token Ring.

## soporte syslog

El soporte para la mensajería de syslog para la información HSRP fue agregado en el Cisco IOS Release 11.3. Esta función permite un registro más eficiente y el rastreo de los routers actuales activos y en espera en servidores syslog.

## Depuración de HSRP

Antes del Cisco IOS Release 12.1, el comando hsrp debugging era relativamente simple. Para habilitar la depuración de HSRP, sólo era necesario usar el comando debug standby, el cual habilitaba la salida del estado HSRP y de la información de paquetes para todos los grupos en espera en todas las interfaces.

Una condición del debug fue agregada en el Cisco IOS Release 12.0(2.1) que permite la salida del **comando standby debug** de ser filtrado basó sobre la interfaz y el número de grupo. El comando utiliza el paradigma de la **condición del debug** introducido en el Cisco IOS Release 12.0, como sigue: condición del debug La interfaz especificada debe ser una interfaz válida capaz de admitir HSRP. El grupo puede ser cualquiera (0 - 255).

Usted puede fijar las condiciones del debug para los grupos que no existen, que permite que usted capture la información del debug durante la inicialización de un nuevo grupo.

Debe habilitar la orden de depuración en espera para generar resultados con el comando de

depuración. Si no configura ninguna condición de depuración en espera, entonces se producirá el resultado de la depuración para todos los grupos en todas las interfaces. Si configura por lo menos una condición de depuración en espera, entonces la salida de depuración en espera es filtrada de acuerdo con todas las condiciones de depuración en espera.

## Depuración HSRP mejorada

Antes del Cisco IOS Release 12.1(0.2), el debugging HSRP era de uso limitado porque la información fue perdida en el ruido de los mensajes de saludo periódico. Por esta razón, se agregó la función mejorada de depuración en el IOS 12.1(0.2) de Cisco .

La siguiente tabla explica las opciones de comandos para mejorar la depuración.

| Comando | Descripción |
|---|---|
| debug standby | Muestra todos los errores, eventos y paquetes HSRP. |
| debug standby terse | Visualiza todos los errores de HSRP, eventos, y paquetes, excepto hola y paquetes de anuncio. |
| depurar errores standby | Muestra errores HSRP. |
| eventos espera del debug [[todos \| conciso] \| [ICMP \| protocolo \| redundancia \| pista]] [detail] | Muestra eventos HSRP. |
| paquetes espera del debug [[todos \| conciso] \| [haga publicidad \| golpe \| hola \| dimita]] [detail] | Muestra paquetes HSRP. |

Puede filtrar el resultado de depuración utilizando la depuración condicional del grupo HSRP y de interfaz. Para habilitar el debugging condicional de la interfaz, utilice el **comando debug condition interface interface**. Para habilitar el debugging condicional del HSRP, utilice el **comando debug condition standby interface group**.

Una condición de depuración de interfaz se aplica sólo cuando usted no ha establecido ninguna condición de depuración en espera. El debugging HSRP se aumenta más a fondo en el Cisco IOS Software Release 12.1(1.3), sobre la base de las mejoras que fueron llevadas a cabo a la tabla de estado de HSRP.

Este defecto tiene el ID de falla de funcionamiento Cisco CSCdp57811 (sólo clientes registrados).

Estas optimizaciones muestran los eventos de la tabla de estado de HSRP. En la salida debajo de la **a**, el **b**, **c**, y así sucesivamente, refiere a los eventos de la máquina de estados finitos del HSRP, que se documentan en el RFC 2281 .

```
SB1: Ethernet0/2 Init: a/HSRP enabled
SB1: Ethernet0/2 Active: b/HSRP disabled (interface down)
SB1: Ethernet0/2 Listen: c/Active timer expired (unknown)
SB1: Ethernet0/2 Active: d/Standby timer expired (20.0.0.3)
SB1: Ethernet0/2 Speak: f/Hello rcvd from higher pri Speak router
SB1: Ethernet0/2 Active: g/Hello rcvd from higher pri Active router
```

```
SB1: Ethernet0/2 Speak: h/Hello rcvd from lower pri Active router
SB1: Ethernet0/2 Standby: i/Resign rcvd
SB1: Ethernet0/2 Active: j/Coup rcvd from higher pri router
SB1: Ethernet0/2 Standby: k/Hello rcvd from higher pri Standby router
SB1: Ethernet0/2 Standby: l/Hello rcvd from lower pri Standby router
SB1: Ethernet0/2 Active: m/Standby mac address changed
SB1: Ethernet0/2 Active: n/Standby IP address configured
```

## Autenticación

La característica de autenticación HSRP consiste en una clave compartida de texto sin cifrar incluida en los paquetes HSRP. Esta característica evita que el router de menor prioridad aprenda la dirección IP de reserva y valores de temporizador en espera del router de mayor prioridad.

Para configurar la cadena de la autentificación del HSRP, utilice el comando standby authentication string.

## Redundancia IP

El HSRP proporciona la redundancia sin estado para el Routing IP. HSRP sólo se limita al mantenimiento de su propio estado. Asume que cada router construye y mantiene sus propias tablas de ruteo independientemente del otro Routers. La característica de la redundancia IP proporciona un mecanismo que permita que el HSRP proporcione un servicio a las aplicaciones de cliente de modo que puedan implementar a la Falla Statefull.

La redundancia IP no proporciona un mecanismo para las aplicaciones de peer a la información de estado de intercambio. Esto se deja a las aplicaciones ellos mismos, y es esencial si las aplicaciones son proporcionar a la Falla Statefull.

La redundancia IP (en enero 2000) se implementa actualmente solamente para los agentes del hogar del IP móvil. Lo que sigue es una configuración de muestra:

```
configure terminal
 router mobile
 ip mobile home-agent standby hsrp-group1
!
interface e0/2
 no shutdown
 ip address 20.0.0.1 255.0.0.0
 standby 1 ip 20.0.0.11
 standby 1 name hsrp-group1
```

**Nota:** A partir de la versión 12.1(3)T del IOS de Cisco, se acepta la palabra clave redundancy además de la palabra clave standby. **La palabra clave standby** será eliminada en un Cisco IOS Release posterior. El comando correcto entonces será la Redundancia móvil **hsrp-group1 del** Home Agent del IP.

Los usos futuros de redundancia de IP pueden comprender:

- NAT - Necesidad de proporcionar los gatewayes redundantes.
- IPSEC - Necesidad de sincronizar la información del estado para actuar cuando el HSRP es funcionando.
- Servidor DHCP – servidores DHCP implementados en varios routers.
- NBAR, CBAC - Necesitan duplicar los estados del firewall para el ruteo asimétrico.
- GPRS - Necesita una manera de seguir el estado TCP.
- PIX

## Base de información para administración de SNMP

El soporte de la base de información de administración de SNMP (MIB) fue agregado al Cisco IOS Release 12.0(3.0)T. Hay dos MIB relevantes para HSRP:

- ciscoMgmt 106: El módulo MIB para administración de HSRP
- ciscoMgmt 107: Módulo MIB de ampliación para administración de HSRP

En las versiones del IOS de Cisco anteriores a la 12.0(6.1)T, cuando está presente una Interfaz virtual de grupo de puente (BVI), un recorrido del MIB HSRP extendido provoca un fallo en el router.

Este defecto tiene la identificación de error Cisco CSCdp57811 (sólo clientes registrados).

## Soporte de HSRP con Multiprotocol Label Switching Virtual Private Networks

En el Cisco IOS Release 12.1(3)T se agregó el soporte HSRP para los Multiprotocol Label Switching Virtual Private Networks (MPLS VPN).

HSRP en una interfaz MPLS VPN es útil cuando se tiene una Ethernet que está conectada entre dos Proveedores de borde (PEs) y se tiene alguno de los siguientes:

- Un borde del cliente (CE) con una ruta predeterminada hacia la dirección IP virtual HSRP.
- Uno o más host con la dirección IP virtual del HSRP configurada como el default gateway.

El siguiente diagrama de red muestra dos PE con HSRP ejecutándose entre sus interfaces VPN de ruteo/reenvío (VRF). Configuramos el CE con una dirección IP virtual HSRP como su ruta predeterminada. Y configuramos HSRP para rastrear las interfaces que conectan los PE al resto de la red proveedora. Por ejemplo, si la interfaz E1 de PE1 falla, la prioridad de HSRP se verá reducida de modo tal que PE2 tomará el control del reenvío de paquetes a la dirección IP/MAC virtual.

Éstas son las configuraciones:

| Router PE1 | Router PE2 |
|---|---|
| **conf terminal** ! ip cef ! ip vrf vrf1 rd 100:1 route-target export 100:1 route-target import 100:1 ! interface ethernet0 no shutdown ip vrf forwarding vrf1 ip address 10.2.0.1 255.255.0.0 standby 1 ip 10.2.0.20 standby 1 priority 105 standby 1 preempt delay minimum 10 standby 1 timers 3 10 standby 1 track ethernet1 10 standby 1 track ethernet2 10 | **conf terminal** ! ip cef ! ip vrf vrf1 rd 100:1 route-target export 100:1 route-target import 100:1 ! interface ethernet0 no shutdown ip vrf forwarding vrf1 ip address 10.2.0.2 255.255.0.0 standby 1 ip 10.2.0.20 standby 1 priority 100 standby 1 preempt delay minimum 10 standby 1 timers 3 10 standby 1 track ethernet1 10 standby 1 track ethernet2 10 |

Puede utilizar los siguientes comandos para verificar que la dirección IP virtual de HSRP se encuentra en las tablas de VRF ARP y de Cisco Express Forwarding correspondientes:

```
ed1-pe1# show ip arp vrf vrf1 Protocol Address Age (min) Hardware Addr Type Interface Internet
```

```
10.2.0.1 - 00d0.bbd3.bc22 ARPA Ethernet0/2 Internet 10.2.0.20 - 0000.0c07.ac01 ARPA Ethernet0/2
ed1-pe1# show ip cef vrf vrf1 Prefix Next Hop Interface 0.0.0.0/0 10.3.0.4 Ethernet0/3
0.0.0.0/32 receive 10.1.0.0/16 10.2.0.1 Ethernet0/2 10.2.0.0/16 attached Ethernet0/2 10.2.0.1/32
receive 10.2.0.20/32 receive 224.0.0.0/24 receive 255.255.255.255/32 receive
```

## Soporte de HSRP para redireccionamiento de ICMP

HSRP se basa en el concepto de que los routers de par HSRP que protegen una subred pueden proporcionar acceso a todas las demás subredes que conforman la red. En consecuencia, es irrelevante cuál router se convierte en un router HSRP activo, ya que todos los routers tenían rutas hacia cada subred.

El HSRP hace uso de una dirección IP virtual especial y de una dirección MAC virtual, que se asocian lógicamente al router activo del HSRP. Las redirecciones ICMP están automáticamente desactivadas en una interfaz cuando se utiliza HRSP en esa interfaz. El IOS 12.1(3)T hacia adelante, característica de las redirecciones ICMP habilita las redirecciones ICMP en las interfaces configuradas con el HSRP. Refiera al Soporte de HSRP para redireccionamiento de ICMP para más detalles. Esto se hace para evitar que los host sean redireccionados fuera de la dirección IP virtual HSPR. Es posible que los dos (o más) routers en una subred no tengan una conectividad idéntica al resto de la red. Es decir, para una dirección de IP de destino particular, es posible que un router o el otro posean un trayecto mucho mejor a dicha dirección o incluso es posible que sea el único router conectado a dicha dirección.

El protocolo ICMP permite que un router redireccione una estación final para enviar paquetes para un determinado destino a otro router en la misma subred, si el primer router sabe que el otro router tiene un mejor trayecto para ese destino específico. Como sucedía en el caso de los gateways predeterminadas, si falla el router al cual se redirige una estación final para un destino en particular, no se entregan los paquetes de la estación final dirigidos a ese destino. Esto es exactamente lo que sucede en HSRP estándar. Por esto, recomendamos deshabilitar las redirecciones ICMP si el HSRP está encendido.

Ampliar la relación entre las redirecciones ICMP y el HSRP proporciona una solución a este problema, permitiendo que usted se aproveche de las ventajas del HSRP y de las redirecciones ICMP. Dos (o más) grupos HSRP se ejecutan en cada subred, con al menos tantos grupos HSRP configurados como haya routers participantes. Las prioridades se configuran a fin de que cada uno de los routers sea el principal de al menos un grupo HSRP. Cuando un router determina para reorientar un endstation a un diverso router para un destino específico, después en vez de reorientar el endstation al IP Address de ese otro router, encuentra que un grupo del HSRP que está siendo dominó por ese router, y reorienta el endstation a la dirección IP virtual correspondiente. Si ocurre que ese router de destino falla, HSRP se asegura de que otro router haga el trabajo y, quizá, redireccione la estación final a otro router virtual.

# Soporte de medios e interfaz HSRP

Esta sección explica qué interfaces y soportes del HSRP de los media, y las posibles advertencias al ejecutar el HSRP sobre estos media.

Desde el Cisco IOS Software Release 10.0, la funcionalidad HSRP ha estado disponible en los Ethernetes, el Token Ring y el Fiber Distributed Data Interface (FDDI). HSRP también admite interfaces Fast Ethernet y ATM.

Las Virtual LANs (VLAN) permiten topologías lógicas de red para superponer la infraestructura física conmutada de manera tal que toda recolección arbitraria de puertos LAN puede combinarse

en un grupo de usuarios autónomo o comunidad de intereses. El soporte a VLAN del HSRP fue agregado en el Cisco IOS Release 11.1 para el Secure Data Exchange del IEEE 802.10 (SDE), y en el Cisco IOS Release 11.3 para el Cisco Inter-Switch Link (ISL).

## Ethernet

Varios controladores Ethernet (Lance y QUICC) en productos básicos sólo pueden tener una sola dirección MAC de unidifusión en su filtro de direcciones. En estas plataformas sólo se permite un solo grupo HSRP, y la dirección de interfaz cambia por la dirección MAC virtual del HSRP cuando el grupo pasa a estar activo. Si se utiliza HSRP en routers con interfaces múltiples de este tipo, se debe configurar cada interfaz con un número distinto de grupo HSRP.

**Nota:** El router 7200 de Cisco también usa el controlador Ethernet Lance, pero admite MHSRP en software.

Cisco recomienda no tener más de veinticuatro procesadores de interfaz Ethernet (EIP) HSRP debido al tiempo que se requiere para actualizar los filtros de direcciones para HSRP. Tener más de veinticuatro HSRP EIP puede causar inestabilidad y recarga excesiva del CPU.

Este defecto tiene Id. de bug Cisco CSCdj29595 (clientes registrados solamente).

Si usted tiene más de veinticuatro EIP, intente substituir los EIP por el Versatile Interface Processors (VIP) y los adaptadores de puerto Ethernet. Los VIP se han aprobado para hasta ochenta grupos HSRP. Usted puede también reducir el número de grupo HSRP, y aumenta el HSRP hello y el tiempo en espera.

## Token Ring

Una limitación del HSRP corriente en una interfaz Token Ring es que usted no puede reprogramar el filtro de direcciones en el chipset del Token Ring la misma manera que usted puede en los Ethernetes, FDDI o emulación de ATM. El Token Ring utiliza a las direcciones funcionales, cuyo hay solamente un pequeño número disponible que no están en conflicto con otras aplicaciones del espacio de dirección funcional.

Al ejecutar HSRP en un entorno de bridging con ruteo de origen (SRB), el uso de direcciones funcionales puede ocasionar una confusión de RIF. Para obtener mayor información, consulte la sección sobre Asignación de HSRP. También, intente configurar el **comando use-bia**.

## 802.1Q

Cisco recomienda usando el Cisco IOS Software Release 12.0(8.1)T o Posterior para el HSRP sobre el 802.1Q.

## ISL

HSRP sobre ISL está disponible en las versiones IOS de Cisco 11.2(6)F, 11.3, 12.X. Se recomienda el uso de la versión 12.0(7) o posterior para evitar el problema descrito en la ID de falla de funcionamiento Cisco CSCdm68811 (sólo para clientes registrados).

## FDDI

Un adaptador de puerto FDDI separa las tramas del anillo si ve una de sus direcciones MAC en la fuente MAC. Si un evento de red hace a ambo Routers ir active, después ambo Routers envía los paquetes del HSRP hello con la misma dirección MAC virtual. Cada router separa de la red por error el paquete de saludo del otro router y ambos permanecen activos.

Este defecto cuenta con depurador Cisco ID CSCdj30049 (únicamente para clientes registrados).

La solución para este problema en la Versión 11.2(11.1) del IOS de Cisco es para que los routers HSRP en un entorno FDDI utilicen su única dirección MAC impresa a fuego para intercambiar mensajes y correr el protocolo HSRP. Para asegurarse de que los puentes de aprendizaje y los switches almacenan la entrada correcta del puerto para la dirección virtual de MAC, el router activo también envía mensajes de actualización periódicos mediante la dirección MAC HSRP.

**Nota:** Es posible que la memoria direccionable por contenido (CAM) de hardware del router de Cisco 4500 en una interfaz FDDI no se llene de manera correcta luego de una recarga, en caso de que haya configurado varias redes RIP y grupos HSRP. La única solución alternativa ahora está borrar las interfaces para restablecer el CAM. Esta falla tiene el ID de error de Cisco CSCdm93122 (sólo para clientes registrados).

### Actualización de MAC

Los routers del HSRP en un entorno FDDI utilizan su propio Burned-In MAC Address único a los mensajes de intercambio y funcionan con el protocolo HSRP. Para asegurarse de que los puentes y los switches de aprendizaje guarden en la memoria caché la entrada correcta de puerto para la dirección MAC virtual, el router activo también envía mensajes de actualización periódicos utilizando la dirección MAC de HSRP. Este defecto cuenta con depurador Cisco ID CSCdj30049 (únicamente para clientes registrados).

Si usted no tiene un Switch o un Learning Bridge en su red, usted puede inhabilitar el envío de restaura los paquetes como se muestra abajo:

```
interface fddi 1/0/0
 ip address 10.1.1.1 255.255.255.0
 standby ip 10.1.1.250
 standby mac-refresh 0
```

### Interfaz virtual de grupo de puente

Se agregó soporte de HSRP para las Interfaces virtuales de grupo de puente (BVI) en la versión 12.0(6.2)T del IOS de Cisco.

### Subinterfaces

Los grupos de HSRP en las subintefaces deben tener un número de grupo único entre todos los otros grupos de todas las subinterfaces en la misma interfaz principal. Esto es porque las subinterfaces no reciben un índice de interfaz de SNMP único. Si tuviera dos grupos con el número N en subinterfaces diferentes, entonces, en la MIB, el grupo N en la subinterfaz 1 y el grupo N en la subinterfaz 2 parecerían el mismo grupo.

## Información Relacionada

- Página de Soporte de HSRP

- HSRP - FAQ
- Soporte Técnico y Documentación - Cisco Systems