

Características e funcionalidade do protocolo de roteador do standby recente

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Background e operações HSRP](#)

[Mecanismos de descoberta de roteador dinâmico](#)

[Operação HSRP](#)

[Endereçamento de HSRP](#)

[Versão do Cisco IOS e matriz de funcionalidade de HSRP](#)

[Imagens de boot e funcionalidade de HSRP do Cisco IOS](#)

[Recursos de HSRP](#)

[Preempção](#)

[Acompanhamento de interface](#)

[Usar endereço de operação antecipada](#)

[Diversos grupos de HSRP](#)

[Endereço MAC configurável](#)

[suporte de syslog](#)

[Depuração HSRP](#)

[depuração de HSRP aprimorada](#)

[Autenticação](#)

[Redundância de IP](#)

[Base de informações de gerenciamento do SNMP](#)

[Suporte HSRP para Virtual Private Networks de switching de rótulo multiprotocolo](#)

[Suporte de HSRP para redirecionamentos de ICMP](#)

[Interface HSRP e suporte de mídia](#)

[Ethernet](#)

[Token Ring](#)

[802.1Q](#)

[ISL](#)

[FDDI](#)

[Atualização de MAC](#)

[Grupo virtual de interface de ponte](#)

[Subinterfaces](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as características e a funcionalidade do Hot Standby Router Protocol (HSRP).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Background e operações HSRP

Uma maneira de obter um tempo de ativação da rede de quase 100% é usar o HSRP, que fornece redundância de rede para redes IP, garantindo que tráfego do usuário se recupere imediatamente e transparentemente a partir das primeiras falhas de nó nos dispositivos de extremidade de rede ou nos circuitos de acesso.

Compartilhando um endereço IP e um endereço MAC (Camada 2), dois ou mais roteadores podem agir como um roteador "virtual" simples. Os membros do grupo de roteadores virtuais transferem continuamente mensagens de status. Esta maneira, um roteador pode supor a responsabilidade de roteamento de outro, se sair da comissão para de planejamento ou motivos não planejados. Os hosts continuam encaminhando os pacotes de IP para um endereço IP e MAC consistente e é transparente a comutação de dispositivos realizando o roteamento.

Mecanismos de descoberta de roteador dinâmico

Estão abaixo as descrições dos mecanismos dinâmicos de descoberta do roteador que estão disponíveis aos anfitriões. Muitos desses mecanismos não fornecem a elasticidade de rede exigida por administradores de rede. Isso é devido ao fato de o protocolo não estar configurado inicialmente para fornecer a elasticidade de rede ou porque é impossível que cada host em uma rede execute o protocolo. Além do que o que está listado abaixo, é importante notar que muitos anfitriões permitem somente que você configure um gateway padrão.

Protocolo de resolução de endereço proxy

Alguns Host IP usam o protocolo proxy address resolution (ARP) para selecionar um roteador. Quando um host executa proxy ARP, envia uma solicitação de ARP para o endereço IP do host remoto que deseja contatar. Um roteador da rede, o Roteador A, responde em nome do host

remoto e fornece seu próprio endereço MAC. Com o ARP proxy, o host se comporta como se o host remoto estivesse conectado ao mesmo segmento da rede. Se o Roteador A falhar, o host continuará a enviar pacotes destinados ao host remota para o endereço MAC do Roteador A, mesmo que esses pacotes não tenham para onde ir e sejam perdidos. Você pode ou esperar o ARP para adquirir o MAC address de um outro roteador, o roteador B, no segmento local enviando uma outra requisição ARP, ou recarregue o host para forçá-lo para enviar uma requisição ARP. Em qualquer dos casos, por um período significativo, o host não pode comunicar-se com o host remoto, mesmo que o protocolo de roteamento convirja, e o roteador B seja preparado para transferir os pacotes que dirigiriam de outra maneira o roteador A.

[Dynamic Routing Protocol](#)

Alguns Host IP executam (ou espião) um protocolo de roteamento dinâmico tal como o Routing Information Protocol (RIP) ou abrem o trajeto de Shortes primeiramente (OSPF) para descobrir o Roteadores. A desvantagem de usar o RIP é que ele é lento para se adaptar às mudanças na topologia. Executar um Dynamic Routing Protocol em cada host pode não ser viável por diversas razões, entre as quais a sobrecarga administrativa, a sobrecarga de processamento ou a falta de uma implementação de protocolo para algumas plataformas.

[Protocolo de descoberta de roteador IRDP](#)

Algun protocolo de descoberta de roteador ICMP (IRDP) mais novo do uso dos Host IP ([RFC 1256](#)) para encontrar um roteador novo quando uma rota se tornar não disponível. [Um host que execute o IRDP escuta olá! mensagens de transmissão múltipla de seu roteador configurado e usa um roteador alternativo quando já não recebe aqueles mensagens Hello Messages. Os valores do temporizador padrão de IRDP indicam que isso não é adequado para a detecção de falha do primeiro nó. A taxa de anúncio padrão é um a cada 7 a 10 minutos, e o tempo de vida padrão é de 30 minutos.](#)

[Protocolo de configuração dinâmica host](#)

O protocolo de configuração dinâmica host (DHCP) ([RFC 1531](#)) fornece um mecanismo passando a informação de configuração aos anfitriões em uma rede TCP/IP. [Um host que executa um cliente DHCP solicita informações de configuração de um servidor DHCP quando é inicializado na rede. Esta informação de configuração compreende tipicamente um endereço IP de Um ou Mais Servidores Cisco ICM NT e um gateway padrão. Não há nenhum mecanismo para comutar a um roteador alternativo se o gateway padrão falha.](#)

[Operação HSRP](#)

Uma grande classe de implementações de host do legado que não apoiam a descoberta dinâmica é capaz de configurar um roteador padrão. Executar um mecanismo de descoberta de roteador dinâmico em cada host pode não ser adequado por diversas razões, incluindo sobrecarga administrativa, sobrecarga de processo, problemas de segurança ou falta de implementação de um protocolo para algumas plataformas. O HSRP proporciona serviços do Failover a estes anfitriões.

Usando o HSRP, um conjunto de roteador trabalha no concerto para apresentar a ilusão de um único roteador virtual aos anfitriões no LAN. Esse conjunto é conhecido como grupo de HSRP ou grupo em espera. Um roteador único eleito a partir do grupo é responsável por encaminhar os pacotes que os hosts enviam ao roteador virtual. Esse roteador é conhecido como o roteador

ativo. Outro roteador está eleito como roteador em standby. Em caso de falha do roteador Ativo, o roteador de Standby assume as funções de encaminhamento de pacotes do Ativo. Embora um número arbitrário de roteadores possa executar o HSRP, somente o roteador ativo encaminhará os pacotes enviados ao roteador virtual.

Para minimizar o tráfego da rede, somente os roteadores Ativo e Em Espera enviam mensagens de HSRP periódicas após o protocolo ter concluído o processo de eleição. Se o roteador ativo falhar, o roteador em standby assume como o roteador ativo. Se o roteador em standby falhar ou se tornar um roteador ativo, então outro roteador é escolhido como roteador em standby.

Em uma LAN específica, diversos grupos de hot-standby podem coexistir e se sobrepor. Cada grupo de standby emula um único roteador virtual. Os roteadores individuais podem participar de vários grupos. Nesse caso, o roteador mantém estado e cronômetros separados para cada grupo.

Cada grupo em standby tem um único endereço MAC e um único endereço IP conhecidos.

Endereçamento de HSRP

Na maioria dos casos, quando você configura roteadores para fazerem parte de um grupo HSRP, eles ouvem o endereço MAC do HSRP desse grupo e também os seus próprios endereços de operação. A exceção é o Roteadores cujos os controladores do Ethernet reconhecem somente um único MAC address (por exemplo, o controlador de lance em Cisco2500 e Cisco 4500 Router). Este Roteadores usa o MAC address HSRP quando é o roteador ativo, e seu endereço operação antecipada quando não é.

O HSRP usa o seguinte MAC address em todos os media exceto o Token Ring:

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

Interfaces de token ring usam endereços funcionais para o endereço HSRP MAC. Os endereços funcionais são o único mecanismo de transmissão múltipla geral disponível. Há um número limitado de endereços funcionais de Token Ring disponíveis e muitos deles são reservados para outras funções. Você pode usar os seguintes três endereços com HSRP:

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

Note: Quando as corridas HSRP em um ambiente da conexão de ligação de rota de origem (SRB) do anel múltiplo e nos roteadores de HSRP residem em anéis diferentes, usar os endereços funcionais pode causar a confusão do campo de informação de roteamento (RIF). Por exemplo, em um ambiente SRB é possível que o roteador HSRP em espera se localize em um anel diferente do roteador ativo. Quando esse roteador em espera se torna ativo, as estações no mesmo anel como o antigo roteador ativo precisam de um novo RIF para enviar pacotes para o novo roteador ativo. No entanto, como o roteador em espera (recém-ativado) está usando o mesmo endereço funcional do roteador ativo anterior, as estações não estão cientes de que devem enviar exploradores de envio para um novo RIF. [Por esta razão, o comando use-bia foi introduzido.](#)

Versão do Cisco IOS e matriz de funcionalidade de HSRP

Imagens de boot e funcionalidade de HSRP do Cisco IOS

A funcionalidade de HSRP foi incluída em imagens de boot do Cisco IOS até a integração da identificação de bug Cisco [CSCec16720](#) ([clientes registrados somente](#)). A identificação de bug Cisco CSCec16720 removeu o HSRP das imagens de boot à exceção 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-bota-MZ
- rpmsf-bota-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

Recursos de HSRP

Preempção

O recurso de antecipação do HSRP permite que o roteador com a prioridade mais alta se torne imediatamente o roteador ativo. A prioridade é determinada, primeiro, pelo valor de prioridade que você configura e, então, pelo endereço IP. Em cada caso, o valor mais alto tem maior prioridade.

Quando um roteador mais prioritário cancela um roteador de baixa prioridade, envia uma mensagem de vitória. Quando um roteador ativo de prioridade mais baixa recebe uma mensagem coup ou hello de um roteador ativo de prioridade mais alta, ele passa para o estado de fala e envia uma mensagem resign.

Retardo antecipado

Os recursos de retardo cancelar permitem a preempção seja atrasada por um período de tempo configurável, permitindo que o roteador povoe sua tabela de roteamento antes de transformar-se o roteador ativo.

Antes do Cisco IOS Software Release 12.0(9), o atraso ligado quando o roteador recarregou. No Cisco IOS versão 12.0(9), o retardo começa quando a antecipação é a primeira tentativa.

[Para configurar a prioridade de HSRP e preempção, use o comando `standby \[group\] \[priority number\] \[preempt \[delay \[minimum\] seconds\] \[sync seconds\]\] command`.](#)

Refira a [documentação HSRP](#) para obter mais informações sobre de configurar o HSRP.

[Acompanhamento de interface](#)

O rastreamento de interfaces permite especificar uma outra interface no roteador que deverá ser monitorada pelo processo HSRP a fim de alterar a prioridade HSRP de um grupo específico.

[Se o protocolo de linha da interface especificada for desativado, a prioridade HSRP desse roteador será reduzida, permitindo que outro roteador HSRP com prioridade mais alta se torne ativo \(caso o recurso de preempção esteja habilitado\).](#)

[Para configurar o rastreamento de interfaces HSRP, utilize o comando `standby \[group\] track interface \[priority\]`.](#)

Quando várias interfaces controladas estão desativadas, a prioridade é reduzida em uma quantidade cumulativa. Se você definir explicitamente o valor de decréscimo, esse valor será reduzido com base nessa quantidade se a interface for desativada e os decréscimos são cumulativos. Se você não definir uma diminuição explícita de valor, o valor será diminuído em 10 para cada interface desativada, e as diminuições serão acumulativas.

O exemplo seguinte usa a seguinte configuração, com o valor de decréscimo padrão do 10.

Note: Quando um número do grupo HSRP não é especificado, o número do grupo padrão é o 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
```

O comportamento HSRP com essa configuração é:

- 0 interface desativada = nenhuma diminuição (a prioridade é 110)
- 1 interface inativa = redução de 10 (a prioridade passa a ser 100)
- 2 interfaces desativada = diminuído por 10 (a prioridade torna-se 90)

O comportamento HSRP acima é verdadeiro mesmo que os valores de decréscimo estejam configurados explicitamente conforme a seguir.

```
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 do Cisco IOS Release 12.1, se você liga um roteador com uma interface inativa, o

acompanhamento de interface HSRP considera a relação como acima.

O defeito tem identificação de bug Cisco CSCdp32289 (somente clientes [registrados](#)).

Usar endereço de operação antecipada

A utilização do recurso de endereço de operação antecipado (BIA), permite que grupos de HSRP utilizem o endereço MAC antecipado da interface, em vez de um endereço MAC do HSRP. O uso do BIA foi implementado pela primeira vez no Cisco IOS versão 11.1(8). [Para configurar o HSRP, utilize o BIA e o comando standby use-bia \[scope interface\]](#).

O comando use-bia foi implementado para superar as limitações do uso de um endereço funcional para o endereço HSRP MAC em interfaces Token Ring.

Note: Quando o HSRP é executado em um ambiente de Source-Routed Bridging e de vários anéis e os roteadores HSRP residem em anéis diferentes, o uso dos endereços funcionais pode causar confusão de Routing Information Field (RIF). Por esta razão, o comando use-bia foi introduzido.

O recurso use-bia também permite o uso de DECnet, Xerox Network Systems (XNS) e HSRP no mesmo roteador, ao possibilitar que o endereço MAC DECnet (o BIA) seja usado como o endereço MAC HSRP. **O comando use-bia** é igualmente útil nas situações da comunicação de rede onde o BIA de um dispositivo foi configurado nos outros dispositivos no LAN.

No entanto, o comando use-bia tem diversas desvantagens:

- Quando um roteador se torna ativo, o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual está movido para um MAC address diferente. O roteador recém-ativado envia uma resposta de ARP gratuita, mas nem todas as implementações de host tratam o ARP gratuito corretamente.
- O ARP do proxy é interrompido quando o comando use-bia é configurado. Um roteador em standby não pode cobrir para a base de dados do proxy ARP perdida de um roteador falho.
- Antes da versão 12.0(3.4)T do Cisco IOS, apenas um grupo de HSRP era permitido se o use-bia estivesse configurado.

Quando você configura o **comando use-bia em uma** subinterface, aparece realmente na interface principal e está aplicada a todas as subinterfaces. Na versão 12.0(6.2) do Cisco IOS (e posterior), o comando use-bia é estendido com as palavras-chave da interface de escopo opcional para permitir que seja aplicado a uma única subinterface.

Este defeito tem a identificação de bug Cisco [CSCdm25468](#) ([clientes registrados somente](#)).

Diversos grupos de HSRP

O recurso de MHSRP (Vários grupos de HSRP) foi incluído no Cisco IOS versão 10.3. Este recurso também habilita a redundância e o compartilhamento de carga nas redes e permite que roteadores redundantes sejam utilizados mais plenamente. Enquanto um roteador estiver encaminhando ativamente o tráfego para um grupo de HSRP, ele poderá ficar em espera ou no estado de escuta para outro grupo.

Até à data do Cisco IOS Release 12.0(3.4)T, você pode usar o **comando use-bia** com os grupos hsrp múltiplos permitidos.

Refira o [compartilhamento de carga com HSRP](#) para configurar o HSRP a fim aproveitar-se de caminhos múltiplos.

[Endereço MAC configurável](#)

Normalmente você usa o HSRP para ajudar estações final a encontrar o primeiro gateway do salto para Roteamento IP. As estações final são configuradas com um gateway padrão. Entretanto, o HSRP pode fornecer a primeira redundância de nó para outros protocolos. Alguns protocolos, como o APPN (Rede peer-to-peer avançada), usam o MAC Address para identificar o primeiro salto para o roteamento.

[Nesse caso, costuma ser necessário poder especificar o endereço MAC virtual usando o comando standby mac-address.](#) O endereço IP virtual não é importante para esses protocolos. A sintaxe real do comando é standby [group] mac-address mac-address.

Note: Você não pode usar este comando em uma interface de token ring.

[suporte de syslog](#)

O apoio para o mensagem de syslog para a informação de HSRP foi adicionado no Cisco IOS Release 11.3. Este recurso permite registro mais eficiente e o rastreamento dos roteadores atualmente ativos e em espera nos servidores de syslog.

[Depuração HSRP](#)

Antes do Cisco IOS Release 12.1, o comando hsrp debugging era relativamente simples. [Para ativar a depuração HSRP, deve-se simplesmente usar o comando debug standby, que habilita a saída do estado de HSRP e as informações do pacote de todos os grupos em standby em todas as interfaces.](#)

Uma condição debugar foi adicionada no Cisco IOS Release 12.0(2.1) que permite a saída do **comando standby debug** ser filtrado baseou na relação e no número do grupo. O comando utiliza o paradigma da **condição debugar** introduzido no Cisco IOS Release 12.0, como segue: [debugar o grupo de interface em standby da circunstância](#). A interface especificada deve ser uma interface válida capaz de dar suporte a HSRP. O grupo pode ser qualquer grupo (0-255).

Você pode ajustar-se debuga condições para os grupos que não existem, que permite que você capture debuga a informação durante a iniciação de um grupo novo.

O standby debug order deve estar habilitado para qualquer tipo de saída de depuração a ser produzida. Se você não configurar nenhuma condição de depuração em standby, o resultado da depuração é produzido para todos os grupos em todas as interfaces. Se pelo menos uma condição de depuração standby for configurada, a saída da depuração standby será filtrada de acordo com todas as condições de depuração standby.

[depuração de HSRP aprimorada](#)

Antes do Cisco IOS Release 12.1(0.2), o hsrp debugging era do uso limitado porque a informação foi perdida no ruído dos mensagens de hello periódico. Assim, o recurso de depuração avançada foi adicionado ao Cisco IOS 12.1(0.2).

A tabela a seguir explica as opções de comando para depuração avançada.

Comando	Descrição
debug standby	Exibe todos os erros, eventos e pacotes HSRP.
debug standby terse	Indica todos os erros de HSRP, eventos, e pacotes, exceto olá! e pacotes de anúncio.
debug standby errors	Exibe erros HSRP.
debugar eventos à espera [[tudo sóbrio] [ICMP protocolo redundância [detail] da trilha]]	Exibe eventos de HSRP.
debugar pacotes à espera [[tudo sóbrio] [anuncie golpe olá! renuncie]] o [detail]	Exibe pacotes HSRP.

Você pode filtrar a saída de depurações, utilizando a depuração condicional de interface de grupo de HSRP. Para permitir o debugging condicional de interface, use o comando **debug condition interface interface**. Para permitir o debugging condicional HSRP, use o comando **debug condition standby interface group**.

Uma condição de depuração de interface se aplica apenas quando não são definidas condições de depuração em espera. O hsrp debugging é aumentado mais no Cisco IOS Software Release 12.1(1.3), com base nas melhorias que foram feitas à tabela de estado de HSRP.

O ID de erro desse defeito é Cisco CSCdp57811 (somente para clientes [registrados](#)).

Estas melhorias apresentam os eventos da tabela de estados de HSRP. Na saída abaixo do **a**, o **b**, **c**, e assim por diante, refere os eventos da máquina de estado finito HSRP, que são documentados no [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
```

[Autenticação](#)

O recurso de autenticação HSRP consiste em uma chave de texto claro compartilhada com os pacotes HSRP. Este recurso impede que o roteador de prioridade mais baixa conheça o endereço IP de standby e os valores do cronômetro em standby do roteador de prioridade mais alta.

Para configurar o string de autenticação HSRP, use o [comando standby authentication string](#).

Redundância de IP

O HSRP fornece a redundância stateless para Roteamento IP. O HSRP, por si só, limita-se a manter o próprio estado. Supõe que cada roteador constrói e mantém suas próprias tabelas de roteamento independentemente do outro Roteadores. A característica da redundância de IP fornece um mecanismo que permita que o HSRP proporcione um serviço aos aplicativos do cliente de modo que possam executar a comutação classificada.

A redundância de IP não fornece um mecanismo para aplicativos de peer à informação de estado de intercâmbio. Isto está deixado aos aplicativos eles mesmos, e é essencial se os aplicativos são fornecer a comutação classificada.

A redundância de IP atualmente (em janeiro 2000) é executada somente para agentes home IP Móveis. Seguir é uma configuração de exemplo:

```
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
```

Note: A partir do Cisco IOS versão 12.1(3)T, a redundância de palavras-chave é aceita além do standby de palavras-chave. **As palavras-chave em standby** serão postas em fase - para fora em um Cisco IOS Release mais atrasado. O comando correto será então a [Redundância móvel](#) **hsrp-group1** do [Home Agent IP](#).

Os usos futuros de redundância de IP podem incluir:

- NAT - Necessidade de fornecer gateways redundantes.
- IPSEC - Necessidade de sincronizar a informação de estado a fim operar-se quando o HSRP estiver no uso.
- Servidor DHCP - Servidores DHCP implementados em vários roteadores.
- NBAR, CBAC - Precisa refletir estados de firewall para roteamento assimétrico.
- GPRS - Precisa uma maneira de seguir o estado TCP.
- PIX

Base de informações de gerenciamento do SNMP

O apoio da base de informação de gerenciamento snmp (MIB) foi adicionado ao Cisco IOS Release 12.0(3.0)T. Há dois MIBs relevantes para HSRP:

- ciscoMgmt 106: O módulo MIB para gerenciamento de HSRP
- ciscoMgmt 107: O módulo de MIB de extensão para o gerenciamento de HSRP

Antes do Cisco IOS versão 12.0(6.1)T, uma passagem da MIB estendida para HSRP quando uma Bridge Group Virtual Interface (BVI) está presente causa um defeito no roteador.

[O ID de bug Cisco desse defeito é CSCdm61257 \(apenas clientes registrados\).](#)

Suporte HSRP para Virtual Private Networks de switching de rótulo multiprotocolo

O suporte HSRP para Virtual Private Networks de switching de rótulo multiprotocolo (MPLS VPNs) foi adicionado ao Cisco IOS versão 12.1(3)T.

O HSRP em uma interface MPLS VPN é útil quando existe um cabo Ethernet conectado entre dois Provider Edges (PEs) e você possui um dos seguintes:

- Um Edge de cliente (CE) com uma rota padrão para o endereço IP virtual de HSRP.
- Uns ou vários anfitriões com o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual HSRP configurado como o gateway padrão.

O diagrama de rede abaixo mostra dois PEs com HSRP em execução entre seus VPN de Routing/Forwarding (VRF) Interfaces. Configuramos o CE com o endereço IP virtual do HSRP como rota padrão. E configuramos o HSRP para rastrear as interfaces que conectam os PES ao restante da rede de provedor. Por exemplo, se a interface E1 ou PE1 falhar, a prioridade HSRP será reduzida de tal forma que o PE2 levará os pacotes de encaminhamento para o endereço IP/MAC virtual.

Estas são as configurações:

Roteador PE1	Roteador PE2
<pre>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</pre>	<pre>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</pre>

Você pode usar os seguintes comandos para verificar se o endereço IP virtual HSRP está no ARP VRF correto e nas tabelas do Cisco Express Forwarding:

```
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	

[Suporte de HSRP para redirecionamentos de ICMP](#)

O HSRP está baseado no conceito de que os roteadores peer que estão protegendo uma sub-rede podem fornecer acesso a todas as demais sub-redes que compõem a rede. Portanto, é irrelevante saber qual roteador se tornou o roteador HSRP ativo, pois todos os roteadores possuíam rotas para cada sub-rede.

O HSRP utiliza um endereço IP de Um ou Mais Servidores Cisco ICM NT e um endereço MAC virtual virtuais especiais, que sejam anexados logicamente ao roteador ativo HSRP. Os redirecionamentos ICMP são desativados automaticamente em uma interface quando utilizam HSRP nessa interface. Os IO 12.1(3)T avante, característica dos redirecionamentos de ICMP permitem redirecionamentos de ICMP nas relações configuradas com HSRP. Refira o [Suporte HSRP para ICM Redirects](#) para mais detalhes. Isso é feito para evitar que os hosts sejam redirecionados para longe do endereço IP virtual do HSRP. É possível que os dois (ou mais) roteadores de uma sub-rede não tenham conectividade idêntica à do restante da rede. Isto é, para um endereço IP de destino específico, um roteador ou o outro deve ter um caminho muito melhor até aquele endereço ou pode até mesmo ser o único roteador conectado àquele endereço.

O protocolo ICMP permite que um roteador redirecione uma estação final para enviar pacotes de um determinado destino para outro roteador na mesma sub-rede. Isto se o primeiro roteador souber que o outro roteador tem um caminho melhor para aquele destino em particular. Como foi no caso dos gateways padrão, se o roteador ao qual uma estação final foi redirecionada para um destino específico falhar, pacotes da estação final para aquele destino não foram entregues. Em HSRP padrão, é exatamente isto o que acontece. Por essa razão, recomendamos desativar os redirecionamentos de ICMP se o HSRP estiver ativado.

Estender o relacionamento entre redirecionamentos de ICMP e HSRP fornece uma solução a este problema, permitindo que você aproveite-se dos benefícios do HSRP e dos redirecionamentos de ICMP. Dois (ou mais) grupos de HSRP são executados em cada sub-rede, com pelo menos o mesmo número de grupos de HSRP configurados que o de roteadores participantes. As prioridades são configuradas de forma que os roteadores sejam mestres de pelo menos um grupo de HSRP. Quando um roteador determina reorientar uma estação final a um roteador diferente para um destino específico, a seguir em vez de reorientar a estação final ao endereço IP de Um ou Mais Servidores Cisco ICM NT desse outro roteador, encontra que um grupo HSRP que esteja sendo dominado por esse roteador, e reorienta a estação final ao endereço IP de Um ou Mais Servidores Cisco ICM NT virtual correspondente. Se o roteador de destino falhar, o HSRP assegura que outro roteador assumirá sua função e talvez redirecione a estação final para outro roteador também virtual.

[Interface HSRP e suporte de mídia](#)

Esta seção explica que relações e apoios dos media HSRP, e possíveis advertências ao executar o HSRP sobre estes media.

Desde o Cisco IOS Software Release 10.0, a funcionalidade de HSRP esteve disponível em Ethernet, em Token Ring e em Fiber Distributed Data Interface (FDDI). Interfaces Fast Ethernet e ATM também são suportadas pelo HSRP.

LANs Virtuais (VLANs) permitem que as topologias de redes lógicas se sobreponham à infraestrutura comutada física de tal modo que qualquer grupo arbitrário de portas de LAN possa ser combinado em um grupo de usuários autônomos ou comunidade de interesses. O suporte de VLAN HSRP foi adicionado no Cisco IOS Release 11.1 para o Secure Data Exchange do IEEE 802.10 (SDE), e no Cisco IOS Release 11.3 para o Cisco Inter-Switch Link (ISL).

[Ethernet](#)

Diversos controladores Ethernet (Lance e QUICC) em produtos low-end podem ter somente um único endereço MAC de envio único em seu filtro de endereço. Nessas plataformas, é permitido somente um grupo de HSRP, e o endereço da interface é alterado para endereço MAC virtual de HSRP quando o grupo fica Ativo. Caso esteja utilizando HSRP em roteadores com diversas interfaces desse tipo, você deve configurar cada interface com um número de grupo HSRP diferente.

Note: O roteador Cisco 7200 também utiliza o controlador Lance Ethernet, mas suporta MHSRP no software.

A Cisco recomenda que você tenha não mais do que 24 Processadores de Interface Ethernet HSRP (EIPs) devido ao tempo que demora para atualizar os filtros de endereço para o HSRP. Mais de vinte e quatro HSRP EIPs podem causar instabilidade e carga excessiva para a CPU.

Este defeito tem a identificação de bug Cisco [CSCdj29595](#) ([clientes registrados somente](#)).

Se você tem mais de twenty-four EIP, tente substituir os EIP com o Versatile Interface Processors (VIP) e os adaptadores de porta Ethernet. Os VIPs foram aprovados para até oitenta grupos HSRP. Você pode igualmente reduzir os números de grupo de hsrp, e aumenta o HSRP hello e o tempo de contenção.

[Token Ring](#)

Uma limitação de executar o HSRP em uma interface de token ring é que você não pode reprogramar o filtro de endereço no chipset do Token Ring a mesma maneira que você pode em Ethernet, FDDI ou emulação de ATM. O Token Ring usa os endereços funcionais, de que há somente um número pequeno disponível que não opõem a outros usos do espaço de endereço funcional.

Ao executar o HSRP em um ambiente de Source-Route Bridging (SRB), o uso de endereços funcionais pode causar confusão de RIF. [Consulte a seção HSRP Addressing para obter mais informações](#). Também, tente configurar o **comando use-bia**.

[802.1Q](#)

Cisco recomenda usar o Cisco IOS Software Release 12.0(8.1)T ou Mais Recente para o HSRP

sobre o 802.1Q.

ISL

O HSRP sobre ISL está disponível nas versões 11.2(6)F, 11.3 e 12.X do Cisco IOS. É recomendável usar a versão 12.0(7) ou posterior para evitar o problema descrito na identificação de bug Cisco CSCdm68811 (somente clientes [registrados](#)).

FDDI

Um adaptador de porta FDDI retira quadros do anel se perceber que um de seus próprios endereços MAC está localizado na fonte MAC. Se um evento de rede faz com que ambos os roteadores vá active, a seguir ambos os roteadores envia pacotes do HSRP hello com o mesmo endereço MAC virtual. Cada roteador retira erroneamente o pacote de saudação do outro roteador da rede e ambos permanecem ativos.

Esse defeito possui a ID Cisco ID CSCdj30049 (somente para clientes [registrados](#)).

A solução desse problema no Cisco IOS versão 11.2(11.1) é para que roteadores HSRP em um ambiente FDDI possam utilizar seu próprio Endereço MAC exclusivo de operação antecipada exclusivo para trocar mensagens e executar o protocolo HSRP. Para assegurar-se de que os bridges de aprendizagem e o Switches ponham em esconderijo a entrada de porta correta para o endereço MAC virtual, o roteador ativo igualmente envia mensagens de atualização periódicos usando o MAC address HSRP.

Note: A memória de conteúdo endereçável (CAM) do hardware do roteador Cisco 4500 em uma interface FDDI talvez não seja preenchida corretamente depois de uma recarga caso você tenha configurado várias redes RIP e grupos de HSRP. A única ação alternativa é neste tempo cancelar as relações para restaurar o CAM. Este defeito apresenta o ID de bug Cisco CSCdm93122 (somente para clientes [registrados](#)).

Atualização de MAC

Os roteadores de HSRP em um ambiente FDDI usam seu próprio endereço MAC de operação antecipada exclusivo aos mensagens de intercâmbio e executam o protocolo de HSRP. Para assegurar que os bridges de aprendizagem e o Switches põem em esconderijo a entrada de porta correta para o endereço MAC virtual o roteador ativo igualmente envia mensagens de atualização periódicos usando o MAC address HSRP. Esse defeito possui a ID Cisco ID CSCdj30049 (somente para clientes [registrados](#)).

Se você não tem um interruptor ou um bridge de aprendizagem em sua rede, você pode desabilitar a emissão de refresca pacotes como mostrado abaixo:

```
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	

[Grupo virtual de interface de ponte](#)

O suporte de HSRP a BVIs (Bridge Group Virtual Interfaces, Grupos virtuais de interface de ponte) foi adicionado no Cisco IOS versão 12.0(6.2)T.

[Subinterfaces](#)

Grupos HSRP em subinterfaces devem ter um número de grupo exclusivo entre todos os outros grupos em todas as subinterfaces na mesma interface principal. Isto é porque as subinterfaces não recebem um índice de interface snmp original. Se houvesse dois grupos com o número N em diferentes sub-interfaces, o grupo N da sub-interface 1 e o grupo N da sub-interface 2 pareceriam ser o mesmo grupo, no MIB.

[Informações Relacionadas](#)

- [Página de suporte de HSRP](#)
- [HSRP - FAQ](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)