

Comprendere le funzionalità e le caratteristiche del protocollo del router in standby a caldo

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Sfondo e operazioni HSRP](#)

[Meccanismi di rilevamento dinamico del router](#)

[Protocollo Proxy Address Resolution](#)

[Dynamic Routing Protocol](#)

[Protocollo ICMP Router Discovery](#)

[Protocollo Dynamic Host Configuration](#)

[Funzionamento HSRP](#)

[Indirizzamento del protocollo HSRP](#)

[Matrice delle funzionalità di Cisco IOS® release e HSRP](#)

[Funzionalità Cisco IOS HSRP](#)

[Funzionalità del protocollo HSRP](#)

[Modalità di prelazione](#)

[Ritardo per diritti di priorità](#)

[Tracciamento dell'interfaccia](#)

[Usa indirizzo incorporato](#)

[Gruppi HSRP molteplici](#)

[Indirizzo MAC configurabile](#)

[Supporto Syslog](#)

[Debug HSRP](#)

[Debug HSRP avanzato](#)

[Autenticazione](#)

[Ridondanza IP](#)

[Base informazioni gestione SNMP](#)

[Supporto HSRP per reti private virtuali di switching etichette multiprotocollo](#)

[Supporto HSRP per reindirizzamenti ICMP](#)

[Supporto interfaccia e supporti HSRP](#)

[Ethernet](#)

[Token Ring](#)

[802.1Q](#)

[ISL](#)

[FDDI](#)

[Aggiornamento MAC](#)

[Bridge Group Virtual Interface](#)

[Sottointerfacce](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il funzionamento e la revisione del protocollo HSRP (Hot Standby Router Protocol).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

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

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Sfondo e operazioni HSRP

Un modo per ottenere un tempo di attività della rete pari a quasi il 100% è utilizzare l'HSRP, che fornisce ridondanza per le reti IP e garantisce che il traffico degli utenti recuperi immediatamente e in modo trasparente i guasti del primo hop nei dispositivi periferici della rete o nei circuiti di accesso.

Quando due o più router condividono un indirizzo IP e un indirizzo MAC (layer 2), possono fungere da router "virtuale" singolo. I membri del gruppo di router virtuali si scambiano continuamente messaggi di stato. In questo modo, un router può assumersi la responsabilità di routing di un altro router se uno dei due non è in servizio per motivi pianificati o non pianificati. Gli host continuano a inoltrare i pacchetti IP a un indirizzo IP e MAC coerente e la sostituzione dei dispositivi che eseguono il routing è trasparente.

Meccanismi di rilevamento dinamico del router

Vengono descritti i meccanismi dinamici di rilevamento dei router disponibili per gli host. Molti di questi meccanismi non forniscono la resilienza della rete richiesta dagli amministratori di rete. Ciò può verificarsi quando il protocollo non è stato inizialmente progettato per fornire resilienza di rete o perché non è possibile per ogni host in una rete eseguire il protocollo. Oltre a quanto elencato, è

importante notare che molti host consentono solo di configurare un gateway predefinito.

Protocollo Proxy Address Resolution

Alcuni host IP utilizzano il protocollo ARP (Proxy Address Resolution Protocol) per selezionare un router. Quando un host esegue ARP proxy, invia una richiesta ARP per l'indirizzo IP dell'host remoto che desidera contattare. Un router A sulla rete risponde per conto dell'host remoto e fornisce il proprio indirizzo MAC. Con il proxy ARP, l'host si comporta come se l'host remoto fosse connesso allo stesso segmento della rete. Se il router A ha esito negativo, l'host continua a inviare i pacchetti destinati all'host remoto all'indirizzo MAC del router A, anche se questi pacchetti non hanno alcun percorso da cui andare e vengono persi. È possibile attendere che ARP acquisisca l'indirizzo MAC di un altro router, il router B, sul segmento locale che invia un'altra richiesta ARP oppure riavviare l'host per forzarlo a inviare una richiesta ARP. In entrambi i casi, per un periodo di tempo significativo, l'host non può comunicare con l'host remoto, anche se il protocollo di routing è convergente, e il router B è pronto a trasferire pacchetti che altrimenti passerebbero attraverso il router A.

Dynamic Routing Protocol

Alcuni host IP eseguono (o eseguono lo snoop) un protocollo di routing dinamico, ad esempio RIP (Routing Information Protocol) o OSPF (Open Shortest Path First) per l'individuazione dei router. Lo svantaggio dell'utilizzo di RIP è rappresentato dalla lentezza con cui si adatta alle modifiche della topologia. L'esecuzione di un protocollo di routing dinamico su ogni host non è una soluzione pratica per diversi motivi, oltre che per il sovraccarico amministrativo. processing sovraccarico, problemi di sicurezza o mancata implementazione di un protocollo per alcune piattaforme.

Protocollo ICMP Router Discovery

In alcuni host IP più recenti, il protocollo IRDP (RFC 1256) (ICMP Router Discovery Protocol) viene utilizzato per trovare un nuovo router quando una route non è disponibile. Un host che esegue IRDP resta in ascolto dei messaggi hello multicast dal router configurato e utilizza un router alternativo quando non riceve più tali messaggi hello. I valori predefiniti del timer per IRDP indicano che non è adatto al rilevamento di errori del primo hop. La frequenza predefinita degli annunci è una volta ogni 7-10 minuti e la durata predefinita è 30 minuti.

Protocollo Dynamic Host Configuration

Il protocollo DHCP (Dynamic Host Configuration Protocol) ([RFC 1531](#)) fornisce un meccanismo per passare le informazioni di configurazione agli host su una rete TCP/IP. Un host che esegue un client DHCP richiede le informazioni di configurazione a un server DHCP all'avvio in rete. Queste informazioni di configurazione in genere includono un indirizzo IP e un gateway predefinito. Non è disponibile alcun meccanismo per passare a un router alternativo in caso di errore del gateway predefinito.

Funzionamento HSRP

Un'ampia classe di implementazioni host legacy che non supporta l'individuazione dinamica può configurare un router predefinito. Per diversi motivi, non è possibile eseguire un meccanismo di rilevamento dinamico dei router su ogni host, oltre che per un sovraccarico amministrativo. processing sovraccarico, problemi di sicurezza o mancanza di un'implementazione del protocollo per

alcune piattaforme. HSRP fornisce servizi di failover a questi host.

Quando si utilizza l'HSRP, un gruppo di router lavora in concerto per presentare l'illusione di un singolo router virtuale agli host della LAN. Questo set è noto come gruppo HSRP o gruppo in standby. Un singolo router scelto dal gruppo è responsabile della distribuzione dei pacchetti che gli host inviano al router virtuale. Questo è il router attivo, mentre un altro router viene scelto come router di standby. In caso di guasto del router attivo, lo standby presume che il pacchetto forwarding dei compiti del router attivo. Sebbene un numero arbitrario di router possa eseguire l'HSRP, solo il router attivo inoltra i pacchetti inviati al router virtuale.

Per ridurre al minimo il traffico di rete, solo i router attivi e in standby inviano messaggi HSRP periodici una volta che il protocollo ha completato il processo di selezione. Se sul router attivo si verifica un errore, il router di standby lo sostituisce, diventando a sua volta attivo. Se il router in standby si guasta o diventa il router attivo, viene scelto un altro router come router in standby.

Su una LAN specifica, è possibile che più gruppi hot standby coesistano e si sovrappongano. Ogni gruppo in standby emula un singolo router virtuale. I singoli router possono partecipare a più gruppi. In questo caso, il router mantiene timer e stati separati per ciascun gruppo. Ogni gruppo in standby ha un indirizzo MAC noto e uno singolo, oltre a un indirizzo IP.

Indirizzamento del protocollo HSRP

Nella maggior parte dei casi, quando si configurano i router per far parte di un gruppo HSRP, questi rimangono in ascolto dell'indirizzo MAC HSRP per tale gruppo e del proprio indirizzo MAC masterizzato. Ad eccezione dei router i cui controller Ethernet riconoscono solo un indirizzo MAC, ad esempio il controller Lance sui router Cisco 2500 e Cisco 4500. Questi router utilizzano l'indirizzo MAC HSRP quando sono il router attivo e il loro indirizzo masterizzato quando non lo sono.

HSRP utilizza questo indirizzo MAC su tutti i supporti tranne Token Ring:

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

Le interfacce Token Ring usano indirizzi funzionali per l'indirizzo MAC HSRP. Gli indirizzi funzionali sono l'unico meccanismo multicast generale disponibile. Sono disponibili un numero limitato di indirizzi funzionali Token Ring e molti di essi sono riservati per altre funzioni. Con HSRP è possibile utilizzare i tre indirizzi seguenti:

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

Nota: Quando HSRP viene eseguito in un ambiente SRB (Source-Route Bridging) a più anelli e i router HSRP risiedono in anelli diversi e utilizzano gli indirizzi funzionali, è possibile che si creino confusione nel campo RIF (Routing Information Field). Ad esempio, in un ambiente SRB, è possibile che un router in standby HSRP risieda su un anello diverso rispetto al router attivo.

Quando il router di standby diventa attivo, le stazioni sullo stesso anello del vecchio router attivo hanno bisogno di un nuovo RIF per inviare i pacchetti al nuovo router attivo. Tuttavia, poiché il router di standby (nuovo router attivo) usa lo stesso indirizzo funzionale del router attivo

precedente, le stazioni non sono a conoscenza del fatto che devono inviare gli elenchi di cartelle per un nuovo RIF. Per questo motivo, è stato introdotto il comando [use-bia](#).

Matrice delle funzionalità di Cisco IOS® release e HSRP

In questo documento viene illustrato quali funzionalità HSRP sono supportate nelle diverse versioni del software Cisco IOS. Fate clic su una feature per visualizzare una descrizione dettagliata. Un numero di versione provvisorio indica in quale release è apparsa per la prima volta una feature o in quale release è cambiata la funzionalità di tale feature.

Funzionalità	10.0	10.2	10.3	11.0	11.1	11.2	11.3	12.0	12,0 T	12.1	12,1T
Modalità di prelazione	X	X	X	X	X	X	X	X	X	X	X
MHSRP (Multiple Groups)	—	—	X	X	X	X	X	X	X	X	X
Ethernet 802.10 SDE	—	—	—	—	X	X	X	X	X	X	X
Interfaccia Tracking	—	—	—	—	X	X	X	X	X	X	X
Utilizza BIA	—	—	—	—	8.0	X	X	X	X	X	X
Ritardo per diritti di priorità	—	—	—	—	—	X	X	6.1	X	X	X
LANE Ethernet	—	—	—	—	—	X	X	X	X	X	X
Token Ring LANE	—	—	—	—	—	—	X	X	X	X	X
ISL	—	—	—	—	—	—	X	X	X	X	X
Supporto Syslog	—	—	—	—	—	—	X	X	X	X	X
Intervallo aggiornamento MAC	—	—	—	—	—	—	—	1.0	X	X	X
MIB SNMP	—	—	—	—	—	—	—	—	3.0	X	X
MHSRP e utilizzo di BIA	—	—	—	—	—	—	—	—	3.4	X	X
Ridondanza IP	—	—	—	—	—	—	—	—	3.4	X	X
BVI	—	—	—	—	—	—	—	—	6.2	X	X
802.1Q	—	—	—	—	—	—	—	—	8.1	X	X
Debug HSRP avanzato	—	—	—	—	—	—	—	—	—	0.2	X
Reindirizzamenti ICMP HSRP	—	—	—	—	—	—	—	—	—	—	3
HSRP MPLS VPN	—	—	—	—	—	—	—	—	—	—	3

Funzionalità Cisco IOS HSRP

Funzionalità del protocollo HSRP

Modalità di prelazione

La funzionalità di interruzione per diritti di priorità HSRP consente al router con la priorità più alta di diventare immediatamente il router attivo. La priorità viene determinata innanzitutto dal valore di priorità configurato e quindi dall'indirizzo IP. In ogni caso, un valore più alto ha una priorità maggiore. Quando un router con priorità più alta ha priorità più alta su un router con priorità più bassa, invia un messaggio di colpo di stato. Quando un router attivo con priorità inferiore riceve un messaggio di colpo di stato o di saluto da un router attivo con priorità superiore, passa allo stato di parlato e invia un messaggio di rifiuto.

Ritardo per diritti di priorità

La funzione di ritardo per diritti di priorità consente di ritardare l'interruzione per un periodo di tempo configurabile e permette al router di popolare la relativa tabella di routing prima di diventare

il router attivo.

Prima della versione software Cisco IOS 12.0(9), il ritardo iniziava quando il router veniva ricaricato. In Cisco IOS versione 12.0(9), il ritardo inizia al primo tentativo di interruzione per diritti di priorità.

Per configurare la priorità e l'interruzione per diritti di priorità dell'HSRP, utilizzare il comando `standby [group] [prioritynumber] [preempt [delay [minimum]seconds] [syncseconds]]`. Per ulteriori informazioni, consultare la [documentazione dell'HSRP](#).

Interfaccia Tracking

Interfaccia `tracking` consente di specificare un'altra interfaccia sul router da monitorare sul processo HSRP per modificare la priorità HSRP di un determinato gruppo.

Se il protocollo di linea specificato dell'interfaccia non è attivo, la priorità HSRP di questo router viene ridotta e consente l'attivazione di un altro router HSRP con priorità più alta (se l'[interruzione per diritti di priorità è abilitata](#)).

Per configurare l'interfaccia HSRP `tracking`, usare il comando `standby [group] track interface [priority]`.

Nota: La disponibilità del comando Interface Track può dipendere dalla versione del software in uso, ma è possibile usare il comando `standby [group] track [object]`.

Quando più interfacce tracciate sono inattive, la priorità viene ridotta di un importo cumulativo. Se si imposta esplicitamente il valore di decremento, tale valore viene diminuito di tale importo se l'interfaccia è inattiva e i decrementi sono cumulativi. Se non si imposta un valore di decremento esplicito, il valore viene diminuito di 10 per ogni interfaccia che scende e i decrementi vengono cumulati.

In questo esempio viene utilizzata questa configurazione con il valore di decremento predefinito 10:

Nota: Se non viene specificato un numero di gruppo HSRP, il numero di gruppo predefinito è il gruppo 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
```

Il comportamento di HSRP con questa configurazione è:

- 0 interfacce verso il basso = nessuna diminuzione (la priorità è 110)
- 1 interfaccia verso il basso = diminuisce di 10 (la priorità diventa 100)
- 2 interfacce verso il basso = diminuisce di 10 (la priorità diventa 90)

Il precedente comportamento HSRP è true anche se i valori di decremento sono configurati esplicitamente come:

```
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
```

Prima della versione 12.1 di Cisco IOS, se si avvia un router con un'interfaccia down, usare l'interfaccia HSRP `tracking` considera l'interfaccia attiva.

Usa indirizzo incorporato

La funzionalità di utilizzo dell'indirizzo incorporato (BIA) consente ai gruppi HSRP di utilizzare un indirizzo MAC incorporato dell'interfaccia anziché un indirizzo MAC HSRP. L'uso di BIA è stato implementato per la prima volta in Cisco IOS versione 11.1(8). Per configurare l'HSRP in modo che utilizzi il comando [BIA \(standby use-bia\) \[scope interface\]](#).

Il comando **use-bia** è stato implementato per superare le limitazioni quando si usa un indirizzo funzionale per l'indirizzo MAC HSRP sulle interfacce Token Ring.

Nota: Quando HSRP viene eseguito in un ambiente con bridging con routing di origine a più anelli e i router HSRP risiedono in anelli diversi e utilizzano gli indirizzi funzionali, è possibile che si creino confusione nel campo RIF (Routing Information Field). Per questo motivo, è stato introdotto il comando **use-bia**.

La funzionalità **use-bia** consente anche l'uso di DECnet, Xerox Network Systems (XNS) e HSRP sullo stesso router tramite l'indirizzo MAC DECnet (BIA) da usare come indirizzo MAC HSRP. Il comando **use-bia** è utile anche per le reti in cui il BIA del dispositivo è stato configurato in altri dispositivi sulla LAN.

Tuttavia, il comando **use-bia** ha diversi svantaggi:

- Quando un router diventa attivo, l'indirizzo IP virtuale viene spostato su un indirizzo MAC diverso. Il router appena attivo invia una risposta ARP gratuita, ma non tutte le implementazioni host gestiscono correttamente l'ARP gratuito.
- L'ARP del proxy si interrompe quando viene configurato **use-bia**. Un router in standby non è in grado di coprire la perdita del database ARP del proxy di un router in errore.
- Nelle versioni precedenti a Cisco IOS versione 12.0(3.4)T, è consentito un solo gruppo HSRP se è configurato **use-bia**.

Quando si configura il comando **use-bia** su una sottointerfaccia, questo viene visualizzato sull'interfaccia principale e viene applicato a tutte le sottointerfacce. In Cisco IOS versione 12.0(6.2) e successive, il comando **use-bia** viene esteso con le parole chiave opzionali dell'interfaccia dell'ambito per consentirne l'applicazione a una singola sottointerfaccia.

Gruppi HSRP molteplici

La funzionalità per più gruppi HSRP (MHSRP) è stata aggiunta in Cisco IOS versione 10.3. Questa funzionalità migliora ulteriormente la ridondanza e la condivisione del carico all'interno delle reti e consente un utilizzo più completo dei router ridondanti. Mentre un router inoltra attivamente il traffico per un gruppo HSRP, può essere in standby o in stato di ascolto per un altro gruppo.

A partire dalla versione Cisco IOS 12.0(3.4)T, è possibile usare il comando **use-bia** con più gruppi HSRP abilitati. Per configurare HSRP e utilizzare più percorsi, fare riferimento a [Condivisione del carico con HSRP](#).

Indirizzo MAC configurabile

Normalmente si usa l'HSRP per aiutare le stazioni terminali a individuare il primo gateway hop per il routing IP. Le stazioni terminali sono configurate con un gateway predefinito. Tuttavia, HSRP può fornire la ridondanza del primo hop per altri protocolli. Alcuni protocolli, ad esempio Advanced Peer-to-Peer Networking (APPN), utilizzano l'indirizzo MAC per identificare il primo hop per il routing.

In questo caso, spesso è necessario essere in grado di specificare l'indirizzo MAC virtuale che utilizza il comando [mac-address di standby](#). L'indirizzo IP virtuale non è importante per questi protocolli. La sintassi effettiva del comando è **standby [group] mac-address mac-address** .

Nota: non è possibile usare questo comando su un'interfaccia Token Ring.

Supporto Syslog

Supporto per syslog messaging per HSRP sono state aggiunte informazioni in Cisco IOS versione 11.3. Questa funzione consente logging e tracking dei router attivi e in standby correnti sui server syslog.

Debug HSRP

Prima della versione 12.1 di Cisco IOS, il comando di debug HSRP era relativamente semplice. Per abilitare il debug HSRP, è sufficiente utilizzare il comando [debug standby](#), che abilita l'output dello stato HSRP e le informazioni sui pacchetti per tutti i gruppi in standby su tutte le interfacce.

In Cisco IOS versione 12.0(2.1) è stata aggiunta una condizione di debug che consente di filtrare l'output del comando **standby debug** in base al numero di interfaccia e di gruppo. Il comando utilizza il paradigma della **condizione di debug** introdotto in Cisco IOS versione 12.0, come segue: [gruppo di interfacce di standby della condizione di debug](#). L'interfaccia specificata deve essere valida e in grado di supportare HSRP. Il gruppo può essere qualsiasi gruppo (0 - 255).

È possibile impostare le condizioni di debug per i gruppi che non esistono, in modo da acquisire le informazioni di debug durante l'inizializzazione di un nuovo gruppo.

Per produrre qualsiasi output di debug, è necessario abilitare l'ordine di **debug in standby**. Se non si configura alcuna condizione di **debug in standby**, l'output del comando debug viene prodotto per tutti i gruppi su tutte le interfacce. Se si configura almeno una condizione di **debug in standby**, l'output del **debug in standby** viene filtrato in base a tutte le condizioni di **debug in standby**.

Debug HSRP avanzato

Prima della versione 12.1(0.2) di Cisco IOS, il debug HSRP aveva un'utilità limitata in quanto le informazioni venivano perse nei messaggi di saluto periodici. Pertanto, la funzionalità di debug avanzata è stata aggiunta in Cisco IOS 12.1(0.2).

Nella tabella vengono illustrate le opzioni dei comandi per il debug avanzato.

Comando	Descrizione
debug standby	Visualizza tutti gli errori, gli eventi e i pacchetti HSRP.
debug standby	Visualizza tutti gli errori, gli eventi e i pacchetti HSRP, eccezione dei pacchetti hello e annuncio.
debug standby errors	Visualizza gli errori HSRP.
debug standby events [all terse] [icmp] protocollo redundancy track]] [detail]	Visualizza gli eventi HSRP.
debug standby packets [[all] terse] [advertise coup hello resign]] [detail]	Visualizza i pacchetti HSRP.

È possibile filtrare l'output di **debug** con l'interfaccia e il debug condizionale del gruppo HSRP. Per abilitare il debug condizionale dell'interfaccia, utilizzare il comando **debug condition interface **. Per abilitare il debug condizionale HSRP, utilizzare il comando **debug condition standby interface group**.

Una condizione di debug dell'interfaccia si applica solo quando non è stata impostata alcuna condizione di **debug in standby**. Il debug HSRP è stato ulteriormente migliorato nel software Cisco IOS versione 12.1(1.3), in base ai miglioramenti apportati alla tabella di stato HSRP.

Questi miglioramenti consentono di visualizzare gli eventi della tabella di stato HSRP. Nell'output **a/**, **b/**, **c/** e così via, fare riferimento agli eventi della macchina a stati finiti HSRP, documentati [nella 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 (10.0.0.3)
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
```

Autenticazione

La funzionalità di autenticazione HSRP è costituita da una chiave non crittografata condivisa contenuta nei pacchetti HSRP. Questa funzione impedisce al router con priorità inferiore di learning l'indirizzo IP di standby e i valori del timer di standby del router con priorità più alta.

Per configurare la stringa di autenticazione HSRP, utilizzare il comando [standby authentication <string>](#).

Ridondanza IP

HSRP fornisce ridondanza stateless per il routing IP. L'HSRP da solo può mantenere solo il proprio stato. Presuppone che ogni router costruisca e gestisca le proprie tabelle di routing indipendentemente dagli altri router. La funzionalità di ridondanza IP fornisce un meccanismo che consente a HSRP di fornire un servizio alle applicazioni client in modo che possano implementare

il failover stateful.

La ridondanza IP non fornisce un meccanismo per lo scambio di informazioni sullo stato tra applicazioni peer. Questa operazione è riservata alle applicazioni stesse ed è essenziale se le applicazioni devono fornire failover stateful.

La ridondanza IP viene in genere implementata solo per gli agenti Home IP mobili. Ecco un esempio di configurazione:

```
configure terminal
router mobile
ip mobile home-agent standby hsrp-group1
!
interface e0/2
no shutdown
ip address 10.0.0.1 255.0.0.0
standby 1 ip 10.0.0.11
standby 1 name hsrp-group1
```

Nota: A partire dalla versione 12.1(3)T di Cisco IOS, oltre alla parola chiave **standby** viene accettata la **ridondanza**. la parola chiave **standby** viene eliminata in una versione più recente di Cisco IOS. Il comando corretto è [ip mobile home-agent redundancy hsrp-group1](#).

Gli utilizzi futuri della ridondanza IP includono:

- NAT - Necessità di fornire gateway ridondanti.
- IPSEC - Necessità di sincronizzare le informazioni sullo stato per poter operare quando HSRP è in uso.
- Server DHCP - Server DHCP implementati in vari router.
- NBAR, CBAC - È necessario eseguire il mirroring degli stati del firewall per il routing asimmetrico.
- GPRS - È necessario un modo per tenere traccia dello stato TCP.

Base informazioni gestione SNMP

Il supporto MIB (Management Information Base) SNMP è stato aggiunto a Cisco IOS versione 12.0(3.0)T. Esistono due MIB rilevanti per l'HSRP:

- ciscoMgmt 106: Modulo MIB utilizzato per gestire HSRP
- ciscoMgmt 107: Modulo MIB di estensione utilizzato per gestire HSRP

Nelle versioni precedenti a Cisco IOS versione 12.0(6.1)T, se è presente un'interfaccia virtuale del gruppo di bridge (BVI), il router si blocca a causa di una presentazione del MIB dell'HSRP esteso.

Supporto HSRP per reti private virtuali di switching etichette multiprotocollo

Il supporto HSRP per Multiprotocol Label Switching Virtual Private Network (MPLS VPN) è stato aggiunto in Cisco IOS versione 12.1(3)T.

L'opzione HSRP su un'interfaccia VPN MPLS è utile quando è presente una rete Ethernet connessa tra due provider Edge (PE) e si dispone di una delle opzioni seguenti:

- A Customer Edge (CE) con un percorso predefinito all'indirizzo IP virtuale HSRP.
- Uno o più host con l'indirizzo IP virtuale HSRP configurato come gateway predefinito.

Nel diagramma di rete sono illustrati due PE con HSRP in esecuzione tra le rispettive VPN routing/forwarding (VRF). Il CE con l'indirizzo IP virtuale HSRP è configurato come percorso predefinito. HSRP è configurato per tenere traccia delle interfacce che connettono i PE al resto della rete del provider. Ad esempio, se l'interfaccia E1 di PE1 ha esito negativo, la priorità HSRP viene ridotta in modo che PE2 assuma il controllo forwarding all'indirizzo IP/MAC virtuale.

Ecco le configurazioni:

Router PE1

```

configure 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

```

PE2 router

```

configure 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

```

È possibile utilizzare i comandi successivi per verificare che l'indirizzo IP virtuale HSRP sia nel VRF ARP corretto e in Cisco Express Forwarding tabelle:

```
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	

Supporto HSRP per reindirizzamenti ICMP

L'HSRP si basa sul concetto che i router peer HSRP che proteggono una subnet possono fornire accesso a tutte le altre subnet della rete. Pertanto, non è rilevante quale router diventi il router HSRP attivo, in quanto tutti i router disponevano di percorsi a ciascuna subnet.

HSRP utilizza un indirizzo IP virtuale speciale e un indirizzo MAC virtuale, che sono collegati

logicamente al router attivo HSRP. I reindirizzamenti ICMP vengono disabilitati automaticamente su un'interfaccia quando su tale interfaccia viene utilizzato HSRP. A partire da Cisco IOS 12.1(3)T, la funzionalità di reindirizzamento ICMP abilita i reindirizzamenti ICMP sulle interfacce configurate con HSRP. per ulteriori informazioni, fare riferimento al [supporto HSRP per i reindirizzamenti ICMP](#). In questo modo si impedisce agli host di eseguire il reindirizzamento lontano dall'indirizzo IP virtuale HSRP. È possibile che i due (o più) router di una subnet non abbiano la stessa connettività al resto della rete. Vale a dire che, per un particolare indirizzo IP di destinazione, uno dei router può avere un percorso molto migliore per quell'indirizzo o può anche essere l'unico router collegato a quell'indirizzo.

Il protocollo ICMP consente a un router di reindirizzare un'endpoint per inviare i pacchetti di una determinata destinazione a un altro router della stessa subnet, a condizione che il primo router sia a conoscenza del fatto che l'altro router ha un percorso migliore verso quella determinata destinazione. Come nel caso dei gateway predefiniti, se il router a cui è stata reindirizzata un'unità terminale per una determinata destinazione ha esito negativo, i pacchetti dell'unità terminale verso tale destinazione non vengono consegnati. In HSRP standard, questo è esattamente ciò che accade. Per questo motivo, si consiglia di disabilitare i reindirizzamenti ICMP se HSRP è attivato.

Quando si estende la relazione tra i reindirizzamenti ICMP e HSRP, viene fornita una soluzione al problema che consente di sfruttare i vantaggi dei reindirizzamenti sia HSRP che ICMP. In ogni subnet vengono eseguiti due o più gruppi HSRP, con un numero di gruppi HSRP configurato almeno pari al numero di router partecipanti. Le priorità sono configurate in modo che ogni router sia il router principale per almeno un gruppo HSRP. Quando un router determina di reindirizzare un'endpoint a un router diverso per una destinazione specifica, anziché reindirizzare l'endpoint all'indirizzo IP dell'altro router, trova un gruppo HSRP con quel router come router primario e reindirizza l'endpoint all'indirizzo IP virtuale corrispondente. Se il router di destinazione si guasta, l'HSRP assicura che un altro router subentri al suo lavoro e forse reindirizzi l'endpoint a un altro router virtuale.

Supporto interfaccia e supporti HSRP

In questa sezione vengono illustrate le interfacce e i supporti supportati da HSRP e vengono visualizzati avvisi quando si esegue HSRP su tali supporti.

Dal software Cisco IOS versione 10.0, la funzionalità HSRP è disponibile su Ethernet, Token Ring e Fiber Distributed Data Interface (FDDI). Anche le interfacce Fast Ethernet e ATM sono supportate da HSRP.

Le VLAN (Virtual LAN) consentono di sovrapporre le topologie di rete logiche all'infrastruttura fisica commutata in modo che qualsiasi insieme arbitrario di porte LAN possa essere combinato in un gruppo di utenti autonomo o in una comunità di interesse. Il supporto per VLAN HSRP è stato aggiunto in Cisco IOS versione 11.1 per IEEE 802.10 Secure Data Exchange (SDE) e in Cisco IOS versione 11.3 per Cisco Inter-Switch Link (ISL).

Ethernet

Diversi controller Ethernet (Lance e QUICC) nei prodotti di fascia bassa possono avere un solo indirizzo MAC unicast nel filtro indirizzi. In queste piattaforme è consentito un solo gruppo HSRP e l'indirizzo di interfaccia viene modificato nell'indirizzo MAC virtuale HSRP quando il gruppo diventa Attivo. Se si utilizza HSRP su router con più interfacce di questo tipo, è necessario configurare ciascuna interfaccia con un numero di gruppo HSRP diverso.

Nota: Il router Cisco 7200 usa anche il controller Lance Ethernet, ma supporta MHSRP nel software.

Cisco consiglia di non avere più di ventiquattro HSRP Ethernet Interface Processor (EIP) a causa del tempo necessario per aggiornare i filtri degli indirizzi per HSRP. Se si dispone di più di ventiquattro EIP HSRP, è possibile che si verifichi un'instabilità e un carico eccessivo della CPU.

Se si hanno più di ventiquattro EIP, provare a sostituirli con processori di interfaccia versatile (VIP) e adattatori di porte Ethernet. I VIP sono stati approvati per un massimo di ottanta gruppi HSRP. È inoltre possibile ridurre il numero di gruppi HSRP e aumentare il tempo di saluto e di attesa.

Token Ring

Se si esegue HSRP su un'interfaccia Token Ring, non è possibile riprogrammare il filtro indirizzi sul chipset Token Ring nello stesso modo in cui lo si può fare su Ethernet, FDDI o emulazione ATM. Token Ring utilizza indirizzi funzionali, dei quali è disponibile solo un piccolo numero che non è in conflitto con altri usi dello spazio degli indirizzi funzionali.

Se si esegue HSRP in un ambiente Source-Route Bridging (SRB), l'utilizzo di indirizzi funzionali può causare confusione nel RIF. Per ulteriori informazioni, vedere la sezione [Indirizzamento HSRP](#). Provare anche a configurare il comando **use-bia**.

802.1Q

Cisco consiglia di utilizzare il software Cisco IOS versione 12.0(8.1)T o successive per HSRP over 802.1Q.

ISL

HSRP over ISL è disponibile nelle versioni 11.2(6)F, 11.3, 12.X di Cisco IOS. Si consiglia di utilizzare la versione 12.0(7) o successive.

FDDI

Un adattatore di porta FDDI rimuove i frame dall'anello se rileva uno dei propri indirizzi MAC nell'origine MAC. Se a causa di un evento di rete entrambi i router diventano attivi, entrambi i router inviano pacchetti Hello HSRP con lo stesso indirizzo MAC virtuale. Ogni router strappa per errore il pacchetto hello dell'altro router dalla rete e entrambi rimangono attivi.

La soluzione a questo problema in Cisco IOS versione 11.2(11.1) è che i router HSRP in ambiente FDDI usino il proprio indirizzo MAC univoco masterizzato per scambiare i messaggi ed eseguire il protocollo HSRP. Per garantire che `learning` I bridge e gli switch memorizzano nella cache la voce della porta corretta per l'indirizzo MAC virtuale. Il router attivo invia inoltre messaggi di aggiornamento periodici tramite l'indirizzo MAC dell'HSRP.

Nota: Se sono stati configurati più reti RIP e gruppi HSRP, non è possibile popolare correttamente dopo un ricaricamento la memoria CAM (Content-Indirissable Memory) hardware del router Cisco 4500 su un'interfaccia FDDI. L'unica soluzione a questo punto consiste nel cancellare le interfacce per ripristinare la CAM.

Aggiornamento MAC

I router HSRP in un ambiente FDDI utilizzano il proprio indirizzo MAC incorporato univoco per scambiare messaggi ed eseguire il protocollo HSRP. Per garantire che learning I bridge e gli switch memorizzano nella cache la voce corretta della porta per l'indirizzo MAC virtuale. Il router attivo invia inoltre messaggi di aggiornamento periodici tramite l'indirizzo MAC HSRP.

Se non si dispone di un interruttore o learning sulla rete, è possibile disabilitare la distribuzione dei pacchetti di aggiornamento come illustrato di seguito:

```
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
```

Bridge Group Virtual Interface

Il supporto HSRP per BVI (Bridge Group Virtual Interfaces) è stato aggiunto in Cisco IOS versione 12.0(6.2)T.

Sottointerfacce

I gruppi HSRP sulle sottointerfacce devono avere un numero di gruppo univoco tra tutti gli altri gruppi su tutte le sottointerfacce sulla stessa interfaccia principale. Infatti, le sottointerfacce non ricevono un indice di interfaccia SNMP univoco. Se si dispone di due gruppi con il numero N su sottointerfacce diverse, nel MIB il gruppo N sulla sottointerfaccia 1 e il gruppo N sulla sottointerfaccia 2 risulteranno essere lo stesso gruppo.

Informazioni correlate

- [Pagina di supporto per HSRP](#)
- [HSRP - Domande frequenti](#)

Informazioni su questa traduzione

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