Comprendre les fonctionnalités du protocole de routeur de secours automatique

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
HSRP - Informations générales et fonctionnement
Mécanismes de découverte de routeurs dynamiques
Protocole ARP (ou PARP)
Protocole de routage dynamique
Protocole de détection de routeur ICMP
Protocole de configuration d'hôte dynamique
Fonctionnement HSRP
Adressage HSRP
Matrice des versions de Cisco IOS® et des fonctionnalités HSRP
Fonctionnalité HSRP de Cisco IOS
Fonctionnalités HSRP
Préemption
Retard de préemption
Suivi d'interface
Adresse gravée en mémoire d'utilisation
Plusieurs groupes HSRP
Adresse MAC configurable
Prise en charge de Syslog
Débogage HSRP
Débogage amélioré de HSRP
Authentification
Redondance IP
SNMP Management Information Base
Support de HSRP pour Multiprotocol Label Switching Virtual Private Networks
Support HSRP pour redirections ICMP
Prise en charge des interfaces et des médias HSRP
Ethernet
Token Ring
802.1Q
Lien ISL
FDDI
Actualisation MAC
Bridge Group Virtual Interface

Sous-interfaces
Informations connexes

Introduction

Ce document décrit le fonctionnement du protocole HSRP (Hot Standby Router Protocol) et passe en revue ses fonctionnalités.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l’impact potentiel de toute commande./p>

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

HSRP - Informations générales et fonctionnement

Un moyen d'atteindre un temps de fonctionnement du réseau proche de 100 % est d'utiliser le protocole HSRP, qui assure la redondance du réseau pour les réseaux IP, et garantit que le trafic utilisateur récupère immédiatement et de manière transparente des pannes au premier saut dans les périphériques de périphérie du réseau ou les circuits d'accès.

Lorsque deux routeurs ou plus partagent une adresse IP et une adresse MAC (couche 2), ils peuvent agir comme un routeur « virtuel » unique. Les membres du groupe de routeurs virtuel échangent continuellement des messages d'état. De cette façon, un routeur peut assumer la responsabilité du routage d'un autre si un routeur est hors service pour des raisons planifiées ou non planifiées. Les hôtes continuent de transférer des paquets IP vers une adresse IP et MAC cohérente, et le basculement des périphériques qui effectuent le routage est transparent.

Mécanismes de découverte de routeurs dynamiques

Cette section décrit les mécanismes de détection dynamique des routeurs disponibles pour les hôtes. La plupart de ces mécanismes ne fournissent pas la résilience réseau requise par les administrateurs réseau. Cela peut se produire lorsque le protocole n’était pas initialement conçu pour fournir une résilience réseau ou parce qu’il n’est pas possible pour chaque hôte d’un réseau d’exécuter le protocole. En plus de ce qui est listé, il est important de noter que de nombreux

hôtes vous permettent seulement de configurer une passerelle par défaut.

Protocole ARP (ou PARP)

Quelques hôtes IP emploient le proxy Protocole de résolution d'adresse (ARP) pour sélectionner un routeur. Quand un hôte exécute le proxy ARP, il envoie une requête ARP pour l'adresse IP de l'hôte distant qu'elle veut contacter. Un routeur, Routeur A, sur le réseau répond au nom de l'hôte distant et fournit sa propre adresse MAC. Avec le proxy ARP, l'hôte se comporte comme si l'hôte distant était connecté au même segment du réseau. Si le Routeur A échoue, l'hôte continue à envoyer des packets destinés à l'hôte distant à l'adresse MAC du Routeur A même si ces paquets n'ont nulle part où aller et sont détruits. Vous pouvez soit attendre qu'ARP acquière l'adresse MAC d'un autre routeur, le routeur B, sur le segment local qui envoie une autre requête ARP, soit redémarrer l'hôte pour le forcer à envoyer une requête ARP. Dans les deux cas, pendant un laps de temps important, l'hôte ne peut pas communiquer avec l'hôte distant, même si le protocole de routage a convergé, et le routeur B est prêt à transférer des paquets qui autrement passeraient par le routeur A.

Protocole de routage dynamique

Certains hôtes IP exécutent (ou surveillent) un protocole de routage dynamique tel que le protocole RIP (Routing Information Protocol) ou OSPF (Open Shortest Path First) pour détecter les routeurs. L'inconvénient du protocole RIP est qu'il est lent à s'adapter aux modifications de la topologie. L'exécution d'un protocole de routage dynamique sur chaque hôte n'est pas pratique pour un certain nombre de raisons, ainsi que la surcharge administrative, processing les problèmes de surcharge, de sécurité ou l'absence d'implémentation de protocole pour certaines plates-formes.

Protocole de détection de routeur ICMP

Certains hôtes IP plus récents utilisent le ICMP Router Discovery Protocol (IRDP) (RFC 1256) pour trouver un nouveau routeur quand une route devient indisponible. Un hôte qui exécute IRDP écoute les messages hello multicast de son routeur configuré et utilise un routeur alternatif lorsqu'il ne reçoit plus ces messages hello. Les valeurs de minuteur par défaut d'IRDP signifient qu'il ne convient pas à la détection d'une défaillance du premier saut. Le taux de publicité par défaut est une fois toutes les 7 à 10 minutes, et la durée de vie par défaut est de 30 minutes.

Protocole de configuration d'hôte dynamique

Le protocole DHCP (Dynamic Host Configuration Protocol) (RFC 1531) fournit un mécanisme permettant de transmettre les informations de configuration aux hôtes sur un réseau TCP/IP. Un hôte qui exécute un client DHCP demande des informations de configuration à un serveur DHCP lorsqu'il démarre sur le réseau. Ces informations de configuration comportent typiquement une adresse IP et une passerelle par défaut. Il n'y a aucun mécanisme pour commuter vers un routeur alternatif si la passerelle par défaut échoue.

Fonctionnement HSRP

Une grande classe d'implémentations d'hôtes hérités qui ne prennent pas en charge la découverte dynamique peut configurer un routeur par défaut. L'exécution d'un mécanisme de détection dynamique de routeur sur chaque hôte n'est pas pratique pour un certain nombre de raisons, ainsi

que la surcharge administrative, processing surcharge, problèmes de sécurité ou absence d'implémentation de protocole pour certaines plates-formes. HSRP fournit des services de basculement à ces hôtes.

Lorsque vous utilisez HSRP, un ensemble de routeurs fonctionne de concert pour présenter l'illusion d'un seul routeur virtuel aux hôtes sur le LAN. Cet ensemble est connu en tant que groupe HSRP ou groupe de veille. Un seul routeur sélectionné dans le groupe est responsable de la distribution des paquets que les hôtes envoient au routeur virtuel. Ce routeur est connu en tant que routeur actif. Un autre routeur est élu comme routeur de veille. En cas de défaillance du routeur actif, le routeur de secours prend en charge le paquetforwarding fonctions du routeur actif. Bien qu'un nombre arbitraire de routeurs puisse exécuter HSRP, seul le routeur actif transfère les paquets envoyés au routeur virtuel.

Pour réduire au minimum le trafic sur le réseau, seul le routeur actif et les routeurs de veille envoient périodiquement des messages HSRP une fois que le protocole a réalisé le processus d'élection. Si le routeur actif échoue, le routeur de veille succède en tant que routeur actif. Si le routeur de veille échoue ou devient le routeur actif, alors un autre routeur est élu en tant que routeur de veille.

Sur un réseau local particulier, plusieurs groupes de secours automatique peuvent coexister et se chevaucher. Chaque groupe de veille émule un seul routeur virtuel. Les routeurs individuels peuvent participer à plusieurs groupes. Dans ce cas, le routeur met à jour un état et des temporisateurs distincts pour chaque groupe. Chaque groupe de veille a une seule adresse MAC bien connue, aussi qu'une adresse IP.

Adressage HSRP

Dans la plupart des cas, quand vous configurez les routeurs pour qu'ils fassent partie d'un groupe HSRP, les routeurs écoutent l'adresse MAC HSRP pour ce groupe ainsi que leur propre adresse MAC gravée en mémoire. L'exception est les routeurs dont les contrôleurs Ethernet identifient seulement une seule adresse MAC (par exemple, le Lance controller sur les routeurs Cisco 2500 et 4500). Ces routeurs utilisent l'adresse MAC HSRP lorsqu'ils sont le routeur actif et leur adresse intégrée lorsqu'ils ne le sont pas.

HSRP utilise cette adresse MAC sur tous les supports sauf Token Ring :

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

Les interfaces Token Ring utilisent des adresses fonctionnelles pour l'adresse MAC de HSRP. Les adresses fonctionnelles sont le seul mécanisme général de multidiffusion. Il y a un nombre limité d'adresses fonctionnelles Token Ring disponibles, et beaucoup d'entre elles sont réservées pour d'autres fonctions. Vous pouvez utiliser ces trois adresses avec HSRP :

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

> **Note**: Lorsque le protocole HSRP s'exécute dans un environnement SRB (Source-Route Bridging) à plusieurs anneaux et que les routeurs HSRP résident sur des anneaux différents et utilisent les adresses fonctionnelles, cela peut entraîner une confusion du RIF (Routing Information Field). Par exemple, dans un environnement SRB, il est possible qu'un routeur de veille HSRP réside sur une boucle différente du routeur actif.

Quand ce routeur de veille devient actif, les stations sur la même boucle que le vieux routeur actif a besoin d'un nouveau RIF afin d'envoyer des paquets au nouveau routeur actif. Cependant, comme le routeur de secours (nouveau routeur actif) utilise la même adresse fonctionnelle que le routeur actif précédent, les stations ne savent pas qu'elles doivent envoyer des explorateurs pour un nouveau RIF. Pour cette raison, la commande use-bia a été introduite.

Matrice des fonctionnalités de la version de Cisco IOS® et de HSRP

Ce document montre quelles fonctionnalités HSRP sont prises en charge dans quelles versions du logiciel Cisco IOS. Cliquez sur une caractéristique pour voir une description détaillée. Un numéro de version intermédiaire indique dans quelle version est apparue pour la première fois une caractéristique, ou une version où la fonctionnalité de cette caractéristique a changé.

Fonctionnalité	10.0	10.2	10.3	11.0	11.1	11.2	11.3	12.0	12.0T	12.1	12.1T
Préemption	X	X	X	X	X	X	X	X	X	X	X
Plusieurs groupes (MHSRP)	—	—	X	X	X	X	X	X	X	X	X
Ethernet 802.10 SDE	—	—	—	—	X	X	X	X	X	X	X
Interface Tracking	—	—	—	—	X	X	X	X	X	X	X
Use BIA	—	—	—	—	8.0	X	X	X	X	X	X
Retard de préemption	—	—	—	—	—	X	X	6.1	X	X	X
Ethernet LANE	—	—	—	—	—	X	X	X	X	X	X
Token Ring LANE	—	—	—	—	—	—	X	X	X	X	X
Lien ISL	—	—	—	—	—	—	X	X	X	X	X
Prise en charge de Syslog	—	—	—	—	—	—	X	X	X	X	X
Intervalle d'actualisation MAC	—	—	—	—	—	—	—	1.0	X	X	X
SNMP MIB	—	—	—	—	—	—	—	—	3.0	X	X
MHSRP et Use BIA	—	—	—	—	—	—	—	—	3.4	X	X
Redondance IP	—	—	—	—	—	—	—	—	3.4	X	X
BVI	—	—	—	—	—	—	—	—	6.2	X	X
802.1Q	—	—	—	—	—	—	—	—	8.1	X	X
Débogage amélioré de HSRP	—	—	—	—	—	—	—	—	—	0,2	X
Redirections ICMP HSRP	—	—	—	—	—	—	—	—	—	—	3
HSRP MPLS VPN	—	—	—	—	—	—	—	—	—	—	3

Fonctionnalité HSRP de Cisco IOS

Fonctionnalités HSRP

Préemption

La caractéristique de préemption de HSRP permet au routeur avec la plus grande priorité de devenir immédiatement le routeur actif. La priorité est d'abord déterminée par la valeur de priorité que vous avez configurée puis par l'adresse IP. Dans chaque cas, une valeur plus élevée a une priorité plus élevée. Lorsqu'un routeur de priorité plus élevée prévaut sur un routeur de priorité plus faible, il envoie un message Coup. Quand un routeur actif de basse priorité reçoit un message Coup ou un message Hello depuis un routeur actif de plus grande priorité, l'état du routeur se change en Speak et envoie un message Resign.

Retard de préemption

La fonction de délai de préemption permet de retarder la préemption pendant une période configurable et permet au routeur de remplir sa table de routage avant de devenir le routeur actif.

Avant le logiciel IOS de Cisco version 12.0(9), le délai commençait lors du redémarrage du routeur. Dans la version 12.0(9) de Cisco IOS, le retard commence à la première tentative de préemption.

Pour configurer la priorité et la préemption HSRP, utilisez la commande standby **[group] [prioritynumber] [preempt [delay [minimum]seconds] [syncseconds]]**. Reportez-vous à la documentation HSRP pour plus d'informations.

Interface Tracking

Interface tracking vous permet de spécifier une autre interface sur le routeur pour le processus HSRP à surveiller afin de modifier la priorité HSRP pour un groupe donné.

Si le protocole de ligne spécifié de l'interface tombe en panne, la priorité HSRP de ce routeur est réduite, et permet à un autre routeur HSRP avec une priorité plus élevée de devenir actif (s'il a la préemption activée).

Pour configurer l'interface HSRP tracking, utilisez la commande **standby [group] track interface [priority]**.

> **Note**: La disponibilité de la commande Interface Track peut dépendre de la version du logiciel utilisé, mais la commande **standby [group] track [object]** peut être utilisée à la place.

Quand plusieurs interfaces de suivi sont désactivées, la priorité est réduite par une quantité cumulative. Si vous configurez explicitement la valeur de décrément, alors la valeur est diminuée de cette quantité si cette interface est désactivée, et les décréments sont cumulatifs. Si vous ne configurez pas une valeur de décrément explicite, alors la valeur est diminuée de 10 pour chaque interface qui se désactive, et les décréments sont cumulatifs.

Cet exemple utilise cette configuration, avec la valeur de décrément par défaut de 10 :

> **Note**: Quand un numéro de groupe HSRP n'est pas spécifié, le numéro de groupe par défaut est 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
```

Le comportement de HSRP avec cette configuration :

- 0 interface désactivée = aucune diminution (la priorité est 110)
- 1 interface désactivée = diminution de 10 (la priorité devient 100)
- 2 interfaces désactivées = diminution de 10 (la priorité devient 90)

Le comportement HSRP mentionné précédemment est vrai même si les valeurs de décrément sont configurées explicitement comme suit :

```
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
```

Avant la version 12.1 de Cisco IOS, si vous démarrez un routeur avec une interface inactive, l'interface HSRP tracking considère l'interface comme active.

Adresse gravée en mémoire d'utilisation

La fonctionnalité d'utilisation d'adresse intégrée (BIA) permet aux groupes HSRP d'utiliser une adresse MAC intégrée de l'interface au lieu d'une adresse MAC HSRP. Use BIA a été implémentée pour la première fois dans la version 11.1(8) de Cisco IOS. Pour configurer HSRP pour utiliser BIA, utilisez la commande standby use-bia [scope interface].

La commande **use-bia** a été implémentée pour surmonter les limitations quand une adresse fonctionnelle pour l'adresse MAC HSRP sur les interfaces Token Ring est utilisée.

> **Note**: Lorsque le protocole HSRP s'exécute dans un environnement de pontage routé par la source à plusieurs anneaux et que les routeurs HSRP résident sur des anneaux différents et utilisent les adresses fonctionnelles, cela peut provoquer une confusion du champ RIF (Routing Information Field). Pour cette raison, la commande **use-bia a été introduite.**

La fonctionnalité **use-**biafeature permet également d'utiliser DECnet, Xerox Network Systems (XNS) et HSRP sur le même routeur en utilisant l'adresse MAC DECnet (BIA) à utiliser comme adresse MAC HSRP. La commande **use-bia** est également utile pour les réseaux où le BIA du périphérique a été configuré dans d'autres périphériques sur le LAN.

Cependant, la commande **use-bia a plusieurs inconvénients :**

- Quand un routeur devient actif, l'adresse IP virtuelle est déplacée vers une adresse MAC différente. Le nouveau routeur actif envoie une réponse ARP gratuite, mais toutes les implémentations d'hôte ne gèrent pas correctement l'ARP gratuit.
- Le proxy ARP est brisé quand **use-bia est configurée.** Un routeur de secours ne peut pas couvrir la base de données ARP proxy perdue d'un routeur défaillant.
- Avant la version 12.0(3.4)T de Cisco IOS, seul un groupe HSRP est autorisé si use-bia est configurée.

Lorsque vous configurez la commande **use-bia** sur une sous-interface, elle apparaît en fait sur l'interface principale et est appliquée à toutes les sous-interfaces. Dans Cisco IOS version 12.0(6.2) et ultérieure, la commande **use-bia** est étendue avec les mots-clés d'interface d'étendue facultatifs pour permettre son application à une seule sous-interface.

Plusieurs groupes HSRP

La fonctionnalité de groupes HSRP multiples (MHSRP) a été ajoutée dans la version 10.3 de Cisco IOS. Cette fonctionnalité permet en outre la redondance et le partage de charge au sein des

réseaux et permet aux routeurs redondants d'être plus pleinement utilisés. Alors qu'un routeur transfère activement le trafic pour un groupe HSRP, il peut être en veille ou en état d'écoute pour un autre groupe.

Depuis la version 12.0(3.4)T de Cisco IOS, vous pouvez utiliser la commande **use-bia avec plusieurs groupes HSRP activés.** Référez-vous à Partage de charge avec HSRP pour configurer HSRP et tirer parti de plusieurs chemins.

Adresse MAC configurable

Normalement, vous utilisez HSRP pour aider les stations d'extrémité à localiser le premier saut de passerelle pour le routage IP. Les stations d'extrémité sont configurées avec une passerelle par défaut. Cependant, HSRP peut fournir la redondance du premier saut pour d'autres protocoles. Certains protocoles, tels que l'Advanced Peer-to-Peer Networking (APPN), emploient l'adresse MAC pour identifier le premier saut pour le routage.

Dans ce cas, il est souvent nécessaire de pouvoir spécifier l'adresse MAC virtuelle qui utilise la commande **standby mac-address**. L'adresse IP virtuelle est sans importance pour ces protocoles. La syntaxe réelle de cette commande est standby [group] mac-address mac-address.

> **Remarque** : vous ne pouvez pas utiliser cette commande sur une interface Token Ring.

Prise en charge de Syslog

Prise en charge de Syslog messaging pour les informations HSRP a été ajouté dans la version 11.3 de Cisco IOS. Cette fonctionnalité permet de logging et tracking des routeurs actifs et en veille actuels sur les serveurs syslog.

Débogage HSRP

Avant Cisco IOS version 12.1, la commande de débogage HSRP était relativement simple. Pour activer le débogage HSRP, vous utiliseriez simplement la commande debug standby, qui a activé la sortie de l'état de HSRP et les informations de paquet pour tous les groupes de veille sur toutes les interfaces.

Une condition de débogage a été ajoutée dans la version 12.0(2.1) de Cisco IOS qui permet la sortie de la commande **standby debug d'être filtrée selon l'interface ou le numéro du groupe.** La commande utilise le paradigme debug condition introduit dans la version 12.0 de Cisco IOS, comme suit : **debug condition standby interface group.** L'interface que vous spécifiez doit être une interface valide pouvant prendre en charge HSRP. Le groupe peut être n'importe quel groupe (0 - 255).

Vous pouvez paramétrer des conditions de débogage pour des groupes qui n'existent pas, ce qui vous permet de capturer des informations de débogage pendant l'initialisation d'un nouveau groupe.

Vous devez activer l'ordre standby debug pour qu'une sortie de débogage soit produite. Si vous ne configurez aucune condition de **débogage de secours**, alors la sortie de débogage est produite pour tous les groupes sur toutes les interfaces. Si vous configurez au moins une condition **standby debug**, alors la sortie **standby debug** est filtrée par toutes les conditions **standby debug**.

Débogage amélioré de HSRP

Avant Cisco IOS version 12.1(0.2), le débogage HSRP était d'usage limité, car les informations étaient perdues dans le bruit des messages Hello périodiques. Ainsi, la fonctionnalité de débogage amélioré a été ajoutée à Cisco IOS 12.1(0.2).

Le tableau décrit les options de commande pour le débogage amélioré.

Commande	Description
debug standby	Affiche toutes les erreurs, les événements, et les pa de HSRP.
debug standby terse	Affiche toutes les erreurs, événements, et paquets d HSRP sauf les paquets hello et les paquets d'annon
debug standby errors	Affiche les erreurs HSRP.
debug standby events [[all | abrégé] | [icmp | protocole | redondance | piste]] [détail]	Affiche les évènements HSRP.
debug standby packets< /a> [[all | abrégé] | [annoncer | coup d'Etat | bonjour | démissionner]] [détail]	Affiche les paquets HSRP.

Vous pouvez filtrer la sortie de **débogage** avec le débogage conditionnel d'interface et de groupe HSRP. Pour activer le débogage conditionnel d'interface, utilisez la commande **debug condition interface < /span>**. Pour activer le débogage conditionnel HSRP, utilisez la commande **debug condition standby interface group.**

Une condition de débogage d'interface s'applique seulement quand vous n'avez paramétré aucune condition **standby debug.** Le débogage HSRP est encore meilleur dans le logiciel IOS de Cisco version 12.1(1.3), grâce aux améliorations apportées au tableau d'état HSRP.

Ces améliorations affichent les événements de la table d'état HSRP. Dans la sortie, les **a/** , **b/** , **c/** , et ainsi de suite, se réfèrent aux événements de la machine à état fini HSRP, qui sont documentés dans 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
```

Authentification

La caractéristique d'authentification HSRP se compose d'une clé partagée en texte clair contenue dans les paquets HSRP. Cette fonctionnalité empêche le routeur de priorité inférieure de learning les valeurs d'adresse IP et de minuteur de secours du routeur de priorité supérieure.

Pour configurer la chaîne d'authentification HSRP, utilisez la commande standby authentication

<string>.

Redondance IP

HSRP fournit la redondance stateless pour le routage IP. Le protocole HSRP seul ne peut conserver que son propre état. Il suppose que chaque routeur construit et met à jour ses propres tables de routage indépendamment des autres routeurs. La fonctionnalité de redondance IP fournit un mécanisme qui permet à HSRP de fournir un service aux applications clientes afin qu'elles puissent mettre en oeuvre un basculement dynamique.

La redondance IP ne fournit pas un mécanisme pour que les applications partenaires échangent des informations d'état. Ceci est laissé aux applications elles-mêmes et est essentiel si les applications doivent fournir un basculement dynamique.

La redondance IP est généralement implémentée uniquement pour les agents mobiles IP domestiques. Voici un exemple de configuration :

```
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
```

> **Note**: Depuis la version 12.1(3)T de Cisco, le mot clé **redundancy est accepté en plus du mot clé standby.** Le mot-clé **standby** est éliminé progressivement dans une version ultérieure de Cisco IOS. La commande correcte est **ip mobile home-agent redundancy hsrp-group1** .

Les utilisations futures de la redondance IP incluent :

- NAT - Besoin de fournir des passerelles redondantes.
- IPSEC - Besoin de synchroniser les informations d'état afin de fonctionner quand HSRP est en service.
- Serveur DCHP - Serveurs DHCP implémentés dans divers routeurs.
- NBAR, CBAC - Besoin de refléter les états du pare-feu pour le routage asymétrique.
- GPRS - Besoin d'un moyen pour suivre l'état TCP.

SNMP Management Information Base

Le support de la Management Information Base (MIB) a été ajouté dans la version 12.0(3.0)T de Cisco IOS. Il y a deux MIB pertinents pour HSRP :

- ciscoMgmt 106: Le module MIB utilisé pour gérer HSRP
- ciscoMgmt 107: Module MIB d'extension utilisé pour gérer HSRP

Avant la version 12.0(6.1)T de Cisco IOS, une marche de la HSRP MIB étendue lorsqu'une Bridge Group Virtual Interface (BVI) est présente, entraîne un crash du routeur.

Support de HSRP pour Multiprotocol Label Switching Virtual Private Networks

Le support HSRP pour Multiprotocol Label Switching Virtual Private Networks (MPLS VPN) a été ajouté dans la version 12.1(3)T de Cisco IOS.

HSRP sur une interface VPN MPLS est utile quand vous avez un Ethernet connecté entre deux Provider Edge (PE) et que vous avez l'un de ces éléments :

- A Customer Périphérie (CE) avec une route par défaut vers l'adresse IP virtuelle HSRP.
- Un ou plusieurs hôtes avec l'adresse IP virtuelle HSRP configurée comme passerelle par défaut.

Le schéma du réseau montre deux PE avec HSRP qui s'exécutent entre leur VPN routing/forwarding (VRF). Les CE avec l'adresse IP virtuelle HSRP sont configurés comme route par défaut. Et HSRP est configuré pour suivre les interfaces qui connectent les PE au reste du réseau du fournisseur. Par exemple, si l'interface E1 de PE1 tombe en panne, la priorité HSRP est réduite de sorte que PE2 prend le relais forwarding à l'adresse IP/MAC virtuelle.

Voici les configurations :

Routeur 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
```

Routeur PE2

```
 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
```

Vous pouvez utiliser les commandes suivantes pour vérifier que l'adresse IP virtuelle HSRP est dans le VRF ARP correct et dans Cisco Express Forwarding tableaux :

```
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
```

Support HSRP pour redirections ICMP

HSRP est basé sur le concept que les routeurs homologues HSRP qui protègent un sous-réseau peuvent fournir un accès à tous les autres sous-réseaux qui composent le réseau. Par conséquent, il est inutile de savoir quel routeur devient le routeur HSRP actif, car tous les routeurs ont eu des routes vers chaque sous-réseau.

HSRP se sert d'une adresse IP virtuelle et d'une MAC virtuelle spéciales, qui sont logiquement attachées au routeur actif HSRP. Les redirections ICMP sont automatiquement désactivées sur une interface lorsque HSRP est utilisé sur cette interface. À partir de la version 12.1(3)T de Cisco IOS, la fonction de redirection ICMP active les redirections ICMP sur les interfaces configurées avec HSRP. Référez-vous à Support HSRP pour les redirections ICMP pour plus de détails. Ceci est fait pour empêcher les hôtes de rediriger loin de l'adresse IP virtuelle HSRP. Il est possible que les deux routeurs (ou plus) d'un sous-réseau n'aient pas la même connectivité avec le reste du réseau. En d'autres termes, pour une adresse IP de destination particulière, l'un ou l'autre des routeurs peut avoir un meilleur chemin vers cette adresse ou peut même être le seul routeur attaché à cette adresse.

Le protocole ICMP permet à un routeur de rediriger une station d'extrémité pour envoyer des paquets pour une destination particulière à un autre routeur sur le sous-réseau, si le premier routeur sait que l'autre routeur a un meilleur chemin vers cette destination particulière. Comme c'était le cas pour les passerelles par défaut, si le routeur vers lequel une station d'extrémité a été redirigée vers une destination particulière échoue, les paquets de la station d'extrémité vers cette destination n'ont pas été remis. Dans le HSRP standard, c'est exactement ce qui se produit. Pour cette raison, il est recommandé de désactiver les redirections ICMP si HSRP est activé.

Lorsque vous étendez la relation entre les redirections ICMP et HSRP fournit une solution à ce problème et cela vous permet de tirer parti des avantages des redirections HSRP et ICMP. Deux (ou plusieurs) groupes HSRP sont exécutés sur chaque sous-réseau, avec au moins autant de groupes HSRP configurés que de routeurs qui participent. Les priorités sont configurées de sorte que chaque routeur soit le routeur principal pour au moins un groupe HSRP. Lorsqu'un routeur détermine de rediriger une station d'extrémité vers un autre routeur pour une destination spécifique, au lieu de la rediriger vers la station d'extrémité vers cette autre adresse IP de routeur, il trouve un groupe HSRP qui a ce routeur comme routeur principal et redirige la station d'extrémité vers l'adresse IP virtuelle correspondante. Si ce routeur cible tombe en panne, HSRP s'assure qu'un autre routeur prend le relais et peut-être redirige la station d'extrémité vers un autre routeur virtuel.

Prise en charge des interfaces et des médias HSRP

Cette section explique quelles interfaces et quels médias HSRP prend en charge, et les avertissements qui se produisent lorsque vous exécutez HSRP sur ces médias.

Depuis le logiciel Cisco IOS Version 10, la fonctionnalité HSRP est disponible sur Ethernet, Token Ring et Fiber Distributed Data Interface (FDDI). Les interfaces Fast Ethernet et ATM sont également supportés par HSRP.

Les LAN virtuels (VLAN) permettent à des topologies de réseau logique de recouvrir l'infrastructure physique commutée, de sorte que toute collecte arbitraire de ports LAN peut être combinée dans un groupe d'utilisateurs ou une communauté d'intérêts autonomes. La prise en charge du VLAN HSRP a été ajoutée dans la version 11.1 de Cisco IOS pour IEEE 802.10 Secure Data Exchange (SDE), et dans Cisco IOS version 11.3 pour l'Inter-Switch Link (ISL) de Cisco.

Ethernet

Plusieurs contrôleurs Ethernet (Lance et QUICC) dans des produits bas de gamme peuvent seulement avoir une adresse MAC monodiffusé dans leur filtre d'adresse. Sur ces plates-formes, un seul groupe HSRP est permis, et l'adresse d'interface est changée pour l'adresse MAC virtuelle de HSRP quand le groupe devient actif. Si vous utilisez HSRP sur des routeurs avec plusieurs interfaces de ce type, vous devez configurer chaque interface avec un numéro de groupe HSRP différent.

> **Note**: Le routeur Cisco 7200 utilise également le contrôleur Ethernet Lance, mais il supporte MHSRP dans le logiciel.

Cisco recommande que vous n'avez pas plus de vingt-quatre processeurs d'interface Ethernet HSRP (EIP) en raison du temps nécessaire pour la mise à jour des filtres d'adresses pour HSRP. Si vous avez plus de vingt-quatre EIP HSRP, cela peut entraîner une instabilité et une charge excessive du CPU.

Si vous disposez de plus de vingt-quatre EIP, essayez de les remplacer par des VIP (Versatile Interface Processors) et des cartes de ports Ethernet. Les VIPs ont été approuvés jusqu'à 80 groupes HSRP. Vous pouvez également réduire le nombre de groupes HSRP et augmenter le temps d'attente et Hello HSRP.

Token Ring

Si vous exécutez HSRP sur une interface Token Ring, vous ne pouvez pas reprogrammer le filtre d'adresse sur le chipset Token Ring de la même façon que vous pouvez sur l'émulation Ethernet, FDDI ou ATM. Le Token Ring utilise des adresses fonctionnelles, dont une petite partie seulement sont disponibles qui ne sont pas en conflit avec d'autres utilisations de l'espace d'adresse fonctionnelle.

Si vous exécutez HSRP dans un environnement SRB (Source-Route Bridging), l'utilisation d'adresses fonctionnelles peut provoquer une confusion RIF. Consultez la section Adressage HSRP pour plus d'informations. Essayez également de configurer la commande **use-bia**.

802.1Q

Cisco recommande d'utiliser la version 12.0(8.1)T ou ultérieure du logiciel Cisco IOS pour HSRP sur 802.1Q.

Lien ISL

HSRP via ISL est disponible dans les versions 11.2(6)F, 11.3 et 12.X de Cisco IOS. Il est recommandé d'utiliser la version 12.0(7) ou ultérieure.

FDDI

Un adaptateur de port FDDI élimine des trames de la boucle s'il voit une de ses propres adresses MAC dans la source MAC. Si un événement du réseau rend les deux routeurs actifs, alors les deux routeurs envoient des paquets hello HSRP avec l'adresse MAC virtuelle. Chaque routeur

supprime par erreur le paquet Hello de l’autre routeur du réseau et les deux restent actifs.

La solution à ce problème dans la version 11.2(11.1) de Cisco IOS est pour des routeurs HSRP dans un environnement FDDI d'utiliser leur propre adresse MAC unique gravée en mémoire pour échanger des messages et exécuter le protocole HSRP. Pour s'assurer que learning Les ponts et les commutateurs mettent en cache l'entrée de port correcte pour l'adresse MAC virtuelle. Le routeur actif envoie également des messages d'actualisation périodiques par l'adresse MAC HSRP.

> **Note**: La mémoire matérielle associative (CAM) du routeur Cisco 4500 sur une interface FDDI ne peut pas être remplie correctement après un rechargement si vous avez configuré plusieurs réseaux RIP et groupes HSRP. La seule solution de contournement pour l'instant est d'effacer les interfaces pour restaurer la CAM.

Actualisation MAC

Des routeurs HSRP dans un environnement FDDI utilisent leur propre adresse MAC unique gravée en mémoire pour échanger des messages et exécuter le protocole HSRP. Pour s'assurer que learning Les ponts et les commutateurs mettent en cache l'entrée de port correcte pour l'adresse MAC virtuelle. Le routeur actif envoie également des messages d'actualisation périodiques par l'adresse MAC HSRP.

Si vous n'avez pas de commutateur ou learning sur votre réseau, vous pouvez désactiver la distribution des paquets d'actualisation comme indiqué ci-dessous :

```
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

Le support HSRP pour les Bridge Group Virtual Interfaces (BVI) a été ajouté dans la version 12.0(6.2)T de Cisco IOS.

Sous-interfaces

Les groupes HSRP sur les sous-interfaces doivent avoir un numéro de groupe unique parmi tous les autres groupes sur toutes les sous-interfaces sur la même interface principale. Cela est dû au fait que les sous-interfaces ne reçoivent pas un index d'interface SNMP unique. Si vous aviez deux groupes avec le numéro N sur des sous-interfaces différentes, alors dans la MIB, le groupe N sur la sous-interface 1 et le groupe N sur la sous-interface 2 apparaîtraient être le même groupe.

Informations connexes

- Page de support HSRP
- HSRP – FAQ

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.