Caractéristiques et fonctionnalités du protocole HSRP (Hot Standby Router Protocol)

Contenu

Introduction

Ce document décrit les caractéristiques et les fonctionnalités du Hot Standby Router Protocol (HSRP).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

HSRP - Informations générales et fonctionnement

Un moyen d'obtenir presque 100 pourcent de temps de fonctionnement du réseau est l'utilisation d'HSRP, qui fournit la redondance du réseau pour des réseaux IP, assurant que le trafic utilisateur récupère immédiatement et d'une manière transparente des pannes au premier saut dans les périphériques à la périphérie du réseau ou les circuits d'accès.

En partageant une adresse IP et une adresse MAC (couche 2), deux routeurs ou plus peuvent agir en tant que simple routeur "virtuel". Les membres du groupe de routeurs virtuel échangent continuellement des messages d'état. Ainsi, un routeur peut assumer la responsabilité du routage d'un autre s'il sort de la commission pour des raisons prévues ou non. Les hôtes continuent à transférer des paquets IP à une adresse IP et MAC, et le changement de périphériques effectuant un routage est transparent.

Mécanismes de découverte de routeurs dynamiques

Ci-dessous détaillées des descriptions des mécanismes de découverte de routeurs dynamiques qui sont disponibles pour les hôtes. Nombre de ces mécanismes ne fournissent pas la résilience du réseau requise par les administrateurs réseau. Ceci peut se produire parce que le protocole n'a pas été destiné au départ à fournir la résilience du réseau ou parce qu'il n'est pas faisable que chaque hôte sur le réseau exécute le protocole. En plus de cette liste, il est important de noter que beaucoup d'hôtes vous permettent seulement de configurer une passerelle par défaut.

Proxy Address Resolution Protocol

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 que l'ARP acquière l'adresse MAC d'un autre routeur, Routeur B, sur le segment local en envoyant une autre requête ARP, soit redémarrer l'hôte pour le forcer à envoyer une requête ARP. Dans un cas ou dans l'autre, pendant une période significative, l'hôte ne peut pas communiquer avec l'hôte distant, même si le protocole de routage a convergé, et le Routeur B est préparé à transférer des paquets qui passeraient autrement par le Routeur A.

Protocole de routage dynamique

Certains hôtes IP exécutent (ou surveillent) un protocole de routage dynamique tel que le Protocole d'informations de routage (RIP) ou l'Open Shortest Path First (OSPF) pour découvrir des routeurs. L'inconvénient d'utiliser RIP est qu'il est lent pour s'adapter aux changements de la topologie. L'exécution d'un protocole de routage dynamique sur chaque hôte peut ne pas être faisable pour un certain nombre de raisons, y compris les temps administratifs, les temps de traitement, les problèmes de sécurité, ou le manque de mise en oeuvre de protocoles pour quelques plates-formes.

ICMP Router Discovery Protocol

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 temporisateur par défaut d'IRDP indiquent qu'il n'est pas approprié pour la détection des pannes au 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 de configuration d'hôte dynamique (DHCP) (RFC 1531) fournit un mécanisme pour passer les informations de configuration aux serveurs 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 de mises en oeuvre d'hôtes traditionnels qui ne supportent pas la découverte dynamique sont capables de configurer un routeur par défaut. L'exécution d'un mécanisme de découverte de routeurs dynamique sur chaque hôte peut ne pas être faisable pour un certain nombre de raisons, y compris les temps administratifs, les temps de traitement, les problèmes de sécurité, ou le manque de mise en oeuvre de protocoles pour quelques plates-formes. HSRP fournit des services de basculement à ces hôtes.

En utilisant le 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 élu dans le groupe est responsable du transfert 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. Au cas où le routeur actif échouerait, le routeur de veille assume les fonctions de transfert de paquets 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 LAN particulier, plusieurs groupes de veille 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 quand ils sont le routeur actif, et leur adresse gravée en mémoire quand ils ne le sont pas.

HSRP utilise l'adresse MAC suivante sur tous les médias à l'exception de 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 les trois adresses suivantes avec HSRP :

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

Note: Quand HSRP s'exécute dans un environnement multiple-ring source-route bridging (BSR) et que les routeurs HSRP résident sur différentes boucles, l'utilisation d'adresses fonctionnelles peut entraîner une confusion de Routing information Field (RIF). 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, puisque le (nouveau) routeur (actif) de veille utilise la même adresse fonctionnelle que le précédent routeur actif, les stations ne se rendent pas compte qu'elles doivent envoyer des explorateurs pour un nouveau RIF. Pour cette raison, la commande use-bia a été introduite.

Tableau des versions de Cisco IOS et des fonctionnalités HSRP

Ce document montre quelles caractéristiques de HSRP sont supportées selon la version 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.

Caractéristique	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
Suivi d'interface					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
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											3

HSRP											
HSRP MPLS VPN											3

Images de démarrage Cisco IOS et fonctionnalités HSRP

La fonctionnalité HSRP a été incluse dans les images de démarrage de Cisco IOS jusqu'à l'intégration de l'ID de bogue Cisco CSCec16720 (clients enregistrés uniquement). L'ID de bogue Cisco CSCec16720 retirait HSRP des images de démarrage excepté :

- 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-boot-mz
- rpmxf-boot-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

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 est de plus grande priorité.

Quand un routeur d'une priorité plus élevée devance un routeur de moins grande priorité, 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 caractéristique de retard de préemption permet de retarder la préemption pour une période configurable, en laissant le routeur remplir sa table de routage avant de devenir le routeur actif.

Avant Logiciel Cisco IOS version 12.0(9), le retard commencé quand le routeur a rechargé. 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 d'HSRP, utilisez la commande standby [group] [priority number] [preempt [delay [minimum] seconds] [sync seconds]].

Référez-vous à la documentation de HSRP pour plus d'informations sur comment configurer HSRP.

Suivi d'interface

Le suivi des interfaces 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 d'interface spécifié se désactive, la priorité HSRP de ce routeur est réduite, permettant à un autre routeur HSRP avec une plus grande priorité de devenir actif (s'il a activé la préemption).

Pour configurer le suivi des interfaces HSRP, utilisez la commande tandby [group] track interface [priority].

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.

L'exemple qui suit utilise la configuration suivante, avec une 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 ci-dessus de HSRP est vrai même si les valeurs de décrément sont configurées explicitement comme ci-dessous.

```
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 Cisco IOS version 12.1, si vous mettez en marche un routeur avec vers le bas une interface, le suivi d'interface de HSRP considère l'interface comme.

Cette anomalie a l'ID de bogue Cisco CSCdp32289 (clients enregistrés uniquement).

Adresse gravée en mémoire d'utilisation

La fonctionnalité burned-in address (BIA) laisse les groupes HSRP utiliser une interface gravée dans une adresse MAC 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 de l'utilisation d'une adresse fonctionnelle pour l'adresse MAC HSRP sur les interfaces Token Ring.

Note: Quand HSRP s'exécute dans un environnement multiple-ring source-routed bridging et que les routeurs HSRP résident sur différentes boucles, l'utilisation des adresses fonctionnelles peut entraîner une confusion de Routing Information Field (RIF). Pour cette raison, la commande **use-bia** a été introduite.

La fonctionnalité **use-bia** active également l'utilisation de DECNet, Xerox Network Systems (XNS), et HSRP sur le même routeur en permettant à l'adresse MAC de DECNet (le BIA) d'être utilisée comme adresse MAC de HSRP. La commande **use-bia** est également utile dans des situations de mise en réseau lorsque le BIA d'un 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 veille ne peut pas couvrir la base de données ARP du proxy perdu 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.

Quand vous configurez la commande **use-bia** dans une sous-interface, elle apparaît en fait sur l'interface principale et est appliquée à toutes les sous-interfaces. Dans les versions 12.0(6.2) et ultérieures de Cisco IOS, la commande **use-bia** est étendue avec le champ facultatif mots clés interface pour lui permettre d'être appliquée à une seule sous-interface.

Cette anomalie a l'ID de bogue Cisco CSCdm25468 (clients enregistrés uniquement).

Plusieurs groupes HSRP

La fonctionnalité multiple HSRP (MHSRP) a été ajoutée dans la version 10.3 de Cisco IOS. Cette

fonctionnalité permet davantage de redondance et de partage de charge dans les réseaux, et permet aux routeurs redondants d'être utilisés de manière plus complète. Alors qu'un routeur transfère activement du trafic pour un groupe HSRP, il peut être dans un état de veille ou 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 au chargement partageant avec le HSRP pour configurer le HSRP afin de tirer profit des 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 en utilisant 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**.

Note: Vous ne pouvez pas utiliser cette commande sur une interface Token Ring.

Prise en charge de Syslog

La prise en charge de la transmission de messages de syslog pour les informations HSRP a été ajoutée dans la version 11.3 de Cisco IOS. Cette caractéristique permet une journalisation et un suivi plus efficaces du routeur actif et des routeurs de veille actuels sur les serveurs de syslog.

Débogage HSRP

Avant Cisco IOS version 12.1, la commande de débogage de 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 capable de supporter 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 pas de conditions **standby debug**, 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 selon toutes les conditions **standby debug**.

Débogage amélioré de HSRP

Avant Cisco IOS version 12.1(0.2), l'élimination des imperfections de HSRP était utile l'utilisation limitée parce que les informations ont été perdues dans le bruit des messages Hello périodiques. Ainsi la caractéristique de débogage amélioré a été ajoutée dans la version 12.1(0.2) de Cisco IOS.

Le tableau suivant détaille les options des commandes pour le débogage amélioré.

Commande	Description
debug standby	Affiche toutes les erreurs, les événements, et les paquets de HSRP.
debug standby terse	Affiche toutes les erreurs, événements, et paquets de HSRP sauf les paquets hello et les paquets d'annonce.
debug standby errors	Affiche les erreurs HSRP.
debug standby events [[all | laconique] | [ICMP | protocole | Redondance | track]] [detail]	Affiche les évènements HSRP.
debug standby packets [[all | laconique] | [annoncez | coup | bonjour | resign]] [detail]	Affiche les paquets HSRP.

Vous pouvez filtrer la **sortie de débogage** en utilisant l'interface et le débogage conditionnel de groupe HSRP. Pour activer le débogage conditionnel d'interface, utilisez la commande **debug condition interface interface**. 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**. L'élimination des imperfections de HSRP est encore améliorée dans la version de logiciel 12.1(1.3) de Cisco IOS, basée sur les améliorations qui ont été apportées au tableau des états HSRP.

Cette anomalie a l'ID de bogue Cisco CSCdp57811 (clients enregistrés uniquement).

Ces améliorations affichent les événements de la table d'état HSRP. Dans la sortie ci-dessous, **a/**, **b/**, **c/**, etc. se rapportent aux événements de la machine à états finis de 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 (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
```

Authentification

La caractéristique d'authentification HSRP se compose d'une clé partagée en texte clair contenue dans les paquets HSRP. Cette caractéristique empêche le routeur de basse priorité d'apprendre l'adresse IP de veille et les valeurs de temporisateurs de veille d'un routeur à la priorité plus élevée.

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

Redondance IP

HSRP fournit la redondance stateless pour le routage IP. HSRP lui-même est limité à la mise à jour de son propre état. Il suppose que chaque routeur construit et met à jour ses propres tables de routage indépendamment des autres routeurs. La caractéristique de redondance IP fournit un mécanisme qui laisse HSRP fournir un service aux applications clientes de sorte qu'ils puissent mettre en place le basculement dynamique.

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

La redondance IP est actuellement (depuis janvier 2000) implémentée uniquement pour les Agents locaux IP mobiles . Voici un exemple de configuration :

```
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: 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** sera éliminé dans une version future de Cisco IOS. La commande correcte sera alors ip mobile home-agent redundancy hsrp-group1.

Les utilisations futures de la redondance IP peuvent inclure :

- NAT - Le besoin de fournir les passerelles redondantes.
- IPSEC - Devez synchroniser les informations d'état afin de fonctionner quand le 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 - A besoin d'une manière de dépister l'état de TCP.

- PIX

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 pour contrôler HSRP
- ciscoMgmt 107: Le module MIB d'extension pour contrôler 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.

Cette anomalie a l'ID de bogue Cisco CSCdm61257 (clients enregistrés uniquement).

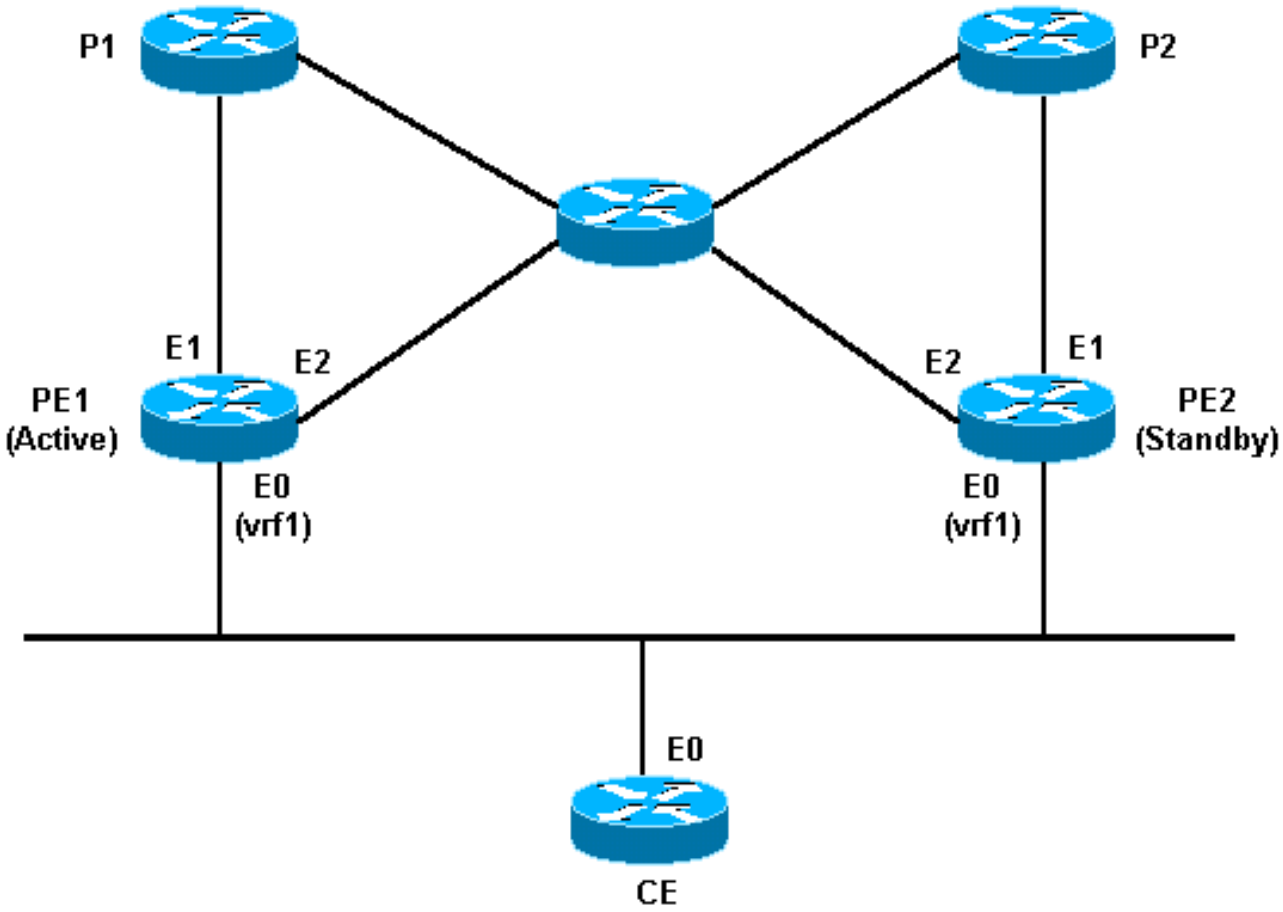
Support de HSRP pour Multiprotocol Label Switching Virtual Private Networks

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 MPLS VPN est utile quand vous avez un Ethernet connecté entre deux Provider Edges (PE) et que vous avez un des éléments suivants :

- Un Customer Edge (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 de réseau ci-dessous montre deux PE avec un HSRP fonctionnant entre leurs interfaces routage/transfert (VRF) VPN. Nous avons configuré le CE avec l'adresse IP virtuelle HSRP en tant que route par défaut. Et nous avons configuré HSRP pour suivre les interfaces connectant le PE au reste du réseau fournisseur. Par exemple, si l'interface E1 de PE1 échoue, la priorité HSRP sera réduite à tel point que PE2 prend le relai sur le transfert de paquets à l'adresse IP/MAC virtuelle.



Ce sont les configurations :

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

Vous pouvez utiliser les commandes suivantes afin de vérifier que l'adresse IP virtuelle HSRP est

dans la VRF ARP le VRF et dans les tables Cisco express forwarding correctes :

```
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 partenaire HSRP protégeant un sous-réseau peuvent permettre d'accéder à tous les autres sous-réseaux composant 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 en utilisant HSRP sur cette interface. A partir de IOS 12.1(3)T, la fonctionnalité ICMP Redirects permet 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 des hôtes d'être redirigés ailleurs que vers l'adresse IP virtuelle HSRP. Il est possible que les deux routeurs (ou plus) d'un sous-réseau n'ont pas la même connectivité au reste du réseau. C'est-à-dire que pour une adresse IP de destination particulière, l'un ou l'autre des routeurs peut avoir un chemin bien meilleur 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 pour une destination particulière échoue, alors les paquets de la station d'extrémité pour cette destination n'ont pas été livrés. Dans le HSRP standard, c'est exactement ce qui se produit. Pour cette raison, nous recommandons de désactiver les redirections ICMP si HSRP est allumé.

Étendre le rapport entre les redirections ICMP et HSRP fournit une solution à ce problème, vous permettant de tirer profit des avantages d'HSRP et des redirections ICMP. Deux groupes HSRP (ou plus) sont exécuté sur chaque sous-réseau, avec au moins autant de groupes de HSRP configurés qu'il y a de routeurs participant. Les priorités sont configurées de sorte que chacun des routeurs est maître d'au moins un groupe HSRP. Quand un routeur détermine la redirection d'une station d'extrémité vers un autre routeur pour une destination spécifique, alors au lieu de rediriger la station d'extrémité vers l'adresse IP de cet autre routeur, il recherche un groupe HSRP qui est maîtrisé par ce routeur, et redirige la station d'extrémité vers l'adresse IP virtuelle correspondante. Si ce routeur de destination échoue alors, HSRP fait en sorte qu'un autre routeur prenne le relai et, peut-être, redirige la station d'extrémité vers encore un autre routeur, virtuel encore une fois.

Prise en charge des interfaces et des médias HSRP

Cette section explique quelles interfaces et supports supporte HSRP, et les possibles obstacles lors de l'exécution de HSRP sur ces supports.

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.

Ethernets

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 devriez 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. Avoir plus de vingt-quatre EIP HSRP peut entraîner l'instabilité et une charge excessive du CPU.

Cette anomalie a l'ID de bogue Cisco CSCdj29595 (clients enregistrés uniquement).

Si vous avez plus de vingt-quatre EIP, essayez de remplacer les EIP par des Versatile Interface Processors (VIP) et des adaptateurs de port Ethernet. Les VIPs ont été approuvés jusqu'à 80 groupes HSRP. Vous pouvez également réduire le nombre de groupes HSRP, et augmenter la durée de hello et d'attente HSRP.

Token Ring

Une limite de l'exécution HSRP sur une interface Token Ring est que vous ne pouvez pas reprogrammer le filtre d'adresses sur le jeu de puces de Token Ring comme vous pouvez le faire en 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.

En exécutant HSRP dans un environnement source-route bridging (BSR), l'utilisation des adresses fonctionnelles peut entraîner une confusion de RIF. Consultez la section Adressage HSRP pour plus d'informations. Essayez également de configurer la commande **use-bia**.

802.1Q

Cisco recommande utilisant la version de logiciel 12.0(8.1)T ou ultérieures de Cisco IOS pour le HSRP au-dessus du 802.1Q.

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 afin d'éviter le problème décrit dans l'ID de bogue Cisco CSCdm68811 (clients enregistrés uniquement).

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. Chacun routeur supprime par erreur le paquet hello de l'autre routeur du réseau, et les deux routeurs restent actifs.

Cette anomalie a l'ID de bogue Cisco CSCdj30049 (clients enregistrés uniquement).

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 les ponts et les commutateurs apprenant mettent en cache l'entrée de port correcte pour l'adresse MAC virtuelle, le routeur actif envoie également périodiquement des messages d'actualisation à l'aide de l'adresse MAC HSRP.

Note: La mémoire de contenu adressable (CAM) du matériel du routeur Cisco 4500 sur une interface FDDI ne peut être alimentée 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. Cette anomalie a l'ID de bogue Cisco CSCdm93122 (clients enregistrés uniquement).

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 les ponts et les commutateurs apprenant mettent en cache l'entrée de port correcte pour l'adresse MAC virtuelle, le routeur actif envoie également périodiquement des messages d'actualisation à l'aide de l'adresse MAC HSRP. Cette anomalie a l'ID de bogue Cisco CSCdj30049 (clients enregistrés uniquement).

Si vous n'avez pas de commutateur ou de pont apprenant sur votre réseau, vous pouvez désactiver l'envoi de paquets d'actualisation comme montré ci-dessous :

```
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
```

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

Informations connexes

- Page de support HSRP
- HSRP - FOIRE AUX QUESTIONS
- Support et documentation techniques - Cisco Systems