Présentation et résolution des problèmes HSRP dans les réseaux de commutateurs Catalyst

Contenu

Introduction

En raison de la nature du protocole Hot Standby Router Protocol (HSRP), des problèmes réseau spécifiques peuvent mener à une instabilité de HSRP. Ce document couvre les problèmes courants avec HSRP et les façons de les dépanner. La plupart des problèmes liés au protocole HSRP ne sont pas vraiment dus à HSRP. Ce sont plutôt des problèmes réseau qui affectent le comportement de HSRP.

Ce document couvre ces problèmes les plus courants associés à HSRP :

- Rapport d'un routeur sur un doublon d'adresse IP de secours HSRP
- Changement constant de l'état du protocole HSRP (active, standby, speak)
- Homologues HSRP manquants
- Messages d'erreur du commutateur liés à HSRP
- Diffusion unicast du réseau excessive sur la configuration de HSRP

> Remarque: Ce document détaille comment dépanner HSRP dans les environnements de commutation Catalyst. Il contient de nombreuses références aux versions de logiciel et à la conception de la topologie du réseau. Néanmoins, le seul but de ce document est de faciliter et de guider les ingénieurs dans le dépannage de HSRP. Ce document n'est pas destiné à être un guide de conception, un document de recommandation de logiciels ou un document des meilleures pratiques.

Conditions préalables

Exigences

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.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Compréhension de HSRP

Informations générales

Les entreprises et consommateurs qui se fondent sur les services intranet et Internet pour les communications critiques à leur mission exigent de leurs réseaux et applications qu'ils soient disponibles sans interruption. Les clients peuvent satisfaire leurs demandes pour environ 10 pour cent du temps de disponibilité du réseau s'ils exploitent HSRP dans le logiciel Cisco IOS®. HSRP, qui est propre aux plates-formes Cisco, fournit la redondance du réseau pour des réseaux IP de telle sorte 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.

Deux ou plusieurs routeurs peuvent agir en tant que simple routeur virtuel s'ils partagent une adresse IP et une adresse MAC (couche L2 [L2]). L'adresse est nécessaire pour la redondance de la passerelle par défaut du poste de travail hôte. La plupart des postes de travail hôtes ne contiennent pas de tables de routage et utilisent seulement une seule adresse IP et MAC au saut suivant. Cette adresse est connue comme étant la passerelle par défaut. Avec HSRP, les membres du groupe de routeurs virtuel échangent continuellement des messages d'état. Un routeur peut assumer la responsabilité du routage d'un autre si un routeur sort de la commission pour des raisons prévues ou non. Les hôtes sont configurés avec une passerelle par défaut et continuent d'expédier des paquets IP à une adresse IP et MAC cohérente. Le changement de périphériques qui font le routage est transparent pour les postes de travail d'extrémité.

> Remarque: Vous pouvez configurer les postes de travail hôtes qui exécutent le système d'exploitation Microsoft pour plusieurs passerelles par défaut. Mais, les passerelles par défaut multiples ne sont pas dynamiques. L'OS utilise seulement une passerelle par défaut à la fois. Le système sélectionne uniquement une passerelle par défaut configurée supplémentaire au moment du démarrage si la première passerelle par défaut configurée est déterminée comme étant inaccessible par le protocole ICMP (Internet Control Management Protocol).

Opération de base

Un ensemble de routeurs qui exécutent HSRP travaillent de concert pour présenter l'illusion d'un seul routeur de passerelle par défaut aux hôtes sur le LAN. Cet ensemble de routeurs est connu en tant que groupe HSRP ou groupe de secours. Un seul routeur élu dans le groupe est responsable de l'expédition des paquets que les hôtes envoient au routeur virtuel. Ce routeur est connu en tant que routeur actif. Un autre routeur est élu en tant que routeur de réserve. Si le routeur actif échoue, le routeur de secours assume les fonctions d'expédition des paquets. Bien qu'un nombre arbitraire de routeurs puisse exécuter HSRP, seul le routeur actif transmet les paquets qui sont envoyés à l'adresse IP du routeur virtuel.

Afin de réduire au minimum le trafic sur le réseau, seuls les routeurs actif et de secours envoient des messages HSRP périodiques après que le protocole a terminé le processus d'élection. Les routeurs supplémentaires dans le groupe HSRP restent dans l'état Listen. Si le routeur actif échoue, le routeur de réserve succède en tant que routeur actif. Si le routeur de secours échoue ou devient le routeur actif, un autre routeur est élu en tant que routeur de secours.

Chaque groupe de secours émule un routeur virtuel unique (passerelle par défaut). Pour chaque groupe, une adresse MAC et IP unique bien connue est allouée à ce groupe. Plusieurs groupes

de secours peuvent coexister et se superposer sur un LAN et des routeurs individuels peuvent participer à plusieurs groupes. Dans ce cas, le routeur met à jour un état et des temporisateurs distincts pour chaque groupe.

Termes HSRP

Terme	Définition
Routeur actif	Routeur qui transmet les paquets pour le routeur virtuel
Routeur de secours	Le routeur principal de secours
Groupe de secours	L'ensemble des routeurs qui participent au HSRP et émulent conjointement un routeur virtuel
Délai Hello	L'intervalle entre les messages Hello successifs de HSRP depuis un routeur donné
Temps d'attente	L'intervalle entre la réception d'un message Hello et la présomption que le routeur éme a échoué

Adressage HSRP

Communication des routeurs HSRP

Les routeurs qui exécutent HSRP communiquent des informations HSRP entre eux par des paquets Hello de HSRP. Ces paquets sont envoyés à l'adresse de multidiffusion IP de destination 224.0.0.2 sur le port 1985 du protocole de datagramme utilisateur (UDP). L'adresse de multidiffusion IP 224.0.0.2 est une adresse de multidiffusion réservée qui est utilisée pour communiquer à tous les routeurs. Le routeur actif approvisionne les paquets Hello depuis son adresse IP configurée et l'adresse MAC virtuelle de HSRP. Le routeur de secours approvisionne les paquets Hello depuis son adresse IP configurée et l'adresse MAC gravée en mémoire (BIA). Cette utilisation de l'adressage source est nécessaire pour que les routeurs HSRP puissent s'identifier correctement.

Dans la plupart des cas, quand vous configurez les routeurs pour qu'ils fassent partie d'un groupe HSRP, les routeurs détectent à l'oreille l'adresse MAC de HSRP pour ce groupe ainsi bien que leur propre BIA. La seule exception à ce comportement est pour les routeurs Cisco 2500, 4000 et 4500. Ces routeurs ont un matériel Ethernet qui n'identifie qu'une seule adresse MAC. Par conséquent, ces routeurs utilisent l'adresse MAC de HSRP quand ils servent de routeur actif. Les routeurs utilisent leur BIA quand ils servent de routeur de secours.

Transmission de l'adresse IP de secours HSRP sur tous les médias, à l'exception de Token Ring

Puisque les postes de travail hôtes sont configurés avec leur passerelle par défaut en tant qu'adresse IP de secours HSRP, les hôtes doivent communiquer avec l'adresse MAC qui est associée à l'adresse IP de secours HSRP. Cette adresse MAC est une adresse MAC virtuelle qui se compose de 0000.0c07.ac**. ** est le numéro du groupe HSRP au format hexadécimal, basé sur l'interface correspondante. Par exemple, le groupe HSRP 1 utilise l'adresse MAC virtuelle de HSRP de 0000.0c07.ac01. Les hôtes sur le segment LAN contigu emploient le processus normal du Protocole de résolution d'adresse (ARP) afin de résoudre les adresses MAC associées.

Transmission de l'adresse IP de secours HSRP sur le support Token Ring

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 de ces dernières sont réservées pour d'autres fonctions. Ces trois sont adresses sont les seules disponibles pour un usage avec HSRP :

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

Par conséquent, vous ne pouvez configurer que trois groupes HSRP sur les interfaces Token Ring, à moins de configurer le paramètre **standby use-bia**.

Redirections ICMP

Les routeurs homologues HSRP qui protègent un sous-réseau peuvent permettre d'accéder à tous les autres sous-réseaux du réseau. C'est la base du protocole HSRP. Par conséquent, il est inutile de savoir quel routeur devient le routeur HSRP actif. Dans les versions du logiciel Cisco IOS antérieures à la version 12.1(3)T, les redirections ICMP sont automatiquement désactivées sur une interface quand le protocole HSRP est utilisé sur cette interface. Sans cette configuration, les hôtes peuvent être redirigés depuis l'adresse IP HSRP virtuelle vers une adresse IP et MAC de l'interface d'un routeur unique. La redondance est perdue.

Le logiciel Cisco IOS Version 12.1(3)T introduit une méthode pour permettre les redirections ICMP avec HSRP. Cette méthode filtre les messages sortants de redirection ICMP par HSRP. L'adresse IP du prochain saut est modifiée en une adresse virtuelle HSRP. L'adresse IP de la passerelle dans le message sortant de redirection ICMP est comparée à une liste de routeurs HSRP actifs qui sont présents sur ce réseau. Si le routeur qui correspond à l'adresse IP de la passerelle est un routeur actif pour un groupe HSRP, l'adresse IP de la passerelle est remplacée par l'adresse IP de ce groupe virtuel. Cette solution permet à des hôtes de retenir les routes optimales vers les réseaux distants et, en même temps, de mettre à jour la résilience fournie par HSRP.

Tableau des fonctionnalités du protocole HSRP

Référez-vous à la section Version Cisco IOS et au tableau des fonctionnalités du protocole HSRP de Fonctionnalités du protocole HSRP pour découvrir les fonctionnalités et les versions du logiciel Cisco IOS qui prennent en charge HSRP.

Fonctionnalités HSRP

Référez-vous à Fonctionnalités du protocole HSRP pour des informations sur la plupart des fonctionnalités de HSRP. Ce document fournit des informations sur ces fonctionnalités HSRP :

- Préemption
- Suivi d'interface
- Utilisation d'un BIA
- Plusieurs groupes HSRP
- Adresses MAC configurables
- Prise en charge de Syslog
- Débogage HSRP
- Débogage amélioré de HSRP
- Authentification

- Redondance IP
- MIB du protocole de gestion de réseau simple (SNMP)
- HSRP pour la commutation multiprotocole par étiquette (MPLS)

Remarque: Vous pouvez utiliser la fonctionnalité de recherche de votre navigateur afin de localiser ces sections dans le document.

Format des paquets

Ce tableau montre le format de la partie « données » de la trame UDP de HSRP :

version	**Op Code**	**État**	**Hellotime**
Holdtime	**Priorité**	Groupe	Réservé
Authentication Data			
Authentication Data			
Adresse IP virtuelle			

Ce tableau décrit chacun des champs dans le paquet HSRP :

Champ du paquet	Description
Op Code (1 octet)	Op Code décrit le type de message que le paquet contient. Les valeurs possibles sont les suivantes : 0 - Hello, 1 - coup et 2 - resign. Des messages Hello sont envoyés pour indique qu'un routeur exécute HSRP et peut devenir le routeur actif. Des message Coup sont envoyés quand un routeur souhaite devenir le routeur actif. Des messages Resign sont envoyés quand un routeur ne souhaite plus être le routeur actif.
State (1 octet)	Chaque routeur du groupe de secours met en application une machine d'état. Le champ d'état décrit l'état actuel du routeur qui envoie le message. Voici des détails sur les différents états : 0 - initial, 1 - learn, 2 - listen, 4 - speak, 8 - standby et 16 - active.
Hellotime (1 octet)	Ce champ est seulement significatif dans les messages Hello. Il contient la période approximative entre les messages Hello envoyés par le routeur. Le temps est donné en secondes.
Holdtime (1 octet)	Ce champ est seulement significatif dans les messages Hello. Il contient le temps pendant lequel les routeurs attendent un message Hello avant de lancer une modification d'état.
Priority (1 octet)	Ce champ est utilisé pour élire les routeurs actif et de secours. Dans une comparaison des priorités de deux routeurs, le routeur avec la valeur la plus élevée devient le routeur actif. L routeur ayant l'adresse IP la plus haute l'emporte.
Group (1 octet)	Ce champ identifie le groupe de secours.
Authentication Data (8 octets)	Ce champ contient un mot de passe à huit caractères en texte clair.
Adresse IP virtuelle (4 octets)	Si l'adresse IP virtuelle n'est pas configurée sur un routeur, l'adresse peut être apprise à partir du message Hello du routeur actif. Une adresse n'est apprise que si aucune adresse IP de secours HSRP n'a été configurée, et le message Hello est authentifié (si l'authentification est configurée).

États HSRP

État	Définition
`Initiale`	C'est l'état au démarrage. Cet état indique que HSRP n'est pas exécuté. Cet état est généré par modification de configuration ou quand une interface devient disponible pour la première fois.

Apprenez	Le routeur n'a pas déterminé l'adresse IP virtuelle et n'a pas encore vu un message Hello auther du routeur actif. Dans cet état, le routeur attend toujours de recevoir des informations du routeur
Écoutez	Le routeur connaît l'adresse IP virtuelle, mais n'est ni le routeur actif, ni le routeur de secours. Il détecte à l'oreille les messages Hello de ces routeurs.
Parlez	Le routeur envoie des messages Hello périodiques et participe activement à l'élection du routeur et/ou de secours. Un routeur ne peut pas entrer dans l'état speak à moins qu'il possède l'adresse virtuelle.
Standby	Le routeur est un candidat pour devenir le prochain routeur actif et envoie des messages Hello périodiques. À l'exclusion de conditions passagères, il y a, tout au plus, un routeur dans le group standby.
Actif	Le routeur transmet les paquets qui sont envoyés à l'adresse MAC virtuelle du groupe. Le routeu envoie des messages Hello périodiques. À l'exclusion de conditions passagères, il doit y avoir, to plus, un routeur dans l'état active dans le groupe.

Temporisateurs HSRP

Chaque routeur utilise seulement trois temporisateurs dans HSRP. Les temporisateurs chronomètrent les messages Hello. Le protocole HSRP converge quand une panne se produit, selon la façon dont les temporisateurs Hello et de maintien de HSRP sont configurés. Par défaut, ces temporisateurs sont définis sur 3 et 10 secondes, respectivement, ce qui signifie qu'un paquet Hello est envoyé entre les périphériques du groupe de secours de HSRP toutes les 3 secondes, et que le périphérique de secours devient actif quand un paquet Hello n'a pas été reçu pendant 10 secondes. Vous pouvez abaisser ces paramètres de temporisation pour accélérer le basculement ou la préemption, mais, pour éviter une utilisation accrue du CPU et un affolement inutile de l'état Standby, ne définissez pas le temporisateur de paquets Hello en-dessous d'une (1) seconde ou le temporisateur de maintien en-dessous de 4 secondes. Notez que, si vous utilisez le mécanisme de suivi de HSRP et que la liaison suivie échoue, un basculement ou une préemption se produit immédiatement, indépendamment des temporisateurs Hello et de maintien. Quand un temporisateur expire, le routeur passe à un nouvel état de HSRP. Les temporisateurs peuvent être changés avec cette commande : **standby [group-number] timers hellotime holdtime**. Par exemple, **standby 1 timers 5 15**.

Cette table fournit plus d'informations sur ces temporisateurs :

Temporisateur	Description
Temporisateur Active	Ce temporisateur est utilisé pour surveiller le routeur actif. Il démarre quand un routeur act reçoit un paquet Hello. Il expire selon la valeur Holdtime qui est définie dans le champ qui est lié du message Hello de HSRP.
Temporisateur de veille	Ce temporisateur est utilisé pour surveiller le routeur de secours. Il démarre quand le routeur de secours reçoit un paquet Hello. Il expire selon la valeur Holdtime qui est définie dans le paquet Hello correspondant.
Temporisateur "Hello"	Ce temporisateur est utilisé pour chronométrer les paquets HELLO. Tous les routeurs HSRP dans n'importe quel état de HSRP produisent un paquet Hello quand ce temporisateur Hello expire.

Événements HSRP

Ce tableau fournit les événements dans la machine à états finis de HSRP :

Key (Clé)	Événements
1	Le protocole HSRP est configuré sur une interface activée.

2	HSRP est désactivé sur une interface ou l'interface est désactivée.
3	L'échéance du temporisateur actif le temporisateur actif est placée à la durée d'attente où le dernie message Hello est vu du routeur actif.
4	L'échéance du temporisateur de réserve le temporisateur de réserve est placée à la durée d'attent le dernier message Hello est vu du routeur de réserve.
5	L'échéance de minuteur Hello la temporisation périodique pour l'envoi des messages Hello est exp
6	Réception d'un message Hello d'une priorité supérieure d'un routeur dans l'état speak
7	Réception d'un message Hello d'une priorité supérieure du routeur actif
8	Réception d'un message Hello d'une priorité inférieure du routeur actif
9	Réception d'un message de démission du routeur actif
10	Réception d'un message Coup d'un routeur de priorité supérieure
11	Réception d'un message Hello d'une priorité supérieure du routeur actif
12	Réception d'un message Hello d'une priorité inférieure du routeur actif

Actions HSRP

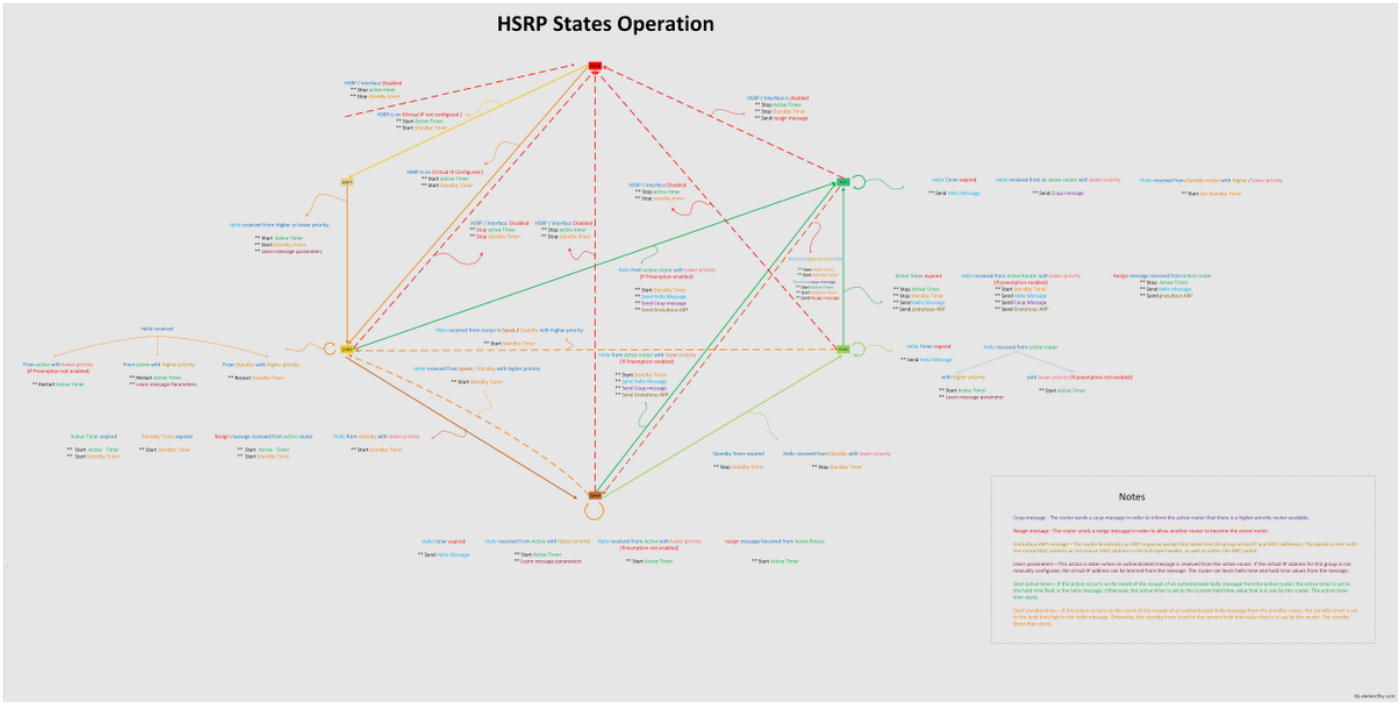
Ce tableau spécifie les actions qui doivent être prises en tant qu'élément de la machine d'état :

Lettre	Action
A	Démarrer le temporisateur actif-Si cette action survient à la suite de la réception d'un message Hell authentifié depuis le routeur actif, le temporisateur actif est défini en fonction du champ du temps d'attente dans le message Hello. Autrement, le temporisateur actif est défini à la valeur actuelle du temps d'attente qui est utilisée par ce routeur. Le temporisateur actif démarre ensuite.
B	Démarrer le temporisateur de veille-Si cette action survient à la suite de la réception d'un message authentifié depuis le routeur de secours, le temporisateur de veille est défini en fonction du champ temps d'attente dans le message Hello. Autrement, le temporisateur de veille est défini à la valeur actuelle du temps d'attente qui est utilisée par ce routeur. Le temporisateur de veille démarre ensui
C	Arrêter le temporisateur actif-Le temporisateur actif s'arrête.
D	Arrêter le temporisateur de veille-Le temporisateur de veille s'arrête.
E	Apprendre les paramètres-Cette action est prise quand un message authentifié est reçu depuis le routeur actif. Si l'adresse IP virtuelle pour ce groupe n'est pas configurée manuellement, l'adresse virtuelle peut être apprise à partir du message. Le routeur peut retenir les valeurs du temps Hello e temps d'attente.
F	Envoyer le message Hello-Le routeur envoie un message Hello avec son état actuel, le temps Hell temps d'attente.
G	Envoyer un message Coup-Le routeur envoie un message Coup afin d'informer le routeur actif qu'i un routeur de priorité supérieure disponible.
H	Envoyer un message de démission-Le routeur envoie un message de démission afin de permettre autre routeur de devenir le routeur actif.
I	Envoyer un message ARP gratuit-Le routeur diffuse un paquet de réponses ARP qui annonce les adresses IP et MAC virtuelles du groupe. Le paquet est envoyé avec l'adresse MAC virtuelle comm adresse MAC source dans l'en-tête de la couche de liaison ainsi que dans le paquet ARP.

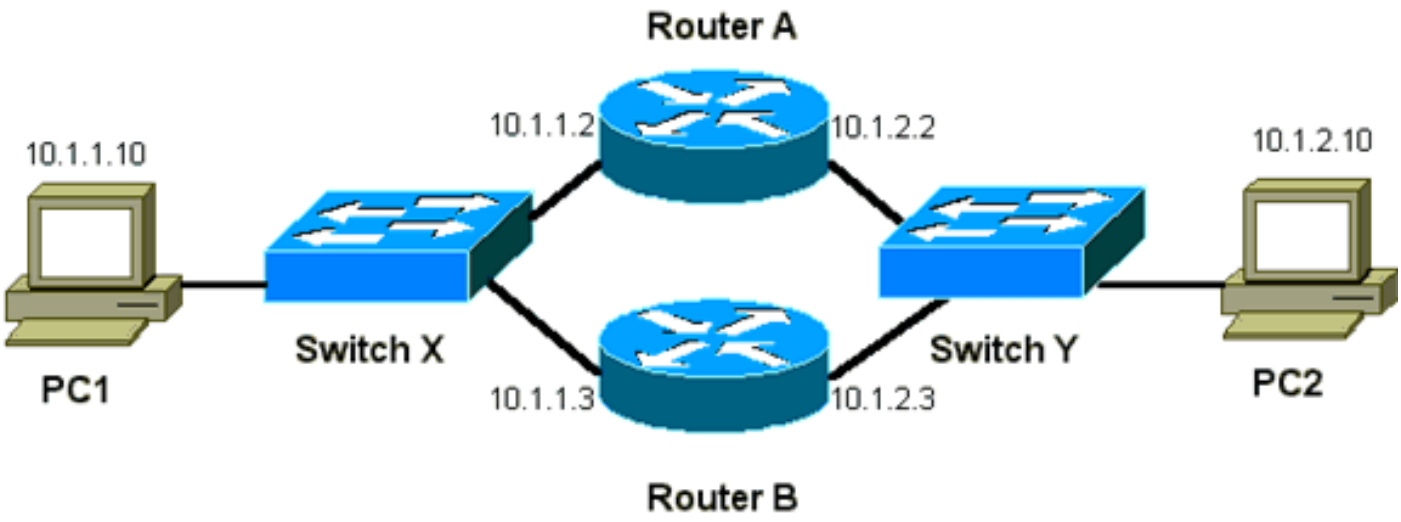
Tableau des états HSRP

Le diagramme de cette section montre les transitions d'état de la machine d'état de HSRP. Chaque fois que se produit un événement, l'action associée en résulte et le routeur passe à l'état HSRP suivant. Dans le diagramme, les numéros indiquent des événements et les lettres indiquent l'action associée. Le tableau dans la section Événements HSRP définit les numéros et le tableau dans la section Actions HSRP définit les lettres. Utilisez ce diagramme seulement comme référence. Le diagramme est détaillé et n'est pas nécessaire pour le dépannage général.

Pour une image de haute résolution du diagramme, voir l'exécution d'états de HSRP.



Flux des paquets



Périphérique	Adresse MAC	Adresse IP	Masque de sous-réseau	Passerelle par défaut
PC1	0000.0c00.0001	10.1.1.10	255.255.255.0	10.1.1.1
PC2	0000.0c00.1110	10.1.2.10	255.255.255.0	10.1.2.1

Configuration du routeur A (routeur actif)

```
interface ethernet 0
    ip address 10.1.1.2 255.255.255.0
    mac-address 4000.0000.0010
    standby 1 ip 10.1.1.1
    standby 1 priority 200
interface ethernet 1
    ip address 10.1.2.2 255.255.255.0
```

```
    mac-address 4000.0000.0011
    standby 1 ip 10.1.2.1
    standby 1 priority 200
```

Configuration du routeur B (routeur de secours)

```
interface ethernet 0
    ip address 10.1.1.3 255.255.225.0
    mac-address 4000.0000.0020
    standby 1 ip 10.1.1.1
interface ethernet 1
     ip address 10.1.2.3 255.255.255.0
     mac-address 4000.0000.0021
     standby 1 ip 10.1.2.1
```

> Remarque: Ces exemples configurent les adresses MAC statiques uniquement à des fins d'illustration. Ne configurez pas les adresses MAC statiques à moins que vous deviez le faire.

Vous devez comprendre le concept de flux de paquets quand vous obtenez des suivi du renifleur afin de dépanner les problèmes de HSRP. Le routeur A utilise la priorité de 200 et devient le routeur actif sur les deux interfaces. Dans l'exemple de cette section, les paquets du routeur qui sont destinés à un poste de travail hôte ont l'adresse MAC source de l'adresse MAC physique du routeur (BIA). Les paquets des machines hôtes qui sont destinés à l'adresse IP HSRP ont l'adresse MAC de destination de l'adresse MAC HSRP virtuelle. Notez que les adresses MAC ne sont pas les mêmes pour chaque flux entre le routeur et le hôte.

Ce tableau montre les informations d'adresse MAC et IP respectives par flux sur la base d'un suivi du renifleur pris du commutateur X.

Flux des paquets	MAC de source	MAC de destination	Source ip	IP de destinat
Les paquets de PC1 qui sont destinés à PC2	PC1 (0000.0c00.0001)	Adresse MAC HSRP virtuelle de l'interface Ethernet 0 (0000.0c07.ac01) du routeur A	10.1.1.10	10.1.2.1
Les paquets qui reviennent par le routeur A de PC2 et qui sont destiné à PC1	Ethernet 0 BIA (4000.0000.0010) du routeur A	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.1
Les paquets de PC1 qui sont destinés à l'adresse IP de secours de HSRP (ICMP, Telnet)	PC1 (0000.0c00.0001)	Adresse MAC HSRP virtuelle de l'interface Ethernet 0 (0000.0c07.ac01) du routeur A	10.1.1.10	10.1.1.1
Les paquets qui sont destinés à l'adresse IP réelle du routeur actif (ICMP, Telnet)	PC1 (0000.0c00.0001)	Ethernet 0 BIA (4000.0000.0010) du routeur A	10.1.1.10	10.1.1.2
Les paquets qui sont destinés à l'adresse IP réelle du routeur de secours (ICMP, Telnet)	PC1 (0000.0c00.0001)	Ethernet 0 BIA (4000.0000.0020) du routeur B	10.1.1.10	10.1.1.3

Dépannage d'études de cas HSRP

Étude de cas #1 : L'adresse IP de secours HSRP est signalée comme doublon d'adresse IP

Ces messages d'erreur peuvent apparaître :

```
Oct 12 13:15:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 13 16:25:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:31:02: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:41:01: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
```

Ces messages d'erreur n'indiquent pas nécessairement un problème de HSRP. En revanche, les messages d'erreur indiquent une boucle SPT (Spanning Tree Protocol) ou un problème éventuel de configuration des routeurs/commutateurs. Les messages d'erreur sont juste les symptômes d'un autre problème.

En outre, ces messages d'erreur n'empêchent pas le bon fonctionnement de HSRP. Le doublon de paquet HSRP est ignoré. Ces messages d'erreur sont limités à des intervalles de 30 secondes. Mais, une faible performance du réseau et une perte de paquets peuvent résulter en l'instabilité du réseau entraînant les messages d'erreur STANDBY-3-DUPADDR de l'adresse HSRP.

Ces messages d'erreur peuvent apparaître :

```
Oct 15 22:41:01: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
  on Vlan25, sourced by 0000.0c07.ac19
```

Ces messages indiquent spécifiquement que le routeur a reçu un paquet de données qui était originaire de l'adresse IP HSRP sur le VLAN 25 avec les adresses MAC 0000.0c07.ac19. Puisque l'adresse MAC HSRP est 0000.0c07.ac19, soit le routeur en question a reçu son propre paquet de nouveau, soit les deux routeurs dans le groupe HSRP sont entrés dans l'état active. Puisque le routeur a reçu son propre paquet, le problème réside très probablement dans le réseau plutôt que le routeur. Divers problèmes peuvent entraîner ce comportement. Parmi les problèmes réseau éventuels qui entraînent les messages d'erreur figurent les suivants :

- Boucles STP momentanées
- Problèmes de configuration d'EtherChannel
- Doublons de trames

Quand vous dépannez ces messages d'erreur, référez-vous aux étapes de dépannage de la section Modules de dépannage de HSRP pour les commutateurs CatOS de ce document. Tous les modules de dépannage s'appliquent à cette section, qui inclut des modules sur la configuration. En outre, notez toutes les erreurs dans le journal des commutateurs et référencez les études de cas supplémentaires selon les besoins.

Vous pouvez utiliser une liste d'accès afin d'empêcher le routeur actif de recevoir son propre paquet Hello de multidiffusion. Mais, ce n'est qu'une solution de contournement pour les messages d'erreur qui cache le symptôme du problème. La solution de contournement consiste à appliquer une liste d'accès étendue en entrée aux interfaces de HSRP. La liste d'accès bloque tout trafic originaire de l'adresse IP physique qui est destiné à l'adresse de multidiffusion 224.0.0.2 des routeurs.

```
access-list 101 deny ip host 172.16.12.3 host 224.0.0.2
access-list 101 permit ip any any

interface ethernet 0
  ip address 172.16.12.3 255.255.255.0
  standby 1 ip 172.16.12.1
  ip access-group 101 in
```

Étude de cas #2 : L'état de HSRP change continuellement (Active, Standby, Speak) ou %HSRP-6-STATECHANGE

Ces messages d'erreur peuvent apparaître :

```
Jan 9 08:00:42.623: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:00:56.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:03.011: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
Jan 9 08:01:29.427: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Standby -> Active
Jan 9 08:01:36.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Active -> Speak
Jan 9 08:01:43.808: %STANDBY-6-STATECHANGE: Standby: 49:
  Vlan149 state Speak -> Standby
```

Ces messages d'erreur décrivent une situation dans laquelle un routeur HSRP de secours n'a pas reçu trois paquets Hello successifs HSRP depuis son homologue HSRP. La sortie montre que le routeur de secours passe de l'état standby à l'état active. Peu après, le routeur revient à l'état standby. À moins que ce message d'erreur se produise pendant l'installation initiale, un problème de HSRP n'est probablement pas à l'origine du message d'erreur. Les messages d'erreur signifient la perte de Hellos HSRP entre les homologues. Quand vous dépannez ce problème, vous devez vérifier la communication entre les homologues de HSRP. Une perte aléatoire et momentanée de communication de données entre les homologues est le problème le plus commun résultant en ces messages. Les changements d'état du protocole HSRP sont souvent dus à l'utilisation élevée du CPU. Si le message d'erreur est dû à l'utilisation élevée du CPU, installez un renifleur de réseau et faites un suivi du système qui entraîne l'utilisation élevée du CPU.

Il y a plusieurs causes possibles de perte de paquets HSRP entre les homologues. Les problèmes les plus communs sont les problèmes de couche physique, un trafic réseau excessif provoqué par des problèmes de spanning tree ou un trafic excessif provoqué par chaque VLAN. Comme avec l'étude de cas #1, tous les modules de dépannage s'appliquent à la résolution des changements d'état du protocole HSRP, en particulier le débogage de la couche 3 de HSRP.

Si la perte de paquets HSRP entre les homologues est due à un trafic excessif provoqué par chaque VLAN comme mentionné, vous pouvez accorder ou augmenter la suppression SPD et maintenir la taille de la file d'attente pour surmonter le problème de perte de la file d'attente d'entrée.

Afin d'augmenter la taille de SPD (Selective Packet Discard), allez au mode de configuration et exécutez ces commandes sur les commutateurs Cat6500 :

```
(config)# ip spd queue max-threshold 600
!--- Hidden Command (config)# ip spd queue min-threshold 500
```

```
!--- Hidden Command
```

Afin d'augmenter la taille de file d'attente d'attente, allez au mode d'interface VLAN et exécutez cette commande :

```
(config-if)# hold-queue 500 in
```

Après avoir augmenté la taille de SPD et de la file d'attente, vous pouvez effacer les compteurs d'interface si vous exécutez la commande clear counter interface.

Étude de cas #3 : HSRP ne reconnaît pas l'homologue

La sortie du routeur dans cette section indique un routeur qui est configuré pour le HSRP mais qui n'identifie pas ses homologues HSRP. Pour que ceci se produise, le routeur doit échouer dans la réception des paquets Hello de HSRP du routeur voisin. Quand vous dépannez ce problème, référez-vous à la section Vérification de la connectivité de la couche physique et la section Vérification de la configuration du routeur HSRP de ce document. Si la connectivité de la couche physique est correcte, vérifiez que les modes VTP ne sont pas mal adaptés.

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

Étude de cas #4 : HSRP change d'état et le commutateur signale SYS-4-P2_WARN : 1/Host <mac_address> s'affole entre le port <port_1> et le port <port_2> dans Syslog

Ces messages d'erreur peuvent apparaître :

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

Dans le logiciel version 5.5.2 et ultérieure pour Catalyst 4500/4000 et 2948G, le commutateur enregistre une adresse MAC qui se déplace si l'adresse MAC hôte se déplace deux fois en 15 secondes. Une cause courante est une boucle STP. Le commutateur rejette les paquets de ce hôte pendant environ 15 secondes afin de réduire au minimum l'incidence d'une boucle STP. Si le mouvement de l'adresse MAC entre deux ports qui est enregistré est l'adresse MAC HSRP virtuelle, le problème est sans doute que les deux routeurs HSRP entrent dans l'état active.

Si l'adresse MAC qui est enregistrée n'est pas l'adresse MAC HSRP virtuelle, le problème peut indiquer la boucle, la duplication ou la réflexion de paquets dans le réseau. Ces types de

conditions peuvent contribuer à des problèmes du protocole HSRP. Les causes les plus communes pour le mouvement d'adresses MAC sont des problèmes de spanning tree ou des problèmes de couche physique.

Lorsque vous dépannez ce message d'erreur, exécutez les étapes suivantes :

> Remarque: En outre, complétez les étapes de la section Modules de dépannage de HSRP pour les commutateurs CatOS de ce document.

1. Déterminez l'adresse MAC source (port) correcte enregistrée par le message d'erreur.
2. Déconnectez le port qui ne doit pas approvisionner l'adresse MAC hôte et contrôlez la stabilité de HSRP.
3. Documentez la topologie STP sur chaque VLAN et vérifiez qu'il n'y a pas de pannes STP.
4. Vérifiez la configuration des canaux de port.Une mauvaise configuration peut avoir comme conséquence l'affolement de messages d'erreur par l'adresse MAC hôte. Ceci est dû à la nature d'équilibrage de charge des canaux de port.

Étude de cas #5 : HSRP change d'état et le commutateur signale RTD-1-ADDR_FLAP dans Syslog

Ces messages d'erreur peuvent apparaître :

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

Ces messages d'erreur signifient qu'une adresse MAC se déplace régulièrement entre différents ports. Ces messages d'erreur s'appliquent seulement aux commutateurs Catalyst 2900XL et 3500XL. Les messages peuvent indiquer que deux routeurs HSRP ou plus sont devenus active. Les messages peuvent indiquer la source d'une boucle STP, des doublons de trames ou des paquets réfléchis.

Afin de recueillir plus d'informations au sujet des messages d'erreur, émettez la commande **debug** :

```
switch#debug ethernet-controller address

Ethernet Controller Addresses debugging is on l

*Mar 9 08:06:06: Add address 0000.0c07.ac02, on port 35 vlan 2
*Mar 9 08:06:06: 0000.0c07.ac02 has moved from port 6 to port 35 in vlan 2
*Mar 9 08:06:07: Add address 0000.0c07.ac02, on port 6 vlan 2
*Mar 9 08:06:07: 0000.0c07.ac02 has moved from port 35 to port 6 in vlan 2
*Mar 9 08:06:08: Add address 0000.0c07.ac02, on port 35 vlan 2
*Mar 9 08:06:08: 0000.0c07.ac02 has moved from port 6 to port 35 in vlan 2
*Mar 9 08:06:10: Add address 0000.0c07.ac02, on port 6 vlan 2
*Mar 9 08:06:10: 0000.0c07.ac02 has moved from port 35 to port 6 in vlan 2
```

```
*Mar 9 08:06:11: Add address 0000.0c07.ac02, on port 35 vlan 2
*Mar 9 08:06:11: 0000.0c07.ac02 has moved from port 6 to port 35 in vlan 2
*Mar 9 08:06:12: %RTD-1-ADDR_FLAP: Fast Ethernet 0/7 relearning 20 addrs per min
*Mar 9 08:06:13: Add address 0000.0c07.ac02, on port 6 vlan 2
*Mar 9 08:06:13: 0000.0c07.ac02 has moved from port 35 to port 6 in vlan 2
```

Les ports référencés par la commande **debug** sont décalés d'une valeur. Par exemple, le port 0 est Fast Ethernet 0/1. Les messages d'erreur indiquent l'affolement d'une adresse MAC entre les ports 5 et 34 sur le commutateur respectif.

> Remarque: Le message RTD-1-ADDR_FLAP peut être incorrect. Référez-vous à ces ID de bogue Cisco afin d'éliminer cette possibilité :
> - Message incorrect CSCdp81680 (clients enregistrés seulement) — RTD-1-ADDR_FLAP
> - (Clients enregistrés seulement) — cause RTD-1-ADDR_FLAP de questions du Fast EtherChannel CSCds27100 (clients enregistrés seulement) et CSCdr30113

Les causes les plus communes pour le mouvement d'adresses MAC sont des problèmes de spanning tree ou des problèmes de couche physique.

Lorsque vous dépannez ce message d'erreur, exécutez les étapes suivantes :

> Remarque: En outre, complétez les étapes de la section Modules de dépannage de HSRP pour les commutateurs CatOS de ce document.

1. Déterminez la source correcte (port) de l'adresse MAC hôte.
2. Déconnectez le port qui ne devrait pas approvisionner l'adresse MAC hôte.
3. Documentez la topologie STP sur une base per-VLAN et vérifiez qu'il n'y a pas de pannes STP.
4. Vérifiez la configuration des canaux de port.Une mauvaise configuration peut avoir comme conséquence l'affolement de messages d'erreur par l'adresse MAC hôte. Ceci est dû à la nature d'équilibrage de charge des canaux de port.

Étude de cas #6 : HSRP change d'état et le commutateur signale MLS-4-MOVEOVERFLOW:Too many moves, stop MLS for 5 sec(20000000) dans Syslog

Ces messages d'erreur peuvent apparaître :

```
switch#debug ethernet-controller address

Ethernet Controller Addresses debugging is on l

*Mar 9 08:06:06: Add address 0000.0c07.ac02, on port 35 vlan 2
*Mar 9 08:06:06: 0000.0c07.ac02 has moved from port 6 to port 35 in vlan 2
*Mar 9 08:06:07: Add address 0000.0c07.ac02, on port 6 vlan 2
*Mar 9 08:06:07: 0000.0c07.ac02 has moved from port 35 to port 6 in vlan 2
*Mar 9 08:06:08: Add address 0000.0c07.ac02, on port 35 vlan 2
*Mar 9 08:06:08: 0000.0c07.ac02 has moved from port 6 to port 35 in vlan 2
*Mar 9 08:06:10: Add address 0000.0c07.ac02, on port 6 vlan 2
*Mar 9 08:06:10: 0000.0c07.ac02 has moved from port 35 to port 6 in vlan 2
*Mar 9 08:06:11: Add address 0000.0c07.ac02, on port 35 vlan 2
*Mar 9 08:06:11: 0000.0c07.ac02 has moved from port 6 to port 35 in vlan 2
```

```
*Mar 9 08:06:12: %RTD-1-ADDR_FLAP: Fast Ethernet 0/7 relearning 20 addrs per min
*Mar 9 08:06:13: Add address 0000.0c07.ac02, on port 6 vlan 2
*Mar 9 08:06:13: 0000.0c07.ac02 has moved from port 35 to port 6 in vlan 2
```

Ces messages indiquent que le commutateur retient la même adresse MAC sur deux ports différents. Ce message n'est signalé que sur les commutateurs Catalyst 5500/5000. Émettez ces commandes afin de recueillir des informations supplémentaires au sujet du problème :

> Remarque: Les commandes mentionnées dans cette section ne sont pas documentées. Vous devez les entrer complètement. La commande **show mls notification** fournit une valeur d'adresse de table (TA). La commande **show looktable** TA-value renvoie une adresse MAC possible que vous pouvez retracer jusqu'à la racine du problème.

```
Switch (enable) show mls notification

1: (0004e8e6-000202ce) Noti Chg TA e8e6 OI 2ce (12/15) V 1
!--- This is the mod/port and VLAN. The MAC address is !--- seen on this module 12, port 15 in
VLAN 1. 2: (0004e8e6-000202cd) Noti Chg TA e8e6 OI 2cd (12/14) V 1 !--- This is the mod/port and
VLAN. The next is seen on !--- module 12, port 14 in VLAN 1.
```

Écrivez la combinaison à quatre chiffres/lettres qui apparaît après Chg TA dans la sortie de cette commande. La commande **show looktable** donne l'adresse MAC qui entraîne la génération du message d'erreur MLS TOO MANY MOVES :

```
150S_CR(S2)> (enable) show looktable e8e6

Table address: 0xe8e6, Hash: 0x1d1c, Page: 6
Entry Data[3-0]: 0x000002cd 0x00800108 0x0008c790 0x215d0005, Entry Map [00]

Router-Xtag QOS SwGrp3 Port-Index
0 0 0x0 0x2cd

Fab AgeByte C-Mask L-Mask Static SwSc HwSc EnSc AL Trap R-Mac
0 0x01 0x0000 0x0000 0 0 0 0 0 0 0

MacAge Pri-In Modify Notify IPX-Sw IPX-Hw IPX-En Valid SwGrp2 Parity2
0 0 1 0 0 0 0 1 0x0 0

Entry-Mac-Address FID SwGrp1 Parity1
00-08-c7-90-21-5d 1 0x0 1
```

L'adresse MAC 00-08-c7-90-21-5d d'entrée est l'adresse MAC qui s'affole entre les ports. Vous devez connaître l'adresse MAC afin de trouver le périphérique attentatoire. Si l'adresse MAC d'entrée est l'adresse MAC virtuelle de HSRP, le problème peut être que les deux routeurs HSRP sont entrés dans l'état active.

Les causes les plus communes pour le mouvement d'adresses MAC sont des problèmes de spanning tree ou des problèmes de couche physique.

Lorsque vous dépannez ce message d'erreur, exécutez les étapes suivantes :

> Remarque: En outre, complétez les étapes de la section Modules de dépannage de HSRP pour les commutateurs CatOS de ce document.

1. Déterminez la source correcte (port) de l'adresse MAC hôte.
2. Déconnectez le port qui ne devrait pas approvisionner l'adresse MAC hôte.

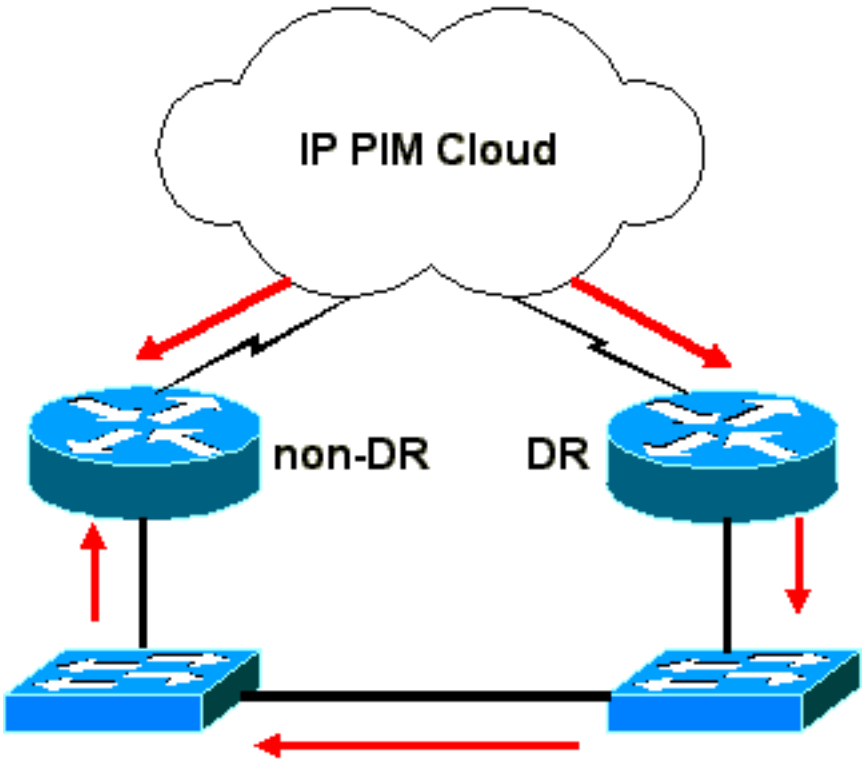
3. Documentez la topologie STP sur une base per-VLAN et vérifiez qu'il n'y a pas de pannes STP.
4. Vérifiez la configuration des canaux de port.Une mauvaise configuration peut avoir comme conséquence l'affolement de messages d'erreur par l'adresse MAC hôte. Ceci est dû à la nature d'équilibrage de charge des canaux de port.
5. Désactivez PortFast sur tous les ports qui se connectent aux périphériques autres qu'un PC ou téléphone IP afin d'éviter les boucles de pontage.

Étude de cas #7 : L'état intermittent de HSRP change sur le réseau tronqué de multidiffusion

Il y a une cause courante aux modifications anormales d'état de HSRP pour un routeur HSRP qui fait partie d'un réseau tronqué de multidiffusion. Cette cause courante réside dans la non-retransmission par le chemin inverse (RPF) détecté par le routeur non désigné (DR). C'est le routeur qui n'expédie pas le flux de trafic de multidiffusion.

Le multicast IP utilise un routeur pour expédier des données sur un LAN dans des topologies redondantes. Si plusieurs routeurs ont des interfaces sur un LAN ou VLAN, seulement un routeur transmet les données. Il n'y a aucun équilibrage de charge pour le trafic de multidiffusion sur des LAN. Tout le trafic de multidiffusion est toujours visible par chaque routeur sur un LAN. C'est également le cas si le protocole CGMP (Cisco Group Management Protocol) ou l'IGMP (Internet Group Management Protocol) snooping est configuré. Les deux routeurs doivent voir le trafic de multidiffusion afin de prendre une décision de transmission.

Ce diagramme fournit un exemple. Les lignes rouges indiquent un flux multidiffusion.



Le routeur redondant, qui est le routeur qui n'expédie pas le flux de trafic de multidiffusion, voit ces données sur l'interface de sortie pour le LAN. Le routeur redondant doit supprimer ce trafic parce qu'il arrive sur la mauvaise interface et donc échoue le contrôle RPF. Ce trafic est désigné sous le nom de trafic non-RPF, car il est reflété vers l'arrière contre le flux depuis la source. Pour ce trafic non-RPF, il y a habituellement aucun état (*, G) ou (S, G) dans le routeur redondant. Par

conséquent, aucun raccourci matériel ou logiciel ne peut être créé afin d'abandonner le paquet. Le processeur doit examiner chaque paquet de multidiffusion individuellement. Cette condition peut provoquer une transitoire du CPU sur ces routeurs ou le fonctionnement du CPU à un taux de traitement très élevé. Souvent, un taux élevé de trafic de multidiffusion sur le routeur redondant a pour conséquence que le protocole HSRP perd des paquets Hello de ses homologues et change d'état.

Par conséquent, activez les listes d'accès de matériel sur les routeurs Catalyst 6500 et 8500 qui ne gèrent pas le trafic non-RPF efficacement par défaut. Les listes d'accès empêchent le CPU de traiter le trafic non-RPF.

> Remarque: N'essayez pas de contourner ce problème avec la désactivation d'IP PIM (Protocol Independent Multicast) sur les interfaces du routeur redondant. Cette configuration peut avoir une incidence indésirable sur le routeur redondant.

Sur les routeurs de 6500/8500, il y a un moteur de liste d'accès qui active le filtrage au débit câble. Vous pouvez employer cette fonctionnalité pour gérer efficacement le trafic non-RPF pour des groupes de mode éparpillés.

Dans les versions de logiciel 6.2.1 et ultérieures, le logiciel active automatiquement le filtrage pour que le non-DR ne reçoive pas le trafic non-RPF inutile. Dans les versions antérieures du logiciel, vous devez configurer les listes d'accès manuellement. Afin de mettre en application cette solution pour les versions de logiciel antérieures à 6.2.1, placez une liste d'accès sur l'interface entrante du réseau tronqué. La liste d'accès filtre le trafic de multidiffusion qui ne provient pas du réseau tronqué. La liste d'accès est poussé vers le matériel dans le commutateur. Cette liste d'accès s'assure que le CPU ne voit jamais le paquet et permet au matériel de supprimer le trafic non-RPF.

Par exemple, supposez que vous avez deux routeurs avec deux VLAN en commun. Vous pouvez augmenter ce nombre de VLAN à autant de VLAN que nécessaire. Le routeur A est HSRP primaire pour le VLAN 1 et secondaire pour le routeur B VLAN 2. est secondaire pour le VLAN 1 et primaire pour VLAN 2. donnez le routeur A ou le routeur B une adresse IP plus élevée afin d'inciter à ce routeur le Dr. à être sûr que seulement un routeur est le DR pour tous les segments, comme indiqué dans cet exemple :

```
150S_CR(S2)> (enable) show looktable e8e6

Table address: 0xe8e6, Hash: 0x1d1c, Page: 6
Entry Data[3-0]: 0x000002cd 0x00800108 0x0008c790 0x215d0005, Entry Map [00]

Router-Xtag QOS SwGrp3 Port-Index
0 0 0x0 0x2cd

Fab AgeByte C-Mask L-Mask Static SwSc HwSc EnSc AL Trap R-Mac
0 0x01 0x0000 0x0000 0 0 0 0 0 0 0

MacAge Pri-In Modify Notify IPX-Sw IPX-Hw IPX-En Valid SwGrp2 Parity2
0 0 1 0 0 0 0 1 0x0 0

Entry-Mac-Address FID SwGrp1 Parity1
00-08-c7-90-21-5d 1 0x0 1
```

Placez cette liste d'accès sur le routeur non-DR :

```
150S_CR(S2)> (enable) show looktable e8e6

Table address: 0xe8e6, Hash: 0x1d1c, Page: 6
Entry Data[3-0]: 0x000002cd 0x00800108 0x0008c790 0x215d0005, Entry Map [00]

Router-Xtag QOS SwGrp3 Port-Index
0 0 0x0 0x2cd

Fab AgeByte C-Mask L-Mask Static SwSc HwSc EnSc AL Trap R-Mac
0 0x01 0x0000 0x0000 0 0 0 0 0 0 0

MacAge Pri-In Modify Notify IPX-Sw IPX-Hw IPX-En Valid SwGrp2 Parity2
0 0 1 0 0 0 0 1 0x0 0

Entry-Mac-Address FID SwGrp1 Parity1
00-08-c7-90-21-5d 1 0x0 1
```

Vous devriez avoir une permission pour chaque sous-réseau partagé par les deux routeurs. D'autres permissions permettent au point de rendez-vous automatique (RP) et aux groupes réservés de fonctionner correctement.

Émettez ces commandes supplémentaires afin d'appliquer les listes de contrôle d'accès (ACL) à chaque interface VLAN sur le non-DR :

- ip access-group 100 in
- no ip redirects
- no ip unreachables

Remarque: Vous devez exécuter le logiciel Catalyst 5.4(3) ou ultérieur pour que les ACL travaillent en configuration hybride.

Remarque: Les configurations de routeur redondant abordées par ce document sont redondantes extérieurement, ce qui signifie qu'il y a deux routeurs 6500 physiques. N'utilisez pas ce contournement pour la redondance interne dans laquelle deux processeurs de routage sont dans un cadre.

Étude de cas #8 : Routage et HSRP asymétriques (monodiffusion excessive du trafic dans le réseau avec les routeurs qui exécutent HSRP)

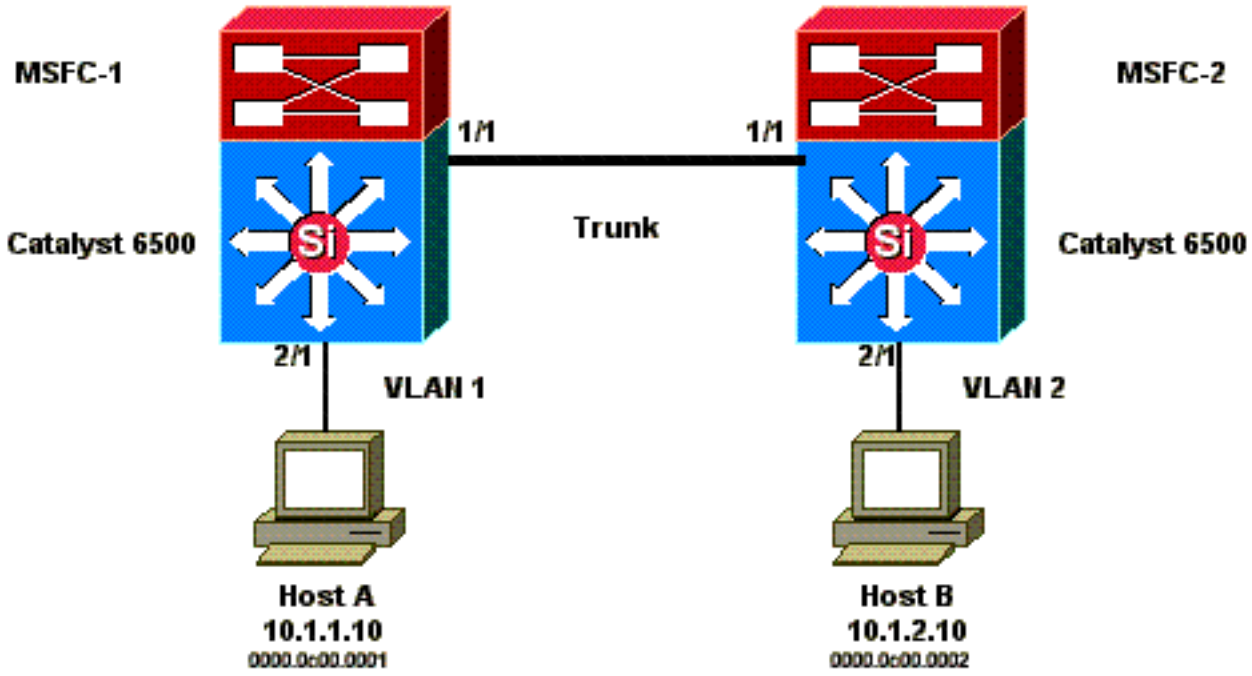
Avec le routage asymétrique, les paquets de transmission et réception suivent des chemins différents entre un hôte et l'homologue avec lesquels ils communiquent. Ce flux de paquets est le résultat de la configuration de l'équilibrage de charge entre les routeurs HSRP, basée sur la priorité HSRP, qui définissent le protocole HSRP comme étant Active ou Standby. Ce type de flux de paquets dans un environnement de commutation peut avoir comme conséquence une monodiffusion excessive inconnue. En outre, les entrées Multilayer Switching (MLS) peuvent être absentes. Une diffusion unicast excessive inconnue se produit quand le commutateur sature un paquet de monodiffusion hors de tous les ports. Le commutateur sature le paquet parce qu'il n'y a aucune entrée pour l'adresse MAC de destination. Ce comportement ne casse pas la connectivité parce que les paquets sont toujours expédiés. Mais, le comportement explique la saturation de paquets supplémentaires sur des ports hôtes. Ce cas étudie le comportement de routage asymétrique et les raisons de la monodiffusion excessive qui en résulte.

Les symptômes du routage asymétrique incluent :

- Monodiffusion excessive des paquets
- Une entrée MLS absente pour les flux
- La trace renifleur de réseau, qui montre que les paquets sur le port hôte ne sont pas destinés au hôte
- Une latence de réseau accrue avec des moteurs de réécriture des paquets au niveau de la couche L2, tels que des balanciers de charge de serveur, des dispositifs de cache web et des appareils réseauLes exemples incluent le moteur Cisco LocalDirector et Cisco Cache.
- Les paquets abandonnés sur les serveurs et les postes de travail connectés qui ne peuvent pas gérer la charge de trafic supplémentaire de la monodiffusion

> Remarque: Le délai de vieillissement du cache ARP par défaut sur un routeur est de quatre heures. Le délai de vieillissement par défaut de l'entrée de mémoire de contenu adressable (CAM, Content-Addressable Memory) du commutateur est de cinq minutes. Le délai de vieillissement ARP des postes de travail hôtes n'est pas significatif pour cette discussion. Mais, l'exemple définit le délai de vieillissement ARP à quatre heures.

Ce diagramme illustre ce problème. Cette topologie inclut les cartes de commutation multicouche de la gamme Cisco Catalyst 6500 (MSFC) dans chacun commutateur. Bien que cet exemple utilise les MSFC, vous pouvez utiliser tout routeur plutôt que la MSFC. Parmi les exemples de routeur que vous pouvez utiliser figurent le commutateur de route (RSM), le routeur de commutation Gigabit (GSR) et Cisco 7500. Les hôtes sont directement connectés aux ports sur le commutateur. Les commutateurs sont interconnectés par une liaison agrégée qui porte le trafic pour le VLAN 1 et VLAN 2.



Ces sorties sont des extraits de la configuration de commande de **show standby de** chaque MSF.

MSFC1

```
interface Vlan 1
   mac-address 0003.6bf1.2a01
    ip address 10.1.1.2 255.255.255.0
    no ip redirects
```

```
    standby 1 ip 10.1.1.1
    standby 1 priority 110

interface Vlan 2
    mac-address 0003.6bf1.2a01
    ip address 10.1.2.2 255.255.255.0
    no ip redirects
    standby 2 ip 10.1.2.1

MSFC1#show standby
Vlan1 - Group 1
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.696
Hot standby IP address is 10.1.1.1 configured
Active router is local
Standby router is 10.1.1.3 expires in 00:00:07
Standby virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:20:40
Vlan2 - Group 2
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.776
Hot standby IP address is 10.1.2.1 configured
Active router is 10.1.2.3 expires in 00:00:09, priority 110
Standby router is local
4 state changes, last state change 00:00:51
MSFC1#exit
Console> (enable)
```

MSFC2

```
interface Vlan 1
    mac-address 0003.6bf1.2a02
    ip address 10.1.1.3 255.255.255.0
    no ip redirects
    standby 1 ip 10.1.1.1

interface Vlan 2
    mac-address 0003.6bf1.2a02
    ip address 10.1.2.3 255.255.255.0
    no ip redirects
    standby 2 ip 10.1.2.1
    standby 2 priority 110

MSFC2#show standby
Vlan1 - Group 1
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.242
Hot standby IP address is 10.1.1.1 configured
Active router is 10.1.1.2 expires in 00:00:09, priority 110
Standby router is local
7 state changes, last state change 00:01:17
Vlan2 - Group 2
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.924
Hot standby IP address is 10.1.2.1 configured
Active router is local
Standby router is 10.1.2.2 expires in 00:00:09
Standby virtual mac address is 0000.0c07.ac02
2 state changes, last state change 00:40:08
```

```
MSFC2#exit
```

Remarque: Sur MSFC1, le VLAN 1 est dans l'état active du protocole HSRP et le VLAN 2 dans l'état standby. Sur MSFC2, le VLAN 2 est dans l'état active du protocole HSRP et le VLAN 1 dans l'état standby. La passerelle par défaut de chaque hôte est l'adresse IP de secours respective.

1. Au départ, tous les caches sont vides. Le hôte A utilise MSFC1 en tant que passerelle par défaut. Le hôte B utilise MSFC2.**Tables d'adresses ARP et MAC avant le lancement de la commande Ping** Remarque: Pour des raisons de brièveté, l'adresse MAC du commutateur 1 pour le routeur HSRP et l'adresse MAC ne sont pas incluses dans les autres tableaux qui apparaissent dans cette section.
2. Le hôte A envoie des pings à l'hôte B, ce qui signifie que l'hôte A envoie un paquet d'écho ICMP. Puisque chaque hôte réside sur un VLAN distinct, l'hôte A transmet ses paquets qui sont destinés à l'hôte B à sa passerelle par défaut. Pour que ce processus se produise, l'hôte A doit envoyer un ARP afin de résoudre son adresse MAC de passerelle par défaut, 10.1.1.1.**Tables d'adresses ARP et MAC après que l'hôte A envoie un ARP pour la passerelle par défaut**
3. MSFC1 reçoit le paquet, réécrit le paquet, et en avant le paquet pour héberger le B. afin de réécrire le paquet, MSFC1 envoie une demande d'ARP d'hôte B parce que l'hôte réside outre d'une interface directement connectée. MSFC2 doit encore recevoir des paquets dans ce flux. Quand MSFC1 reçoit la réponse ARP de l'hôte B, les deux commutateurs retiennent le port source associé à l'hôte B.**Tables d'adresses ARP et MAC après que l'hôte A envoie un paquet à la passerelle par défaut et que MSFC1 envoie un ARP pour l'hôte B**
4. Le hôte B reçoit le paquet d'écho du hôte A par MSFC1. L'hôte B doit maintenant envoyer une réponse d'écho à l'hôte A. Puisque l'hôte A réside sur un VLAN distinct, l'hôte B transmet la réponse par sa passerelle par défaut, MSFC2. Afin d'expédier le paquet par MSFC2, l'hôte B doit envoyer un ARP pour son adresse IP de passerelle par défaut, 10.1.2.1.**Tables d'adresses ARP et MAC après que l'hôte B envoie un ARP pour sa passerelle par défaut**
5. L'hôte B transmet maintenant le paquet de réponse en écho à MSFC2. Le MSFC2 envoie une demande d'ARP de l'hôte A parce qu'il est directement connecté sur VLAN 1. remplit Comm2 sa table d'adresse MAC avec l'adresse MAC de l'hôte B.**Tables d'adresses ARP et MAC après que le paquet d'écho a été reçu par l'hôte A**
6. La réponse en écho atteint l'hôte A et le flux est complet.

Conséquences du routage asymétrique

Considérez le cas du ping continu de l'hôte B par l'hôte A. Remember qui hébergent A envoie le paquet d'écho à MSFC1, et l'hôte B envoie la réponse d'écho au MSFC2, qui est dans un état asymétrique de routage. La seule fois où le commutateur 1 retient l'adresse MAC source de l'hôte B est quand l'hôte B répond à une requête ARP de MSFC1. C'est parce que le hôte B utilise MSFC2 comme sa passerelle par défaut et n'envoie pas les paquets à MSFC1 et, par conséquent, au commutateur 1. Puisque le délai d'attente ARP est de quatre heures par défaut, par défaut, le commutateur 1 vieillit l'adresse MAC du hôte B après cinq minutes. Le commutateur 2 vieillit l'hôte A après cinq minutes. En conséquence, le commutateur 1 doit traiter n'importe quel paquet avec une destination MAC de l'hôte B comme une monodiffusion inconnue. Le commutateur inonde le paquet qui vient de l'hôte A et est destiné à l'hôte B de tous les ports. En outre, parce qu'il n'y a pas d'hôte B d'entrée avec l'adresse MAC dans le commutateur 1, il n'y a pas non plus d'entrée

MLS.

Tables d'adresses ARP et MAC après 5 minutes de ping continu de l'hôte B par l'hôte A

Table ARP Hôte A	Commutez 1 port VLAN MAC de Tableau d'adresse MAC	Table ARP MSFC1	Table ARP MSFC2	Comm2 port VLAN MAC de Tableau d'adresse MAC	Table ARP Hôte B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 : 0003.6bf1.2a01
10.1.1.3 : 0003.6bf1.2a0		10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001		10.1.2.1 : 0000.0c07.ac01

Les paquets de réponse d'écho qu'une expérience provenue d'hôte B la même question après que l'entrée d'adresse MAC pour l'hôte A vieillisse sur l'hôte B du commutateur 2. en avant la réponse d'écho au MSFC2, qui consécutivement conduit le paquet et l'envoie sur le VLAN 1. Le commutateur n'a pas un hôte d'entrée A dans la table d'adresse MAC et doit inonder le paquet de tous les ports dans le VLAN 1.

Les problèmes de routage asymétrique ne cassent pas la connectivité. Mais, le routage asymétrique peut entraîner une diffusion unicast excessive et des entrées MLS manquantes. Il existe trois modifications de configuration qui peuvent remédier à cette situation :

- Ajustez la durée de vieillissement MAC sur les commutateurs respectifs à 14.400 secondes (quatre heures) ou plus.
- Changez le délai d'attente ARP sur les routeurs à cinq minutes (300 secondes).
- Changez la durée de vieillissement MAC et le délai d'attente ARP à la même valeur d'attente.

La méthode préférable est de changer la durée de vieillissement MAC à 14.400 secondes. Voici les directives de configuration :

- CatOS :set cam agingtime vlan_aging_time_in_msec
- Logiciel Cisco IOS/2900XL/3500XL :mac-address-table aging-time seconds [vlan vlan_id]

Étude de cas #9 : l'adresse IP virtuelle de HSRP est signalée comme étant une adresse IP différente

Le message d'erreur STANDBY-3-DIFFVIP1 se produit quand il y a une fuite inter-VLAN en raison de boucles de pontage dans le commutateur.

Si vous recevez ce message d'erreur et qu'il existe une fuite inter-VLAN en raison de boucles de pontage dans le commutateur, complétez ces étapes afin de résoudre l'erreur :

1. Identifiez le chemin que les paquets devraient prendre entre les nœuds d'extrémité.S'il y a un routeur sur ce chemin, complétez ces étapes :Dépannez le chemin depuis le premier commutateur jusqu'au routeur.Dépannez le chemin depuis le routeur jusqu'au deuxième commutateur.
2. Connectez-vous à chaque commutateur sur le chemin et contrôlez l'état des ports qui sont utilisés sur le chemin entre les nœuds d'extrémité.

Étude de cas #10 : HSRP entraîne une violation de MAC sur un port sécurisé

Quand la sécurité du port est configurée sur les ports de commutation qui sont connectés aux routeurs activés par HSRP, cela entraîne une violation MAC puisque vous ne pouvez pas avoir la même adresse MAC sécurisée sur plus d'une interface. Une violation de la sécurité se produit sur un port sécurisé dans une de ces situations :

- Le nombre maximal d'adresses MAC sécurisées est ajouté à la table d'adresses et un poste dont l'adresse MAC n'est pas dans la table d'adresses essaye d'accéder à l'interface.
- Une adresse qui est retenue ou configurée sur une interface sécurisée est vue sur une autre interface sécurisée dans le même VLAN.

Par défaut, une violation de la sécurité du port provoque le passage de l'interface de commutation à un état désactivé suite à une erreur et à son arrêt immédiat, ce qui bloque les messages d'état de HSRP entre les routeurs.

Solution de contournement

- Émettez la commande standby use-bia sur les routeurs. Ceci force les routeurs à utiliser une adresse gravée en mémoire pour le HSRP au lieu de l'adresse MAC virtuelle.
- Désactivez la sécurité du port sur les ports de commutation qui se connectent aux routeurs activés par HSRP.

Étude de cas #11 : %le matériel %Interface ne peut pas prendre en charge plusieurs groupes

Si plusieurs groupes HSRP sont créés sur l'interface, ce message d'erreur est reçu :

```
interface Vlan 1
    mac-address 0003.6bf1.2a02
    ip address 10.1.1.3 255.255.255.0
    no ip redirects
    standby 1 ip 10.1.1.1

interface Vlan 2
    mac-address 0003.6bf1.2a02
    ip address 10.1.2.3 255.255.255.0
    no ip redirects
    standby 2 ip 10.1.2.1
    standby 2 priority 110

MSFC2#show standby
Vlan1 - Group 1
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.242
Hot standby IP address is 10.1.1.1 configured
Active router is 10.1.1.2 expires in 00:00:09, priority 110
Standby router is local
7 state changes, last state change 00:01:17
Vlan2 - Group 2
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.924
Hot standby IP address is 10.1.2.1 configured
Active router is local
Standby router is 10.1.2.2 expires in 00:00:09
Standby virtual mac address is 0000.0c07.ac02
```

```
2 state changes, last state change 00:40:08
MSFC2#exit
```

Ce message d'erreur est reçu en raison de la limitation matérielle sur quelques routeurs ou commutateurs. Il n'est pas possible de surmonter la limitation par une méthode logicielle. Le problème est que chaque groupe HSRP utilise une adresse MAC supplémentaire sur l'interface de sorte que la puce Ethernet MAC doit prendre en charge des adresses MAC programmables multiples pour activer plusieurs groupes HSRP.

Le contournement est d'utiliser la commande de configuration d'interface **standby use-bia**, qui utilise l'adresse gravée en mémoire (BIA) de l'interface comme son adresse MAC virtuelle au lieu de l'adresse MAC pré-assignée.

Modules de dépannage de HSRP pour les commutateurs CatOS

A. Vérifiez la configuration de routeur de HSRP

1. Vérifiez la seule adresse IP d'interface de routeur

Vérifiez que chaque routeur HSRP a une seule adresse IP pour chaque sous-réseau par interface. En outre, vérifiez que le protocole de ligne de chaque interface est up. Afin de vérifier rapidement l'état actuel de chaque interface, émettez la commande show ip interface brief. Voici un exemple :

```
Router_1#show ip interface brief
Interface                  IP-Address       OK?  Method    Status      Protocol
Vlan1                   192.168.1.1    YES   manual        up             up
Vlan10                  192.168.10.1    YES   manual        up             up
Vlan11                  192.168.11.1    YES   manual        up             up

Router_2#show ip interface brief
Interface                  IP-Address       OK?  Method   Status       Protocol
Vlan1                   192.168.1.2    YES   manual      up             up
Vlan10                  192.168.10.2   YES   manual      up             up
Vlan11                  192.168.11.2   YES   manual      up             up
```

2. Vérifiez les adresses IP (de HSRP) et les nombres de groupe de veille de réserve

Vérifiez que les adresses IP de secours configurées (HSRP) et les numéros de groupe de secours correspondent à chaque routeur participant au protocole HSRP. Une erreur d'assortiment des groupes de secours ou des adresses de secours HSRP peut provoquer des problèmes de HSRP. La commande show standby détaille la configuration des groupes de secours et des adresses IP de secours de chaque interface. Voici un exemple :

```
Router_1#show standby
Vlan10 - Group 10
  Local state is Active, priority 110, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:00.216
  Hot standby IP address is 192.168.10.100 configured
  Active router is local
  Standby router is 192.168.10.2 expires in 00:00:08
  Standby virtual mac address is 0000.0c07.ac0a
  8 state changes, last state change 00:18:04
```

```
Vlan11 - Group 11
  Local state is Active, priority 110, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:01.848
  Hot standby IP address is 192.168.11.100 configured
  Active router is local
  Standby router is 192.168.11.2 expires in 00:00:08
  Standby virtual mac address is 0000.0c07.ac0b
  2 state changes, last state change 00:04:45


Router_2#show standby
Vlan10 - Group 10
  Local state is Standby, priority 109, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:01.710
  Hot standby IP address is 192.168.10.100 configured
  Active router is 192.168.10.1 expires in 00:00:09, priority 110
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac0a
  9 state changes, last state change 00:20:22

Vlan11 - Group 11
  Local state is Standby, priority 109, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.506
  Hot standby IP address is 192.168.11.100 configured
  Active router is 192.168.11.1 expires in 00:00:09, priority 110
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac0b
  4 state changes, last state change 00:07:07
```

3. Vérifiez que l'adresse IP de réserve (de HSRP) est différente par interface

Vérifiez que l'adresse IP HSRP de secours est unique par rapport à l'adresse IP configurée sur chaque interface. La commande show standby est une référence rapide pour visualiser ces informations. Voici un exemple :

```
Router_1#show standby
Vlan10 - Group 10
  Local state is Active, priority 110, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:00.216
  Hot standby IP address is 192.168.10.100 configured
  Active router is local
  Standby router is 192.168.10.2 expires in 00:00:08
  Standby virtual mac address is 0000.0c07.ac0a
  8 state changes, last state change 00:18:04

Vlan11 - Group 11
  Local state is Active, priority 110, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:01.848
  Hot standby IP address is 192.168.11.100 configured
  Active router is local
  Standby router is 192.168.11.2 expires in 00:00:08
  Standby virtual mac address is 0000.0c07.ac0b
  2 state changes, last state change 00:04:45

Router_2#show standby
```

```
Vlan10 - Group 10
  Local state is Standby, priority 109, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:01.710
  Hot standby IP address is 192.168.10.100 configured
  Active router is 192.168.10.1 expires in 00:00:09, priority 110
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac0a
  9 state changes, last state change 00:20:22

Vlan11 - Group 11
  Local state is Standby, priority 109, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:02.506
  Hot standby IP address is 192.168.11.100 configured
  Active router is 192.168.11.1 expires in 00:00:09, priority 110
  Standby router is local
  Standby virtual mac address is 0000.0c07.ac0b
  4 state changes, last state change 00:07:07
```

4. Quand utiliser la commande standby use-bia

Àmoins que le protocole HSRP ne soit configuré sur une interface Token Ring, n'utilisez que la commande standby use-bia dans des circonstances spéciales. Cette commande indique au routeur d'utiliser son BIA au lieu de l'adresse MAC virtuelle de HSRP pour le groupe HSRP. Sur un réseau Token Ring, si SRB (source-route bridging) est en service, la commande standby use-bia permet au nouveau routeur actif de mettre à jour le cache RIF (Routing Information Field) hôte avec un ARP gratuit. Mais, pas toutes les implémentations de hôte gèrent correctement l'ARP gratuit. Un autre obstacle à la commande standby use-bia implique le proxy ARP. Un routeur de secours ne peut pas couvrir la base de données ARP du proxy perdu d'un routeur actif défaillant.

5. Vérifiez la configuration de liste d'accès

Vérifiez que les listes d'accès qui sont configurées sur tous les homologues de HSRP ne filtrent aucune adresse HSRP configurées sur leurs interfaces. Spécifiquement, vérifiez l'adresse de multidiffusion qui est utilisée pour envoyer le trafic à tous les routeurs sur un sous-réseau (224.0.0.2). En outre, vérifiez que le trafic UDP qui est destiné au port 1985 de HSRP n'est pas filtré. Le protocole HSRP Utilise cette adresse et port pour envoyer des paquets Hello entre les homologues. Émettez la commande show access-lists comme référence rapide pour noter les listes d'accès configurées sur le routeur. Voici un exemple :

```
Router_1#show access-lists
Standard IP access list 77
    deny   167.19.0.0, wildcard bits 0.0.255.255
    permit any
Extended IP access list 144
    deny pim 238.0.10.0 0.0.0.255 any
    permit ip any any (58 matches)
```

6. Seules configurations de routeur d'examen (MSM et 4232-L3)

> Remarque: Le commutateur multicouche (MSM) pour Catalyst 6500/6000 et la lame 4232-L3 pour Catalyst 4000 ont des configurations particulières. Quand vous dépannez les problèmes du protocole HSRP, vérifiez la configuration de non seulement le 4232-L3 ou MSM, mais également du port de commutation contigu. Si vous négligez de configurer correctement les ports de commutation contigus, des problèmes d'instabilité de HSRP et

d'autres problèmes de connectivité peuvent résulter. Les message d'erreur pour un doublon d'adresse IP HSRP est le message le plus courant associé à une configuration incorrecte de ces modules matériels.

Référez-vous à ces documents pour plus d'informations :

- Note d'installation et de configuration pour le module de services de la couche 3 de Catalyst 4000
- Note d'installation/configuration de MSM de la gamme Catalyst 6000

B. Vérifiez le Fast EtherChannel et la configuration de jonction de Catalyst

1. Vérifiez la configuration de jonction

Si une liaison agrégée est utilisée pour connecter les routeurs de HSRP, vérifiez les configurations d'agrégation sur les routeurs et commutateurs. Il existe cinq modes d'agrégation possibles :

- sur
- desirable
- automatique
- outre de
- nonegotiate

Vérifiez que les modes d'agrégation qui sont configurés fournissent la méthode d'agrégation désirée.

Utilisez la configuration desirable pour des connexions commutateur à commutateur quand vous dépannez les problèmes de HSRP. Cette configuration peut isoler des problèmes où des ports de commutation ne peuvent pas établir correctement des liaisons agrégées. Définissez une configuration routeur à commutateur comme nonegotiate parce que la plupart des routeurs de Cisco IOS ne prennent pas en charge la négociation d'une liaison agrégée.

Pour le mode d'agrégation IEEE 802.1Q (dot1q), vérifiez que les deux côtés de la liaison agrégée sont configurés pour utiliser le même VLAN natif. Puisque les produits Cisco ne marquent pas le VLAN natif par défaut, une non-correspondance des configurations de VLAN natif se traduit par une absence de connectivité sur des VLAN mal adaptés. Enfin, vérifiez que la liaison agrégée est configurée pour porter les VLAN configurés sur le routeur et que les VLAN ne sont pas élagués ni dans l'état STP pour les ports connectés au routeur. Émettez la commande **show trunk mod/port** pour une référence rapide qui montre ces informations. Voici un exemple :

```
Switch_1> (enable) show trunk 2/11
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/11     desirable    isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/11     1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
```

```
 2/11     1-2

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
2/11     1-2

Switch_2> (enable) show trunk 2/10
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/10     desirable    isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/10     1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 2/10     1-2

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
2/10     1-2

Switch_1> (enable) show trunk 2/11
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/11     nonegotiate isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/11     1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 2/11     1-2

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 2/11     1-2

Switch_1> (enable) show trunk 2/11
Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 2/11     nonegotiate  dot1q          trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 2/11     1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 2/11     1-2

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 2/11     1-2
```

2. Vérifiez la configuration de Fast EtherChannel (port creusant des rigoles)

Si un canal de port est utilisé pour connecter les routeurs de HSRP, vérifiez la configuration d'EtherChannel sur les routeurs et les commutateurs. Configurez un canal de port commutateur à commutateur comme desirable au moins d'un côté. L'autre côté peut être dans l'un de ces modes :

- sur
- desirable
- automatique

Voici un exemple :

```
Switch_1> (enable) show port channel
Port  Status     Channel              Admin Ch
                 Mode                 Group Id
----- ---------- -------------------- ----- -----
 1/1  connected  desirable silent       16   769
 1/2  connected  desirable silent       16   769
----- ---------- -------------------- ----- -----
Port  Device-ID                       Port-ID                   Platform
----- ------------------------------ ------------------------- ----------------
 1/1  SCA031700TR                    1/1                       WS-C6509
 1/2  SCA031700TR                    1/2                       WS-C6509
----- ------------------------------ ------------------------- ----------------
Switch_2> (enable) show port channel
Port  Status     Channel              Admin Ch
                 Mode                 Group Id
----- ---------- -------------------- ----- -----
 1/1  connected  desirable silent        29   769
 1/2  connected  desirable silent        29   769
----- ---------- -------------------- ----- -----
Port  Device-ID                       Port-ID                   Platform
----- ------------------------------ ------------------------- ----------------
 1/1  TBA03501066                    1/1                       WS-C6506
 1/2  TBA03501066                    1/2                       WS-C6506
----- ------------------------------ ------------------------- ----------------
```

[3 Exemples supplémentaires de configuration des canaux et des liaisons agrées]

Référez-vous à configurer l'EtherChannel entre le Catalyst 4500/4000, 5500/5000, et 6500/6000 de Commutateurs qui exécutent le logiciel système de CatOS.

4. Étudiez le Tableau d'expédition d'adresse MAC de commutateur

Vérifiez que les entrées de la table d'adresses MAC existent sur le commutateur pour les routeurs de HSRP pour l'adresse MAC virtuelle de HSRP et les BIA physiques. La commande **show standby** sur le routeur fournit l'adresse MAC virtuelle. La commande **show interface** fournit le BIA physique. Voici des exemples de sortie :

```
Router_1#show standby
Vlan1 - Group 1
  Local state is Active, priority 100
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:01.820
  Hot standby IP address is 10.1.1.254 configured
  Active router is local
  Standby router is 10.1.1.2 expires in 00:00:07
  Standby virtual mac address is 0000.0c07.ac01
  2 state changes, last state change 00:50:15
Vlan2 - Group 2
  Local state is Active, priority 200, may preempt
  Hellotime 3 holdtime 10
  Next hello sent in 00:00:00.724
  Hot standby IP address is 10.2.1.254 configured
```

```
  Active router is local
  Standby router is 10.2.1.2 expires in 00:00:09
  Standby virtual mac address is 0000.0c07.ac02
  6 state changes, last state change 00:07:59
Switch_1> (enable) show cam 00-00-0c-07-ac-01
* = Static Entry + = Permanent Entry # = System Entry R = Router Entry X = Port Security
Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ----------------------------------------
1     00-00-0c-07-ac-01  R          15/1 [ALL]
Total Matching CAM Entries Displayed = 1
Switch_1> (enable) show cam 00-00-0c-07-ac-02
* = Static Entry  + = Permanent Entry  # = System Entry R = Router Entry X = Port Security
Entry
VLAN  Dest MAC/Route Des    [CoS]  Destination Ports or VCs / [Protocol Type]
----  ------------------    -----  ----------------------------------------
2     00-00-0c-07-ac-02  R          15/1 [ALL]
Total Matching CAM Entries Displayed = 1
```

Soyez sûr de contrôler la durée de vieillissement de la mémoire CAM afin de déterminer à quelle rapidité les entrées sont vieillies. Si la durée est égale à la valeur configurée pour le retard de retransmission STP, qui est de 15 secondes par défaut, il y a une forte possibilité qu'il y ait une boucle STP dans le réseau. Voici un exemple de sortie de commande :

```
Switch_1> (enable) show cam agingtime
VLAN    1 aging time = 300 sec
VLAN    2 aging time = 300 sec
VLAN 1003 aging time = 300 sec
VLAN 1005 aging time = 300 sec

Switch_2> (enable) show cam agingtime
VLAN    1 aging time = 300 sec
VLAN    2 aging time = 300 sec
VLAN 1003 aging time = 300 sec
VLAN 1005 aging time = 300 sec
```

C. Vérifiez la Connectivité de couche physique

Si plusieurs routeurs dans un groupe HSRP deviennent actifs, ces routeurs ne reçoivent pas uniformément les paquets Hello des autres homologues de HSRP. Des problèmes de couche physique peuvent empêcher le passage cohérent du trafic entre des homologues et provoquer ce scénario. Soyez sûr de vérifier la connectivité physique et la connectivité IP entre les homologues HSRP quand vous dépannez HSRP. Émettez la commande show standby afin de vérifier la connectivité. Voici un exemple :

```
Router_1#show standby
Vlan10 - Group 10
  Local state is Active, priority 110, may preempt
  Hellotime 3 holdtime 10
  Hot standby IP address is 192.168.10.100 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac0a
  12 state changes, last state change 00:00:48

Vlan11 - Group 11
  Local state is Active, priority 110, may preempt
  Hellotime 3 holdtime 10
  Hot standby IP address is 192.168.11.100 configured
 Active router is local
```

```
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac0b
  6 state changes, last state change 00:00:48
Router_2#show standby
Vlan10 - Group 10
  Local state is Active, priority 109, may preempt
  Hellotime 3 holdtime 10
  Hot standby IP address is 192.168.10.100 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac0a
  15 state changes, last state change 00:01:18

Vlan11 - Group 11
  Local state is Active, priority 109, may preempt
  Hellotime 3 holdtime 10
  Hot standby IP address is 192.168.11.100 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac0b
  10 state changes, last state change 00:01:18
```

1. Contrôler l'état de l'interface

Contrôlez les interfaces. Vérifiez que toutes les interfaces configurées pour HSRP sont up/up, comme le montre cet exemple :

```
Router_1#show ip interface brief
Interface                  IP-Address      OK? Method Status                      Protocol
Vlan1                      10.1.1.1            YES manual administratively down   down
Vlan2                      10.2.1.1            YES manual up                      up

Router_2#show ip interface brief
Interface                  IP-Address      OK? Method Status              Protocol
Vlan1                      10.1.1.2            YES manual up                  up
Vlan2                      10.2.1.2            YES manual down                down
```

Si des interfaces sont administrativement down/down, écrivez le mode de configuration sur le routeur et émettez la commande no shutdown spécifique à l'interface. Voici un exemple :

```
Router_1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_1(config)# interface vlan 1
Router_1(config-if)# no shutdown
Router_1(config-if)# ^Z

Router_1#show ip interface brief
Interface                  IP-Address      OK? Method Status                    Protocol
Vlan1                      10.1.1.1            YES manual up                    down
Vlan2                      10.2.1.1            YES manual up                    up
```

Si des interfaces sont down/down ou up/down, passez en revue le journal des avis de changement d'interface. Pour les commutateurs basés sur le logiciel Cisco IOS, les messages suivants apparaissent pour des situations de liaisons up/down :

```
%LINK-3-UPDOWN: Interface "interface", changed state to up
%LINK-3-UPDOWN: Interface "interface", changed state to down

Router_1#show log
3d04h: %STANDBY-6-STATECHANGE: Standby: 0: Vlan2 state Active-> Speak
```

```
3d04h: %LINK-5-CHANGED: Interface Vlan2, changed state to down
3d04h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to down
```

Inspectez les ports, les câbles et tous les émetteurs-récepteurs ou autres périphériques qui sont entre les homologues de HSRP. Est-ce que quelqu'un a retiré ou desserré des connexions ? Y a-t-il des interfaces qui perdent une liaison à plusieurs reprises ? Les types de câble appropriés sont-ils utilisés ? Examinez les interfaces pour déceler toute erreur, comme indiqué dans cet exemple :

```
Router_1#show interface vlan2
Vlan2 is down, line protocol is down
  Hardware is Cat5k RP Virtual Ethernet, address is 0030.f2c9.5638 (bia 0030.f2c9.5638)
  Internet address is 10.2.1.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     155314 packets input, 8259895 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     8185 packets output, 647322 bytes, 0 underruns
     0 output errors, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

2. Modification et erreurs de port de lien

Contrôlez les modifications de liaison aux ports de commutateur et autres erreurs. Émettez ces commandes et passez en revue la sortie :

- show logging buffer
- show port
- show mac

Ces commandes vous aident à déterminer s'il y a un problème de connectivité entre les commutateurs et d'autres périphériques.

Ces messages sont normaux pour des situations de liaisons up/down :

```
PAGP-5-PORTTOSTP:Port [dec]/[dec] joined bridge port [dec]/[chars]
PAGP-5-PORTFROMSTP: Port [dec]/[dec] left bridge port [dec]/[chars]

Switch_1> (enable) show logging buffer
2001 Jan 08 20:37:24 %PAGP-5-PORTTOSTP:Port 2/1 joined bridge port 2/1
2001 Jan 08 20:37:25 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
2001 Jan 08 20:37:25 %PAGP-5-PORTTOSTP:Port 2/3 joined bridge port 2/3
2001 Jan 08 20:37:25 %PAGP-5-PORTTOSTP:Port 2/11 joined bridge port 2/11
2001 Jan 08 20:46:39 %PAGP-5-PORTTOSTP:Port 2/12 joined bridge port 2/12
2001 Jan 08 20:46:29 %PAGP-5-PORTFROMSTP:Port 2/11 left bridge port 2/11
2001 Jan 08 20:46:29 %PAGP-5-PORTFROMSTP:Port 2/12 left bridge port 2/12
2001 Jan 08 20:47:05 %DTP-5-TRUNKPORTON:Port 2/11 has become isl trunk
2001 Jan 08 20:52:15 %PAGP-5-PORTTOSTP:Port 2/11 joined bridge port 2/11
2001 Jan 08 22:18:24 %DTP-5-TRUNKPORTON:Port 2/12 has become isl trunk
```

```
2001 Jan 08 22:18:34 %PAGP-5-PORTTOSTP:Port 2/12 joined bridge port 2/12
```

Émettez la commande **show port** afin de déterminer l'état de fonctionnement général d'un port. Voici un exemple :

```
Switch_1> (enable) show port status 2/11
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
2/11                     connected  trunk      normal a-full a-100 10/100BaseTX
```

L'état du port est-il connected, notconnect ou errdisable ? Si l'état est notconnect, vérifiez que le câble est branché des deux côtés. Vérifiez que le câble approprié est utilisé. Si l'état est errdisable, passez en revue les compteurs pour déceler des erreurs excessives. Référez-vous à Récupération de l'état de port errDisable sur les plates-formes CatOS pour plus d'informations.

Pour quel VLAN ce port est-il configuré ? Soyez sûr que l'autre côté de la connexion est configuré pour le même VLAN. Si la liaison est configurée pour être une liaison agrégée (trunk), soyez sûr que les deux côtés transportent les mêmes VLAN.

Quelle est la configuration de vitesse et de duplex ? Si la configuration est précédée de a-, le port est configuré pour négocier automatiquement la vitesse et le duplex. Sinon, l'administrateur réseau a prédéterminé cette configuration. Pour configurer la vitesse et le duplex d'une liaison, les paramètres des deux côtés de la liaison doivent correspondre. Si un port de commutation est configuré pour l'autonégociation, l'autre côté de la liaison doit également l'être. Si un côté est codé en dur à une vitesse et un duplex spécifiques, l'autre côté doit également l'être. Si vous laissez un côté autonégocier tandis que l'autre est codé en dur, vous cassez le processus d'autonégociation.

```
Switch_1> (enable) show port counters 2/11
Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 2/11  0          0          0          0          0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 2/11          0          0          0          0         0         0         -

Last-Time-Cleared
--------------------------
Fri Jan 5 2001, 13:30:45
```

Y a-t-il beaucoup de Align-Err, FCS-Err ou Runts ? Cela indique une erreur de correspondance de vitesse ou de duplex entre le port et le périphérique de connexion. Changez les paramètres de vitesse et de duplex pour ce port afin de corriger ces erreurs.

Émettez la commande **show mac** afin de vérifier que le port fait circuler le trafic. Les colonnes Rcv- et Xmit- indiquent le nombre de paquets de monodiffusion, multidiffusion et de diffusion qui sont reçus et transmis sur un port particulier. Les compteurs inférieurs indiquent combien de paquets sont jetés ou perdus et s'ils font partie du trafic entrant ou sortant. Lrn-Discrd, In-Lost et Out-Lost comptent le nombre de paquets qui sont expédiés ou abandonnés de manière erronée en raison de mémoires tampons insuffisantes.

```
Switch_1> (enable) show mac 2/11
Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
2/11                     9786                 9939                 2678
Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
```

```
-------- ------------------- ------------------- --------------------
 2/11                    587                55517                  148

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
 2/11                2354136              7206386

MAC      Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
 2/11             0          -         13          0          0          0

Last-Time-Cleared
--------------------------
Fri Jan 5 2001, 13:30:45
```

3. Vérifiez la connectivité IP

Vérifiez la connectivité IP. Émettez un ping IP du routeur associé. Ceci aide à exposer toute perte de connectivité momentanée. Un ping étendu est seulement disponible dans le mode enable. Voici un exemple de sortie de commande :

```
router_1#ping
Protocol [ip]:
Target IP address: 10.2.1.2
Repeat count [5]: 1000
Datagram size [100]: 1500
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1000, 1500-byte ICMP Echos to 10.2.1.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 4/4/20 ms
```

Émettez le ping de chaque routeur HSRP à ses homologues afin de déterminer l'emplacement de la panne de connectivité.

4. Vérifier l'absence de liaison unidirectionnelle

Examinez le commutateur pour déceler toute liaison unidirectionnelle entre les homologues de HSRP. Une liaison unidirectionnelle se produit chaque fois que le trafic transmis par un équipement local sur une liaison est reçu par le voisin, mais que le trafic transmis par le voisin n'est pas reçu par l'équipement local. Les versions ultérieures de CatOS ont une fonctionnalité qui peut détecter une liaison unidirectionnelle. Cette fonctionnalité est appelée « mode agressif UDLD » (UniDirectional Link Detection). L'utilisation de UDLD est seulement possible si les deux

côtés de la connexion prennent en charge la fonctionnalité. Le mode agressif UDLD fonctionne au niveau de la couche L2 pour déterminer si une liaison est correctement connectée et si le trafic circule de façon bidirectionnelle entre des voisins adéquats. Vous pouvez configurer le mode agressif d'UDLD dans la version 5.4(3) et ultérieure de CatOS pour des connexions point-à-point sur une base de port-par-port. Voici des exemples de sorties de commande :

> Remarque: L'activation d'UDLD sans activation du mode agressif se limite à vérifier que le branchement du câble à fibre est correct. Dans ce cas, UDLD contrôle où se croisent la réception et la transmission parmi les multiples connexions.

```
Switch_1> (enable) set udld enable
UDLD enabled globally

Console> (enable) set udld aggressive-mode enable 1/1-2
Aggressive UDLD enabled on ports 1/1-2.
Console> (enable) show udld
UDLD      : enabled
Message Interval : 15 seconds

Console> (enable) show udld port 1
UDLD : enabled
Message Interval : 15 seconds
Port Admin Status Aggressive Mode Link State
-------- ------------ --------------- ----------------
1/1 enabled enabled undetermined
1/2 enabled enabled undetermined
```

Dans CatOS 5.4.3 et antérieur, dans lesquels le commutateur ne prend pas en charge UDLD, ou si la liaison en question a un routeur sur une extrémité, vous pouvez activer le protocole CDP (Cisco Discovery Protocol). L'activation de CDP est une autre façon de détecter l'existence d'une liaison unidirectionnelle. Si seulement un côté d'une liaison peut voir son équipement voisin, remplacez le câble entre les périphériques et vérifiez les interfaces défectueuses.

```
Switch_1> (enable) show cdp
CDP               : enabled
Message Interval  : 60
Hold Time         : 180
Switch_1> (enable) show cdp neighbors
* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port     Device-ID                      Port-ID                   Platform
-------- ------------------------------ ------------------------- ------------
2/5     066560091(Switch_2)            2/9                       WS-C5505
2/6     066560091(Switch_2)            2/10                      WS-C5505
15/1     Router_1                      Vlan1                     cisco Cat5k-RSFC

Switch_2> (enable) show cdp
CDP               : enabled
Message Interval  : 60
Hold Time         : 180
Switch_2> (enable) show cdp neighbors
* - indicates vlan mismatch.
# - indicates duplex mismatch.
Port     Device-ID                      Port-ID                   Platform
-------- ------------------------------ ------------------------- ------------
2/9     066565061(Switch_1)            2/5                       WS-C5505
2/10    066565061(Switch_1)            2/6                       WS-C5505
15/1     Router_2                      Vlan1                     cisco Cat5k-RSFC
```

5. Références supplémentaires de dépannage de couche physique

Référez-vous à ces documents :

- Configuration et dépannage de la négociation automatique de transmission semi-duplex/duplex intégral simultanée Ethernet 10/100/1000 MB
- **Récupération d'un état de port errDisable sur les plates-formes CatOS**
- **Dépannage de problèmes de compatibilité des commutateurs Cisco Catalyst avec NIC**
- Section Compréhension des erreurs de liaison de données de Dépannage des problèmes de compatibilité entre les commutateurs Cisco Catalyst et les NIC
- **Résolution des problèmes de port et d'interface de commutateur**

D. Débogage de HSRP de la couche 3

Si les changements d'état du protocole HSRP sont fréquents, employez les commandes de débogage de HSRP dans le mode enable sur le routeur afin d'observer l'activité de HSRP. Ces informations vous aident à déterminer quel paquets HSRP sont reçus et envoyés par le routeur. Recueillez ces informations si vous créez une demande de service avec l'assistance technique Cisco. La sortie de débogage fournit également des informations sur l'état de HSRP, ainsi que des comptes détaillés des paquets Hello de HSRP.

1. Débogage standard de HSRP

Dans le logiciel Cisco IOS Version 12.1 et antérieure, la commande de débogage de HSRP est simplement **debug standby**. Ces informations sont utiles en cas de problèmes intermittents qui n'affectent que quelques interfaces. Le débogage vous permet de déterminer si le routeur HSRP en question reçoit et transmet les paquets Hello de HSRP à des intervalles spécifiques. Si le routeur ne reçoit pas les paquets Hello, vous pouvez en déduire que soit l'homologue ne transmet pas les paquets Hello, soit le réseau les supprime.

Commande	Objectif
debug standby	Active le débogage de HSRP

Voici un exemple de sortie de commande :

```
Router_1#debug standby

HSRP debugging is on

Router_1#
4d01h: SB1: Vlan1 Hello  out 10.1.1.1 Active  pri 100 ip 10.1.1.254
4d01h: SB1: Vlan1 Hello  in  10.1.1.2 Standby pri 100 ip 10.1.1.254
4d01h: SB2: Vlan2 Hello  in  10.2.1.2 Standby pri 100 ip 10.2.1.254
4d01h: SB2: Vlan2 Hello  out 10.2.1.1 Active  pri 100 ip 10.2.1.254
```

2. Débogage conditionnel de HSRP (limitant la sortie basée sur le groupe de veille et/ou le VLAN)

Le logiciel Cisco IOS Version 12.0(3) a introduit une condition de débogage pour permettre à la

sortie de commande debug standby d'être filtrée selon l'interface et le nombre de groupes. La commande utilise le paradigme de condition de débogage introduit dans le logiciel Cisco IOS Version 12.0.

Commande	Objectif
debug condition standby interface_group	Active le débogage conditionnel HSRP du groupe (0-255)

L'interface doit être une interface valide qui peut prendre en charge HSRP. Le groupe peut être tout groupe de 0 à 255. Une condition de débogage peut être définie pour des groupes qui n'existent pas. Ceci permet de capturer des débogages pendant l'initialisation d'un nouveau groupe. Le débogage de secours doit être activé afin de produire une sortie de débogage. Si la condition de débogage de secours n'existe pas, la sortie de débogage est produite pour tous les groupes sur toutes les interfaces. S'il existe au moins une condition de débogage de secours, la sortie de débogage de secours est filtrée en fonction de toutes les conditions de débogage de secours. Voici un exemple de sortie de commande :

```
Router_1#debug condition standby vlan 2 2
Condition 1 set
Router_1#
4d01h: Vl2 SB2 Debug: Condition 1, standby Vl2 SB2 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
4d01h: SB2: Vlan2 Hello  in  10.2.1.2 Standby pri 100 ip 10.2.1.254
4d01h: SB2: Vlan2 Hello  out 10.2.1.1 Active  pri 100 ip 10.2.1.254
4d01h: SB2: Vlan2 Hello  out 10.2.1.1 Active  pri 100 ip 10.2.1.254
4d01h: SB2: Vlan2 Hello  in  10.2.1.2 Standby pri 100 ip 10.2.1.254
```

3. Débogage amélioré de HSRP

Le logiciel Cisco IOS Version 12.1(1) a ajouté un débogage amélioré de HSRP. Afin de vous aider à trouver des informations utiles, le débogage amélioré de HSRP limite le bruit des messages Hello périodiques et inclut des informations d'état supplémentaires. Ces informations sont particulièrement utiles quand vous travaillez avec un ingénieur de l'assistance technique Cisco et créez une demande de service.

Commande	Objectif
debug standby	Affiche toutes les erreurs, tous les événements tous les paquets de HSRP
debug standby errors	Affiche les erreurs HSRP
debug standby events [[all] | [hsrp | Redondance | track]] [detail]	Affiche les évènements HSRP
debug standby packets [[all | laconique] | [annoncez | coup | bonjour | resign]] [detail]	Affiche les paquets HSRP

Voici un exemple de sortie de commande :

```
Router_2#debug standby terse
HSRP:
  HSRP Errors debugging is on
  HSRP Events debugging is on
  HSRP Packets debugging is on
  (Coup, Resign)
Router_2#
00:39:50: SB2: Vlan2 Standby: c/Active timer expired (10.2.1.1)
```

```
00:39:50: SB2: Vlan2 Standby -> Active
00:39:50: %STANDBY-6-STATECHANGE: Standby: 2: Vlan2 state Standby -> Active
00:40:30: SB2: Vlan2 Standby router is 10.2.1.1
00:41:12: SB2: Vlan2 Active: d/Standby timer expired (10.2.1.1)
00:42:09: SB2: Vlan2 Coup   in  10.2.1.1 Listen  pri 200 ip 10.2.1.254
00:42:09: SB2: Vlan2 Active: j/Coup rcvd from higher pri router
00:42:09: SB2: Vlan2 Active -> Speak
00:42:09: %STANDBY-6-STATECHANGE: Standby: 2: Vlan2 state Active -> Speak
00:42:09: SB2: Vlan2 Active router is 10.2.1.1
00:42:19: SB2: Vlan2 Speak: d/Standby timer expired (unknown)
00:42:19: SB2: Vlan2 Speak -> Standby
00:42:19: %STANDBY-6-STATECHANGE: Standby: 2: Vlan2 state Speak  -> Standby
```

Vous pouvez utiliser le débogage conditionnel de l'interface et/ou du groupe HSRP afin de filtrer cette sortie de débogage.

Commande	Objectif
debug condition interface interface	Active le débogage conditionnel de l'interface
debug condition standby interface_group	Active le débogage conditionnel d'HSRP

En cet exemple, le routeur rejoint un groupe HSRP préexistant :

```
Router_2#debug standby terse
HSRP:
  HSRP Errors debugging is on
  HSRP Events debugging is on
  HSRP Packets debugging is on
  (Coup, Resign)
Router_2#
00:39:50: SB2: Vlan2 Standby: c/Active timer expired (10.2.1.1)
00:39:50: SB2: Vlan2 Standby -> Active
00:39:50: %STANDBY-6-STATECHANGE: Standby: 2: Vlan2 state Standby -> Active
00:40:30: SB2: Vlan2 Standby router is 10.2.1.1
00:41:12: SB2: Vlan2 Active: d/Standby timer expired (10.2.1.1)
00:42:09: SB2: Vlan2 Coup   in  10.2.1.1 Listen  pri 200 ip 10.2.1.254
00:42:09: SB2: Vlan2 Active: j/Coup rcvd from higher pri router
00:42:09: SB2: Vlan2 Active -> Speak
00:42:09: %STANDBY-6-STATECHANGE: Standby: 2: Vlan2 state Active -> Speak
00:42:09: SB2: Vlan2 Active router is 10.2.1.1
00:42:19: SB2: Vlan2 Speak: d/Standby timer expired (unknown)
00:42:19: SB2: Vlan2 Speak -> Standby
00:42:19: %STANDBY-6-STATECHANGE: Standby: 2: Vlan2 state Speak  -> Standby
```

E. Dépannage du spanning tree

Des boucles STP ou une instabilité dans le réseau peuvent empêcher la bonne communication des homologues de HSRP. En raison de cette transmission inadéquate, chaque homologue devient un routeur actif. Les boucles STP peuvent entraîner des tempêtes de diffusion, des doublons de trames et une incohérence dans la table MAC. Tous ces problèmes affectent l'ensemble du réseau et particulièrement le protocole HSRP. Les messages d'erreur HSRP peuvent être la première indication d'un problème de STP.

Quand vous dépannez STP, vous *devez* comprendre la topologie STP du réseau sur chaque VLAN. Vous devez déterminer quel commutateur est le pont racine et quels ports sur le commutateur sont sur blocage et transmission. Puisque chaque VLAN a sa propre topologie STP, ces informations sont très importantes pour chaque VLAN.

1. Vérifiez la configuration de spanning tree

Soyez sûr que STP est configuré sur chaque commutateur et périphérique de pontage dans le réseau. Notez l'emplacement du pont racine supposé par chaque commutateur. En outre, notez les valeurs de ces temporisateurs :

- Root Max Age
- Délai Hello
- Délai de transmission

Émettez la commande show spantree pour afficher toutes ces informations. Par défaut, la commande indique ces informations pour le VLAN 1. Mais, vous pouvez également voir les autres informations si vous fournissez le numéro du VLAN avec la commande. Ces informations sont très utiles quand vous dépannez les problèmes de STP.

Ces trois temporisateurs que vous notez dans la sortie show spantree sont appris du pont racine. Ils n'ont pas besoin de correspondre aux temporisateurs définis sur ce pont spécifique. Mais, assurez-vous que les temporisateurs correspondent au pont racine dans le cas où ce commutateur deviendrait le pont racine à un moment quelconque. Cette correspondance des temporisateurs avec le pont racine permet d'assurer la continuité et la facilité de la gestion. Elle empêche également un commutateur avec des temporisateurs incorrects de paralyser le réseau.

> Remarque: Activez STP pour tous les VLAN à tout moment, que ce soit des liaisons redondantes dans le réseau ou pas. Si vous activez STP dans les réseaux non redondants, vous empêchez une rupture. Une rupture peut se produire si quelqu'un fait un pont entre des commutateurs avec des concentrateurs ou d'autres commutateurs et crée accidentellement une boucle physique. STP est également très utile dans l'isolement de problèmes spécifiques. Si l'activation de STP affecte le fonctionnement de quelque chose dans le réseau, il peut y avoir un problème existant que vous devez isoler.

Voici un exemple de sortie de la commande show spantree :

```
Switch_1> (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-01-64-34-90-00
Designated Root Priority    98
Designated Root Cost        0
Designated Root Port        1/0
Root Max Age   20 sec       Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-01-64-34-90-00
Bridge ID Priority          98
Bridge Max Age 20 sec       Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------- ----- -------- ---------- ----------
1/1                       1    not-connected     4       32 disabled   0
1/2                       1    not-connected     4       32 disabled   0
2/1                       1    forwarding      100       32 disabled   0
2/2                       1    not-connected   100       32 disabled   0
2/3                       1    not-connected   100       32 disabled   0
2/4                       1    not-connected   100       32 disabled   0
2/5-6                     1    forwarding       12       32 disabled   803
2/10                      1    not-connected   100       32 disabled   0
2/11                      1    not-connected   100       32 disabled   0
2/12                      1    not-connected   100       32 disabled   0
```

```
15/1                     1    forwarding        5       32 disabled   0

Switch_1> (enable) show spantree 2
VLAN 2
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-30-96-73-74-01
Designated Root Priority    8192
Designated Root Cost        12
Designated Root Port        2/5-6 (agPort 13/35)
Root Max Age   20 sec       Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-01-64-34-90-01
Bridge ID Priority          16384
Bridge Max Age 20 sec       Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------ ----- -------- ---------- ----------
2/5-6                     2    forwarding       12       32 disabled   803
2/7                       2    not-connected   100       32 disabled   0
2/8                       2    not-connected   100       32 disabled   0
2/9                       2    not-connected   100       32 disabled   0
15/1                      2    forwarding        5       32 disabled   0
```

Le commutateur 1 est la racine du VLAN 1 et croit que qui est Comm2 la racine de VLAN 2. concourt Comm2.

```
Switch_2> (enable) show spantree
VLAN 1
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-01-64-34-90-00
Designated Root Priority    98
Designated Root Cost        12
Designated Root Port        2/9-10 (agPort 13/37)
Root Max Age   20 sec       Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-30-96-73-74-00
Bridge ID Priority          16384
Bridge Max Age 20 sec       Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------ ----- -------- ---------- ----------
1/1                       1    not-connected     4       32 disabled   0
1/2                       1    not-connected     4       32 disabled   0
2/6                       1    not-connected   100       32 disabled   0
2/7                       1    not-connected   100       32 disabled   0
2/8                       1    not-connected   100       32 disabled   0
2/9-10                    1    forwarding       12       32 disabled   805
2/11                      1    not-connected   100       32 disabled   0
2/12                      1    not-connected   100       32 disabled   0
15/1                      1    forwarding        5       32 disabled   0

Switch_2> (enable) show spantree 2
VLAN 2
Spanning tree enabled
Spanning tree type          ieee

Designated Root             00-30-96-73-74-01
Designated Root Priority    8192
Designated Root Cost        0
```

```
Designated Root Port        1/0
Root Max Age   20 sec       Hello Time 2  sec   Forward Delay 15 sec

Bridge ID MAC ADDR          00-30-96-73-74-01
Bridge ID Priority          8192
Bridge Max Age 20 sec       Hello Time 2  sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------ ----- -------- ---------- ----------
2/1                       2    not-connected   100       32 disabled   0
2/2                       2    not-connected   100       32 disabled   0
2/3                       2    not-connected   100       32 disabled   0
2/4                       2    not-connected   100       32 disabled   0
2/5                       2    not-connected   100       32 disabled   0
2/9-10                    2    forwarding       12       32 disabled   805
15/1                      2    forwarding        5       32 disabled   0
```

2. États de boucle de spanning tree

Pour qu'une boucle STP survienne, il doit y avoir une redondance physique au niveau de la couche L2 dans le réseau. Un STP ne se produit pas s'il n'y a aucune possibilité d'une condition de boucle physique. Les symptômes d'une condition de boucle STP sont :

- Une panne totale de réseau
- Une perte de connectivité
- Le signalement par l'équipement réseau d'une utilisation élevée du processus et du système

La commande show system vous aide à déterminer l'utilisation du système d'un commutateur particulier. La commande show system dénote les éléments suivants :

- Pourcentage de trafic en cours
- Pourcentage de trafic maximal
- Date et heure du dernier pic

Une utilisation du système au-dessus de 20 pour cent indique habituellement une boucle. Une utilisation au-dessus de sept pour cent indique une possible boucle. Mais, ces pourcentages sont seulement des approximations. Les approximations varient quelque peu selon le matériel, tel que Supervisor Engine I par rapport à Supervisor Engine IIIG ou Catalyst 4000 par rapport à Catalyst 6000.

Voici un exemple de sortie de la commande show system :

```
Switch_1> (enable) show system
PS1-Status PS2-Status Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
---------- ---------- ---------- ---------- ---------- -------------- ---------
ok         none       ok         off        ok         5,00:58:16     20 min
PS1-Type     PS2-Type     Modem   Baud  Traffic Peak Peak-Time
------------ ------------ ------- ----- ------- ---- -------------------------
WS-C5008B    none         disable  9600   0%     70% Tue Jan 9 2001, 16:50:52
System Name              System Location          System Contact
------------------------ ------------------------ ------------------------
Switch_1
```

Cette sortie montre les éléments suivants :

- Le pourcentage de trafic en cours, 0%
- Le pourcentage de trafic maximal, 70%
- La date et l'heure du dernier pic

Une utilisation du système à 70 pour cent indique une possible boucle au moment de la sortie de la commande **show system**.

Un seul VLAN avec une condition de boucle STP peut congestionner une liaison et priver les autres VLAN de bande passante. La commande **show mac** indique les ports qui transmettent ou reçoivent un nombre excessif de paquets. Une diffusion et une multidiffusion excessives peuvent indiquer des ports qui font partie d'une boucle STP. Cet exemple de sortie de la commande **show mac** indique un nombre élevé de paquets de multidiffusion et de diffusion sur le port 2/11. Étudiez ce port. En règle générale, suspectez une liaison d'une condition de boucle STP chaque fois que la multidiffusion ou la diffusion dépasse le nombre de paquets de monodiffusion.

> Remarque: Le commutateur compte également les unités de données des protocoles BDPU qui sont reçues et transmises comme des trames de multidiffusion. Un port qui est toujours dans l'état de blocage STP continue de transmettre et de recevoir des unités de données des protocoles BDPU.

```
Switch_1> (enable) show mac
Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                        0                    0                    0
 1/2                        0                    0                    0
 2/1                   551277               296902              1025640
 2/2                        0                    0                    0
 2/3                        0                    0                    0
 2/4                        0                    0                    0
 2/5                        0                69541                    0
 2/6                        0                44026                    0
 2/7                        0                    0                    0
 2/8                        0                    0                    0
 2/9                        0                    0                    0
 2/10                       0                    0                    0
 2/11                   12836              5911986              1126018
 2/12                 6993144            177795414             19063645

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                        0                    0                    0
 1/2                        0                    0                    0
 2/1                   326122              1151895               431125
 2/2                        0                    0                    0
 2/3                        0                    0                    0
 2/4                        0                    0                    0
 2/5                        0               157414                    0
 2/6                       10               652821                    1
 2/7                        0                    0                    0
 2/8                        0                    0                    0
 2/9                        0                    0                    0
 2/10                       0                    0                    0
 2/11                20969162            127255514             56002139
 2/12                   13598              7378244                 3166

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
1/1                        0                    0
1/2                        0                    0
2/1                544904490            295721712
2/2                        0                    0
2/3                        0                    0
```

```
2/4                    0                  0
2/5              6997319           15860816
2/6              4787570          185054891
2/7                    0                  0
2/8                    0                  0
2/9                    0                  0
2/10                   0                  0
2/11           560753237         8058589649
2/12          6822964273          815810803

MAC      Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
1/1               0          0          0          0          0          0
1/2               0          0          0          0          0          0
2/1               0          0     718920          0          0          0
2/2               0          0          0          0          0          0
2/3               0          0          0          0          0          0
2/4               0          0          0          0          0          0
2/5               0          -          3          0          1          0
2/6               0          -          0          0          0          0
2/7               0          0          0          0          0          0
2/8               0          0          0          0          0          0
2/9               0          0          0          0          0          0
2/10              0          0          0          0          0          0
2/11              0          0         67          0          0          0
2/12              0          0        869          0          3          0
```

Émettez la commande session afin de voir les compteurs ATM et de routeurs.

```
Switch_1> (enable) show mac
Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                     0                    0                    0
 1/2                     0                    0                    0
 2/1                551277               296902              1025640
 2/2                     0                    0                    0
 2/3                     0                    0                    0
 2/4                     0                    0                    0
 2/5                     0                69541                    0
 2/6                     0                44026                    0
 2/7                     0                    0                    0
 2/8                     0                    0                    0
 2/9                     0                    0                    0
 2/10                    0                    0                    0
 2/11                12836              5911986              1126018
 2/12              6993144            177795414             19063645

Port     Xmit-Unicast         Xmit-Multicast       Xmit-Broadcast
-------- -------------------- -------------------- --------------------
 1/1                     0                    0                    0
 1/2                     0                    0                    0
 2/1                326122              1151895               431125
 2/2                     0                    0                    0
 2/3                     0                    0                    0
 2/4                     0                    0                    0
 2/5                     0               157414                    0
 2/6                    10               652821                    1
 2/7                     0                    0                    0
 2/8                     0                    0                    0
 2/9                     0                    0                    0
 2/10                    0                    0                    0
```

```
 2/11                20969162            127255514             56002139
 2/12                   13598              7378244                 3166

Port     Rcv-Octet            Xmit-Octet
-------- -------------------- --------------------
1/1                         0                    0
1/2                         0                    0
2/1                 544904490            295721712
2/2                         0                    0
2/3                         0                    0
2/4                         0                    0
2/5                   6997319             15860816
2/6                   4787570            185054891
2/7                         0                    0
2/8                         0                    0
2/9                         0                    0
2/10                        0                    0
2/11                560753237           8058589649
2/12               6822964273            815810803

MAC      Dely-Exced MTU-Exced  In-Discard Lrn-Discrd In-Lost    Out-Lost
-------- ---------- ---------- ---------- ---------- ---------- ----------
1/1               0          0          0          0          0          0
1/2               0          0          0          0          0          0
2/1               0          0     718920          0          0          0
2/2               0          0          0          0          0          0
2/3               0          0          0          0          0          0
2/4               0          0          0          0          0          0
2/5               0          -          3          0          1          0
2/6               0          -          0          0          0          0
2/7               0          0          0          0          0          0
2/8               0          0          0          0          0          0
2/9               0          0          0          0          0          0
2/10              0          0          0          0          0          0
2/11              0          0         67          0          0          0
2/12              0          0        869          0          3          0
```

3. Avis de changement de topologie

Une autre commande qui est essentielle au diagnostic des problèmes de STP est la commande **show spantree statistics**. Cette commandes suit les messages d'avis de modification de la topologie (TCN) renvoyés au créateur. Ces messages, envoyés en tant qu'unités BPDU spéciales entre les commutateurs, indiquent qu'il y a eu une modification de topologie sur un commutateur. Ce commutateur envoie un TCN de son port racine. Le TCN se déplace en amont vers le pont racine. Le pont racine envoie alors une autre BPDU spéciale, un accusé de réception de modification de topologie (TCA), de tous ses ports. Le pont racine définit le bit TCN dans la configuration BPDU. Ceci a pour conséquence que tous les ponts non racine définissent leur durée de vieillissement de la table d'adresses MAC sur le retard de retransmission du protocole STP de la configuration.

Afin d'isoler ce problème, accédez au pont racine pour chaque VLAN et émettez la commande **show spantree statistics** pour les ports connectés au commutateur. L'entrée last topology change occurred donne l'heure à laquelle le dernier avis TCN a été reçu. Dans cette situation, vous êtes trop en retard pour voir qui a émis les TCN qui ont pu provoquer la possible boucle STP. L'entrée de topology change count vous donne une idée du nombre de TCN qui se produisent. Pendant une boucle STP, ce compteur peut incrémenter chaque minute. Référez-vous à Problèmes de protocole STP et considérations de conception associées pour plus d'informations. Ce document contient plus d'informations sur la façon d'interpréter la commande **show spantree statistics**.

Autres informations utiles :

- Port du dernier TCN
- Heure du dernier TCN
- Nombre actuel de TCN

Voici un exemple de sortie de commande :

```
Switch_1> (enable) show spantree statistics 2/5 1
Port  2/5   VLAN 1
SpanningTree enabled for vlanNo = 1
                BPDU-related parameters
port spanning tree                   enabled
state                                forwarding
port_id                              0x8323
port number                          0x323
path cost                            12
message age (port/VLAN)              20(20)
designated_root                      00-01-64-34-90-00
designated_cost                      0
designated_bridge                    00-01-64-34-90-00
designated_port                      0x8323
top_change_ack                       FALSE
config_pending                       FALSE
port_inconsistency                   none
                PORT based information & statistics
config bpdu's xmitted (port/VLAN)    29660(357027)
config bpdu's received (port/VLAN)   2(215721)
tcn bpdu's xmitted (port/VLAN)       0(521)
tcn bpdu's received (port/VLAN)      2(203)
forward trans count                  1
scp failure count                    0
                Status of Port Timers
forward delay timer                  INACTIVE
forward delay timer value            15
message age timer                    INACTIVE
message age timer value              0
topology change timer                INACTIVE
topology change timer value          35
hold timer                           INACTIVE
hold timer value                     1
delay root port timer                INACTIVE
delay root port timer value          0
                VLAN based information & statistics
spanningtree type                    ieee
spanningtree multicast address       01-80-c2-00-00-00
bridge priority                      98
bridge mac address                   00-01-64-34-90-00
bridge hello time                    2 sec
bridge forward delay                 15(15) sec
topology change initiator:           2/2
last topology change occurred:        Wed Jan 10 2001, 18:16:02
topology change                      FALSE
topology change time                 35
topology change detected             FALSE
topology change count                80
topology change last recvd. from     00-10-7b-08-fb-94
                  Other port-specific info
dynamic max age transitions          0
port bpdu ok count                   0
msg age expiry count                 0
```

```
link loading                        1
bpdu in processing                  FALSE
num of similar bpdus to process     1
received_inferior_bpdu              FALSE
next state                          3
src mac count:                      0
total src mac count                 0
curr_src_mac                        00-00-00-00-00-00
next_src_mac                        00-00-00-00-00-00
channel_src_mac                     00-10-7b-08-e1-74
channel src count                   0
channel ok count                    0
```

Cette sortie montre que la dernière modification de topologie s'est produite à partir du périphérique 00-10-7b-08-fb-94 du port 2/2. Ensuite, émettez la même commande **show spantree statistics** du périphérique 00-10-7b-08-fb-94. Voici un extrait de la sortie **show spantree statistics** du périphérique contigu :

```
VLAN based information & statistics
spanningtree type                   ieee
spanningtree multicast address      01-80-c2-00-00-00
bridge priority                     98
bridge mac address                  00-10-7b-08-fb-94
bridge hello time                   2 sec
bridge forward delay                15(15) sec
topology change initiator:          5/2
last topology change occurred:       Wed Jan 10 2001, 18:16:02
topology change                     FALSE
topology change time                35
topology change detected            FALSE
topology change count               80
topology change last recvd. from    00-00-00-00-00-00
```

La sortie indique l'adresse MAC avec tous les zéros, ce qui signifie que ce commutateur est l'initiateur de la modification de topologie. Le port 5/2 est le port par lequel a transité les états, sans doute parce que le port passe de up à down. Si ce port est relié à un PC ou à un simple hôte, vérifiez que STP PortFast est activé sur ce port. STP PortFast supprime les TCN de STP quand un port transite entre des états.

Référez-vous à ces documents pour plus d'informations sur STP et sur la façon de dépanner les transitions de liaison associées aux cartes réseau (NIC) :

- Dépannage de problèmes de compatibilité des commutateurs Cisco Catalyst avec NIC
- >Utilisation de PortFast et d'autres commandes pour remédier aux délais de connectivité lors du démarrage de la station de travail
- Configuration et dépannage de la négociation automatique de transmission semi-duplex/duplex intégral simultanée Ethernet 10/100/1000 MB
- Présentation des changements de topologie SPT (Spanning-Tree Protocol)
- Problèmes liés au protocole STP (Spanning Tree Protocol) et considérations de conception

4. Ports bloqués déconnectés

En raison de la nature d'équilibrage de charge de Fast EtherChannel (FEC) (canaux de port), les problèmes de FEC peuvent contribuer à des problèmes de HSRP et STP. Quand vous dépannez STP ou HSRP, supprimez la configuration pour toute connexion FEC. Une fois les modifications de configuration en place, émettez la commande **show spantree blockedports** sur les deux

commutateurs. Assurez-vous qu'au moins un des ports commence à bloquer l'un ou l'autre des côtés de la connexion. Voici un exemple de sortie de commande :

```
Switch_1> (enable) show spantree blockedports
T = trunk
g = group
Ports       Vlans
-----       ----------
 2/6  (T)   2
Number of blocked ports (segments) in the system : 1

Switch_2> (enable) show spantree blockedports
T = trunk
g = group
Ports       Vlans
-----       ----------
2/10 (T)   1
Number of blocked ports (segments) in the system : 1
```

Référez-vous à ces documents pour des informations sur Fast EtherChannel :

- Présentation de l'équilibrage de charge et de la redondance EtherChannel sur les commutateurs Catalyst
- Configuration d'EtherChannel entre des commutateurs Catalyst 4500/4000, 5500/5000 et des commutateurs 6500/6000 qui exécutent le logiciel système CatOS

5. Suppression de diffusion

Activez la suppression de diffusion afin de réduire l'incidence d'une tempête de diffusion. Une tempête de diffusion est l'un des principaux effets secondaires d'une boucle STP. Voici un exemple de sortie de commande :

```
Switch_1> (enable) set port broadcast 2/5 ?
                   Packets per second
                Percentage
Switch_1> (enable) set port broadcast 2/5 10%
Port(s) 2/1-12 broadcast traffic limited to 10%.
Switch_1> (enable) show port broadcast 2/5
Port     Broadcast-Limit Broadcast-Drop
-------- --------------- --------------
 2/5                10 %              -
```

6. Console et telnet Access

Le trafic Console ou Telnet au commutateur devient souvent trop lent pour détecter correctement un équipement attentatoire pendant une boucle STP. Afin de forcer le réseau à récupérer immédiatement, supprimer toutes les liaisons physiques redondantes. Après que STP est autorisé à reconverger sur la nouvelle topologie non redondant, rattachez une liaison redondante à la fois. Si la boucle STP retourne après que vous ajoutez un segment particulier, vous avez identifié les périphériques attentatoires.

7. Caractéristiques de spanning-tree : Portfast, Uplinkfast et BackboneFast

Vérifiez que PortFast, UplinkFast et BackboneFast sont configurés correctement. Quand vous dépannez les problèmes de STP, désactivez tout Advanced STP (Uplinkfast et BackboneFast). En

outre, vérifiez que STP PortFast est seulement activé sur les ports qui sont directement connectés aux hôtes de non-pontage. Parmi les hôtes de non-pontage figurent des postes de travail utilisateur et des routeurs sans groupes de pontage. N'activez pas PortFast sur les ports qui sont connectés aux concentrateurs ou à d'autres commutateurs. Voici un exemple de sortie de commande :

```
Switch_2> (enable) show port spantree
Port(s)                  Vlan Port-State    Cost  Priority Portfast   Channel_id
------------------------ ---- ------------ ----- -------- ---------- ----------
1/1                      1    not-connected     4       32 disabled   0
1/2                      1    not-connected     4       32 disabled   0
2/1                      2    not-connected   100       32 disabled   0
2/2                      2    not-connected   100       32 disabled   0
2/3                      2    not-connected   100       32 disabled   0
2/4                      2    not-connected   100       32 disabled   0
2/5                      2    not-connected   100       32 disabled   0
2/6                      1    forwarding       19       32 disabled   0
2/7                      1    not-connected   100       32 disabled   0
2/8                      1    not-connected   100       32 disabled   0
2/9                      1    blocking         19       32 disabled   0
2/9                      2    forwarding       19       32 disabled   0
2/9                      3    forwarding       19       32 disabled   0
2/9                      1003 not-connected    19       32 disabled   0
2/9                      1005 not-connected    19        4 disabled   0
2/10                     1    blocking         19       32 disabled   0
2/10                     2    forwarding       19       32 disabled   0
2/10                     3    blocking         19       32 disabled   0
2/10                     1003 not-connected    19       32 disabled   0
2/10                     1005 not-connected    19        4 disabled   0
2/11                     2    forwarding      100       32 enabled    0
2/12                     1    not-connected   100       32 disabled   0
15/1                     1    forwarding        5       32 disabled   0
15/1                     2    forwarding        5       32 disabled   0
```

Activez seulement UplinkFast sur des commutateurs de nœuds terminaux. Les commutateurs de nœuds terminaux sont des commutateurs en armoire auxquels les utilisateurs se connectent directement. UplinkFast est une optimisation STP qui est destinée seulement aux ports de liaison ascendante à la distribution ou à la couche centrale du réseau. Voici un exemple de sortie de commande :

```
Switch_1> (enable) set spantree uplinkfast enable
VLANs 1-1005 bridge priority set to 49152.
The port cost and portvlancost of all ports set to above 3000.
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.
uplinkfast enabled for bridge.

Switch_1> (enable) show spantree uplinkfast
Station update rate set to 15 packets/100ms.
uplinkfast all-protocols field set to off.

VLAN          port list
-----------------------------------------
1             2/2(fwd) ,2/5-6
2             2/5(fwd) ,2/6
```

Configurez BackboneFast sur tous les Commutateurs dans le réseau. BackboneFast est une optimisation de STP, qui modifie le temporisateur Max Age à la réception d'une BPDU inférieure envoyée par le pont désigné. Voici un exemple de sortie de commande :

```
Switch_1> (enable) set spantree backbonefast enable
Backbonefast enabled for all VLANs
Switch_1> (enable) show spantree backbonefast
Backbonefast is enabled.
```

8. BPDU guard

Quand vous activez PortFast BPDU Guard, un port sans agrégation avec PortFast activé est placé dans l'état errdisable à la réception d'une BPDU sur ce port. Cette fonctionnalité vous aide à trouver les ports qui ne sont pas configurés correctement pour PortFast. La fonctionnalité détecte également l'emplacement où des périphériques peuvent se refléter ou intercepter des BPDU de STP dans le réseau. Quand vous dépannez les problèmes de STP, activez cette fonctionnalité sur tous les ports. Voici exemple pour CatOS :

```
Switch_1>(enable) set spantree portfast bpdu-quard enable
Spantree PortFast bpdu-guard enabled on this switch.
```

9. Élagage VTP

Quand l'Élagage de VTP est activé dans le réseau, cela peut provoquer l'activation des périphériques d'un groupe HSRP. Ceci a comme conséquence des conflits d'IP parmi les passerelles et des problèmes de trafic. Assurez-vous que le VLAN d'un groupe HSRP n'est pas élagué par VTP dans le réseau.

F. CGMP Leave traitant et Interopérabilité de HSRP

HSRP communique à l'adresse MAC de destination de 01-00-5e-00-00-02, qui est identique à celle utilisée par le traitement fast-leave du protocole IGMP. Le traitement fast-leave d'IGMP est une fonctionnalité de la version 2 d'IGMP. Avec le traitement CGMP Leave activé sur les commutateurs Cisco, tout le trafic de multidiffusion avec l'adresse MAC de destination de 01-00-5e-00-00-02 est expédié au CPU du commutateur. Si le paquet n'est pas un message d'IGMP, le CPU du commutateur régénère le paquet et l'envoie à tous les ports du routeur. Puisque HSRP utilise la même adresse multicast de destination, tous les paquets HSRP doivent d'abord être envoyés au CPU du commutateur, qui les régénère et les envoie ensuite à tous les ports du routeur. Par conséquent, quand vous dépannez des problèmes de HSRP, désactivez le traitement CGMP Leave entre les homologues de HSRP.

> Remarque: L'utilisation d'IGMP Snooping sur Catalyst les 6500 et 5500 avec NetFlow Feature Card (NFFC) II ne pose pas ce problème.

Afin de déterminer si le traitement CGMP Leave est activé sur des commutateurs CatOS, émettez la commande show cgmp leave. Voici un exemple :

```
Switch> (enable) show cgmp leave
CGMP: disabled
CGMP leave: disabled
For Catalyst 2900XL/3500XL switches, issue the show cgmp state command:
```

```
s-2924xl-27a#show cgmp state
CGMP is running.
CGMP Fast Leave is not running.
Default router timeout is 300 sec.
```

G. Divisez et conquérez

Si toutes les autres tentatives d'isoler ou de résoudre HSRP échouent, la méthode « diviser pour mieux régner » est l'approche suivante. Elle aide à isoler le réseau et les composants qui constituent le réseau. « Diviser pour mieux régner » implique l'une ou l'autre des directives de cette liste :

Remarque: Cette liste reprend quelques directives d'autres sections de ce document.

- Créez un VLAN test pour le HSRP et un VLAN isolé au commutateur avec les routeurs de HSRP.
- Déconnectez tous les ports redondants.
- Divisez les ports FEC en ports connectés simples.
- Réduisez les membres du groupe HSRP à seulement deux.
- Élaguez les ports de liaison de sorte que seuls les VLAN nécessaires se propagent à travers ces ports.
- Déconnectez les commutateurs connectés dans le réseau jusqu'à ce que les problèmes cessent.

H. CPU de haute avec le trafic asymétrique dans le HSRP

L'utilisation du CPU pourrait devenir élevée puisque le trafic circule d'une interface POS à une interface Gigabit Ethernet dans un environnement asymétrique de HSRP. Les paquets deviennent fragmentés car la taille du MTU de POS est de 4470 octets et la taille du MTU Gigabit de 1.500 octets. La fragmentation consomme plus de CPU.

Afin de résoudre ce problème, exécutez l'une de ces commandes :

```
!--- On the gigabit interface mtu 4770
```

ou

```
!--- On the POS interface ip tcp adjust-mss 1460
```

Problèmes identifiés

Nombre de groupes HSRP pris en charge pour Catalyst 6500/6000 de la gamme PFC2/MSFC2 et Catalyst 3550

La carte de fonctionnalités de politique (PFC) 2 (PFC2)/MSFC2 pour la gamme Catalyst 6500/6000 prend en charge un maximum de 16 groupes HSRP uniques. Si vous avez besoin de plus de 16 groupes HSRP, vous pouvez réutiliser les mêmes numéros de groupe HSRP dans différents VLAN. Pour plus d'informations sur les limitations de groupes HSRP pour la gamme

Catalyst 6500/6000, référez-vous à Questions fréquemment posées sur les limitations de groupes HSRP sur les commutateurs de la gamme Catalyst 6500/6000.

Une limitation semblable existe pour la gamme Catalyst 3550, qui prend en charge un maximum de 16 groupes HSRP. C'est une limitation matérielle et il n'y a aucun contournement.

Oscillation/instabilité de l'état de HSRP quand vous utilisez Cisco 2620/2621, Cisco 3600 avec Fast Ethernet ou PA-2FEISL

Ce problème peut se poser avec des interfaces Fast Ethernet à l'interruption de la connectivité réseau ou à l'ajout d'un routeur HSRP avec un réseau de priorité supérieure. Quand l'état du protocole HSRP passe de Active à Speak, le routeur réinitialise l'interface pour supprimer l'adresse MAC de HSRP du filtre de l'adresse MAC de l'interface. Seul le matériel spécifique qui est utilisé sur les interfaces Fast Ethernet pour les commutateurs Cisco 2600, 3600 et 7500 ont ce problème. La réinitialisation de l'interface du routeur entraîne une modification d'état de la liaison sur des interfaces Fast Ethernet et le routeur détecte la modification. Si le commutateur exécute STP, la modification entraîne une transition STP. STP prend 30 secondes pour faire passer le port à l'état forwarding. C'est deux fois plus que le temps de retard de retransmission par défaut, qui est de 15 secondes. En même temps, le routeur à l'état Speak passe à l'état standby après 10 secondes, ce qui est le temps de maintien de HSRP. STP n'expédie pas encore, donc aucun message Hello de HSRP n'est reçu du routeur actif. Ceci a pour conséquence que le routeur de secours devient actif après environ 10 secondes. Les deux routeurs sont maintenant dans l'état active. Quand les ports STP passent à l'état de transmission, le routeur de faible priorité passe de l'état active à speak et tout le processus se répète.

Plateforme	Description	ID de débogage Cisco	Difficulté	Solution de contournement
Cisco 2620/2621	L'interface Fast Ethernet commence à s'affoler quand le protocole HSRP est configuré et que le câble est débranché.		Mise à niveau logicielle ; référez-vous au bogue pour des détails sur la révision.	Active Spannin Tree Portfast s port de commu connecté.
Cisco 2620/2621	L'état de HSRP s'affole sur 2600 avec Fast Ethernet.		Logiciel Cisco IOS® Version 12.1.3	Active Spannin Tree Portfast s port de commu connecté.
Cisco 3600 avec NM-1FE-TX[1]	L'état de HSRP s'affole sur 2600 et 3600 Fast Ethernet.		Logiciel Cisco IOS® Version 12.1.3	Active Spannin Tree Portfast s port de commu connecté.
Cisco 4500 avec l'interface Fast Ethernet	L'état de HSRP s'affole sur 4500 Fast Ethernet.	CSCds16055 (clients enregistrés seulement)	Logiciel Cisco IOS® Version 12.1.5	Active Spannin Tree Portfast s port de commu connecté.
Cisco 7200/7500 avec du PA-2FEISL[2]	L'état de HSRP s'affole sur PA-2FEISL.		Logiciel Cisco IOS® Version 12.1.5	Active Spannin Tree Portfast s port de commu connecté.

[1]NM-1FE-TX = module réseau de Fast Ethernet de port unique (interface 10/100BASE-TX).

[1] PA-2FEISL = adaptateur à deux orifices de port de l'InterSwitch Link de Fast Ethernet [ISL].

Un contournement alternatif consiste à ajuster les temporisateurs HSRP de sorte que le délai de retard de retransmission STP est inférieur à la moitié du temps d'attente de HSRP par défaut. Le délai de retard de retransmission de STP par défaut est de 15 secondes et le temps d'attente de HSRP par défaut est de 10 secondes.

Quand vous utilisez la commande **track** sous le processus HSRP, Cisco recommande d'employer une valeur particulière de décrément afin d'éviter l'affolement de HSRP.

Voici un exemple de configuration dans un routeur actif de HSRP quand vous utilisez la commande **track** :

```
standby 1 ip 10.0.0.1
 standby 1 priority 105
 standby 1 preempt delay minimum 60
 standby 1 name TEST
 standby 1 track Multilink100 15
```

Où 15 est la valeur de décrément quand le multilink100 s'affole.

HSRP bloqué dans l'état Initial ou Active sur Cisco 2620/2621, Cisco 3600 avec Fast Ethernet ou PA-2FEISL

Les interfaces Fast Ethernet sur les routeurs Cisco 2600, 3600 et 7200 peuvent connaître ces problèmes quand le protocole HSRP est configuré :

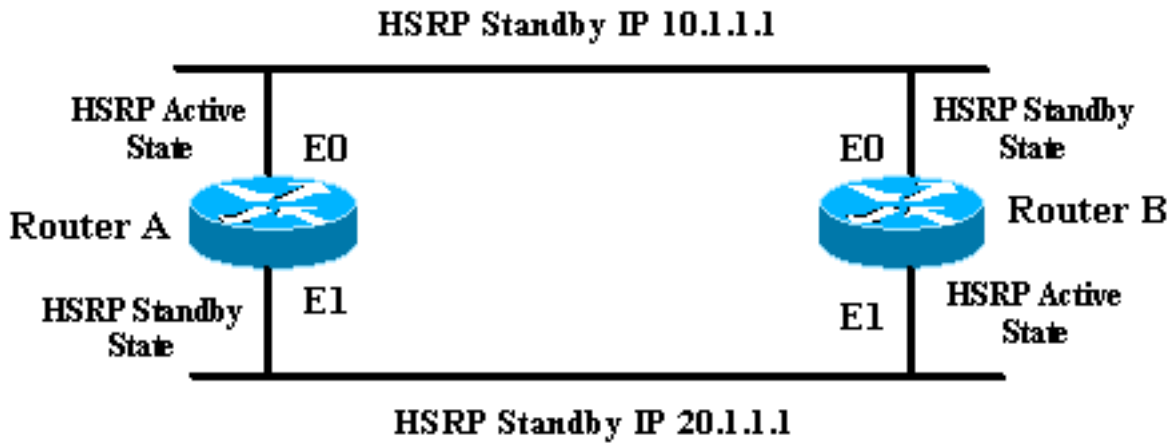
- HSRP reste dans l'état active quand l'interface passe à down ou est débranchée.
- HSRP reste dans l'état initial statequand l'interface passe à up.
- Le suivi des interfaces ne fonctionne pas.

Un problème de détection de la temporisation de l'interface up/down entraîne ces problèmes de HSRP. Le problème de temporisation est qu'il existe un retard entre l'occurrence de l'événement de l'interface et la mise à niveau de l'état de l'interface du routeur.

Plateforme	Description	ID de débogage Cisco	Difficulté	Solution de contournement
Cisco 2620/2621	HSRP est bloqué à l'état initial.	CSCdp24680 (clients enregistrés seulement)	Mise à niveau logicielle ; référez-vous au bogue pour des détails sur la révision.	Émettez les commandes shutdown and no shutdown afin de réinitialiser l'interface.
Cisco 3600 avec NM-1FE-TX	HSRP est bloqué à l'état initial sur le module NM-1FE-TX en 3600.	CSCdp24680 (clients enregistrés seulement)	Mise à niveau logicielle ; référez-vous au bogue pour des détails sur la révision.	Émettez les commandes shutdown and no shutdown afin de réinitialiser l'interface.
Cisco 7200/7500 avec PA-	HSRP est bloqué à l'état initial sur le module PA-2FEISL dans 7200/7500.	CSCdr01156 (clients enregistrés	Mise à niveau logicielle ; référez-vous au bogue pour des détails sur la	Émettez les commandes shutdown and no

2FEISL	seulement)	révision.	shutdown afin de réinitialiser l'interface.

Incapable d'envoyer des pings à l'adresse HSRP standby sur les routeurs de la gamme Cisco 2500 et 4500



Dans ce diagramme, le routeur A représente un routeur de la gamme Cisco 2500 et le routeur B représente un routeur de la gamme Cisco 4500. Si le routeur A envoie un ping à l'adresse IP virtuelle sur le LAN 1, 10.1.1.1, le routeur envoie d'abord une requête ARP. Le routeur B répond avec une réponse ARP qui contient l'adresse MAC virtuelle. Le routeur B ignore cette réponse ARP parce que l'adresse MAC virtuelle est identique à l'adresse d'interface E1 du routeur B.

Il existe une restriction connue avec le contrôleur Ethernet 10 MB sur les routeurs de la gamme Cisco 2500 et 4500. Le contrôleur Ethernet ne prend en charge qu'une adresse MAC simple dans son filtre d'adresse. En conséquence, seulement un groupe HSRP peut être configuré dans une interface. L'adresse MAC de HSRP est également utilisée comme l'adresse MAC de l'interface. Ceci pose des problèmes quand le même groupe HSRP est configuré sur différents Ethernet sur le même routeur. La commande show standby indique l'utilisation de l'adresse MAC comme adresse MAC de HSRP.

Il existe deux contournements à ce problème :

- Configurer différents groupes HSRP sur différentes interfaces.Remarque: Ce contournement est recommandé.
- Émettez la commande standby use-bia sur une ou les deux interfaces.

Les flux MLS ne sont pas créés pour les périphériques qui utilisent l'adresse IP de secours de HSRP comme passerelle par défaut

La commutation MLS peut échouer quand le HSRP est activé et que vous utilisez le logiciel Cisco IOS Version 12.1(4)E sur l'un des éléments suivants :

- Supervisor Engine 1/MSFC1
- Supervisor Engine 2/MSFC2

- Supervisor Engine 1/MSFC2

Les symptômes sont différents pour chaque combinaison, comme indiqué dans cette liste :

- Pour Supervisor Engine 1/MSFC1 et Supervisor Engine 1/MSFC2 (qui utilisent Netflow-MLS) - la création de raccourcis MLS peut échouer quand le trafic est envoyé à une adresse MAC de HSRP. Tout client qui utilise l'adresse IP de secours de HSRP comme passerelle par défaut utilise l'adresse MAC de HSRP.
- Pour Supervisor Engine 2/MSFC2 (qui utilise Cisco Express Forwarding-MLS) - il est possible que la table de juxtaposition Cisco Express Forwarding ne puisse pas être remplie correctement sur le commutateur.

Référez-vous à l'ID de débogage Cisco CSCds89040 (clients enregistrés seulement). Le correctif est disponible avec le logiciel Cisco IOS Version 12.1(5a)E pour les images CatOS (c6msfc), et avec le logiciel Cisco IOS Version 12.1(5a)E1 pour les images du logiciel Cisco IOS (c6sup).

Problèmes d'interopérabilité HSRP-CGMP avec Catalyst 2948G, 2980G, 4912G, 4003 et 4006

La gamme de produits du logiciel Catalyst 4000 (2948G, 2980G, 4912G, 4003 et 4006) a plusieurs problèmes liés à l'interopérabilité entre HSRP et CGMP. Tous les problèmes sont résolus dans les versions logicielles 6.3.6 et 7.2.1.

L'activation de CGMP peut poser des problèmes avec HSRP. Ce problème est résolu dans la version logicielle 6.3(6). Un routeur dans l'état standby de HSRP passe à l'état active. Quand l'état est restauré, le routeur ne retourne pas de l'état active à l'état standby. Ce problème est résolu dans la version logicielle 6.3(6).

Si vous exécutez HSRP et que vous avez activé CGMP Leave, l'utilisation de McastRxpeut montre une utilisation du CPU à 25 pour cent. Ce problème se produit parce que CGPM Leave et les paquets Hello de HSRP partagent la même adresse MAC de destination. Le problème est résolu dans la version logicielle 6.3(6).

Informations connexes

- Support pour les produits LAN
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems