Résolution des problèmes HSRP dans les réseaux de commutateurs Catalyst

Table des matières

Introduction

Ce document décrit les problèmes courants et les façons de dépanner les problèmes liés au protocole HSRP (Hot Standby Router Protocol).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Compréhension de HSRP

Informations générales

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 absents
- Messages d'erreur du commutateur liés à HSRP
- Diffusion unicast du réseau excessive sur la configuration de HSRP

> **Remarque** : ce document explique en détail comment dépanner HSRP dans les environnements de commutateurs 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.

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 des stations 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 sélectionné dans le groupe est chargé de transférer les paquets que les hôtes envoient au routeur virtuel. Ce routeur est connu en tant que routeur actif. Un autre routeur est choisi comme routeur de secours. 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 transfère 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 tombe en panne, le routeur de secours prend le relais comme 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.

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 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 fonction Rechercher de votre navigateur pour 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	**Code Op**	**Province**	**Hellotime (temps du message Hello)**
Temps D'Attente	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 : 0 - bonjour, 1 - coup d'État et 2 - démission. Des messages Hello sont envoyés pour indiquer 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 - apprendre, 2 - écouter, 4 - parler, 8 - veille et 16 - actif.
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	Ce champ contient un mot de passe à huit caractères en texte clair.

Data (8 octets)	
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

Province	Définition
`Initialement`	C'est l'état au démarrage. Cet état indique que HSRP n'est pas exécuté. Cet état est gén par une modification de configuration ou quand une interface devient disponible pour la première fois.
`Renseignez-vous`	Le routeur n'a pas déterminé l'adresse IP virtuelle et n'a pas encore vu un message Hello authentifié du routeur actif. Dans cet état, le routeur attend toujours de recevoir des informations du routeur actif.
`Écouter`	Le routeur connaît l'adresse IP virtuelle, mais n'est ni le routeur actif, ni le routeur de secc détecte à l'oreille les messages Hello de ces routeurs.
`Parler`	Le routeur envoie des messages Hello périodiques et participe activement à l'élection du routeur actif et/ou de secours. Un routeur ne peut pas entrer dans l'état `speak à moins qu' possède l'adresse IP virtuelle.`
`En veille`	Le routeur est un candidat pour devenir le prochain routeur actif et envoie des messages périodiques. À l'exclusion de conditions passagères, il y a, tout au plus, un routeur dans le groupe `standby.`
`Actif`	Le routeur transmet les paquets qui sont envoyés à l'adresse MAC virtuelle du groupe. Le routeur envoie des messages Hello périodiques. À l'exclusion de conditions passagères, y avoir, tout au 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 diminuer ces paramètres de minuteur pour accélérer le basculement ou la préemption, mais pour éviter une utilisation accrue du processeur et un basculement inutile de l'état de veille, ne réglez pas le minuteur Hello sur une (1) seconde ou le minuteur de mise en attente sur une (4) seconde. 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 timers peuvent être modifiés 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 :

Minuteur	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	Expiration du minuteur de routeur actif Le minuteur de routeur actif est défini en fonction du délai d'attente lorsque le dernier message Hello est détecté par le routeur actif.
4	Expiration du minuteur de routeur de secours Le minuteur de routeur de secours est défini en fonct délai d'attente lorsque le dernier message Hello est détecté par le routeur de secours.
5	Expiration du minuteur de message Hello Le minuteur périodique de l'envoi des messages Hello a expiré.
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 :

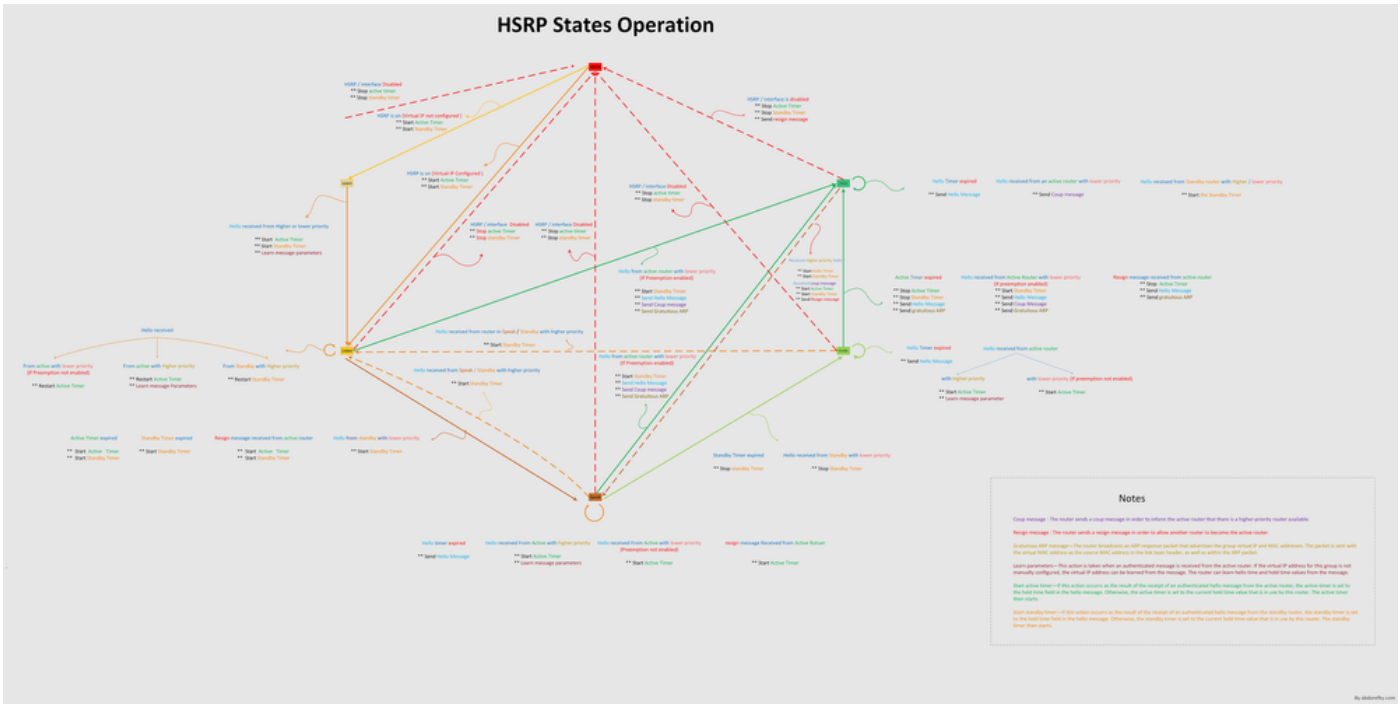
Lettre	Action
A	Start active timer : si cette action se produit suite à la réception d'un message Hello authentifié du routeur actif, le minuteur actif est défini sur le champ de durée d'attente dans le message Hello. Autrement, le temporisateur actif est défini à la valeur actuelle du temps d'attente qui est utilisée pa routeur. Le temporisateur actif démarre ensuite.
B	Start standby timer : si cette action se produit suite à la réception d'un message Hello authentifié du routeur de secours, le compteur de secours est défini sur le champ de durée d'attente dans le mess 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 ensuite.
C	Stop active timer : le minuteur actif s'arrête.
D	Stop standby timer : le compteur de veille s'arrête.
E	Learn parameters : cette action est effectuée lorsqu'un message authentifié est reçu du routeur act l'adresse IP virtuelle pour ce groupe n'est pas configurée manuellement, l'adresse IP virtuelle peut apprise à partir du message. Le routeur peut retenir les valeurs du temps Hello et du temps d'atten
F	Send hello message : le routeur envoie un message Hello avec son état actuel, sa durée Hello et s durée d'attente.
G	Send coup message : le routeur envoie un message coup afin d'informer le routeur actif qu'un route priorité supérieure est disponible.
H	Send resign message : le routeur envoie un message de démission afin de permettre à un autre ro de devenir le routeur actif.
I	Send gratuitous ARP message : le routeur diffuse un paquet de réponse ARP qui annonce les adre IP et MAC virtuelles du groupe. Le paquet est envoyé avec l'adresse MAC virtuelle comme adresse

MAC source dans l'en-tête de la couche de liaison ainsi que dans le paquet ARP.

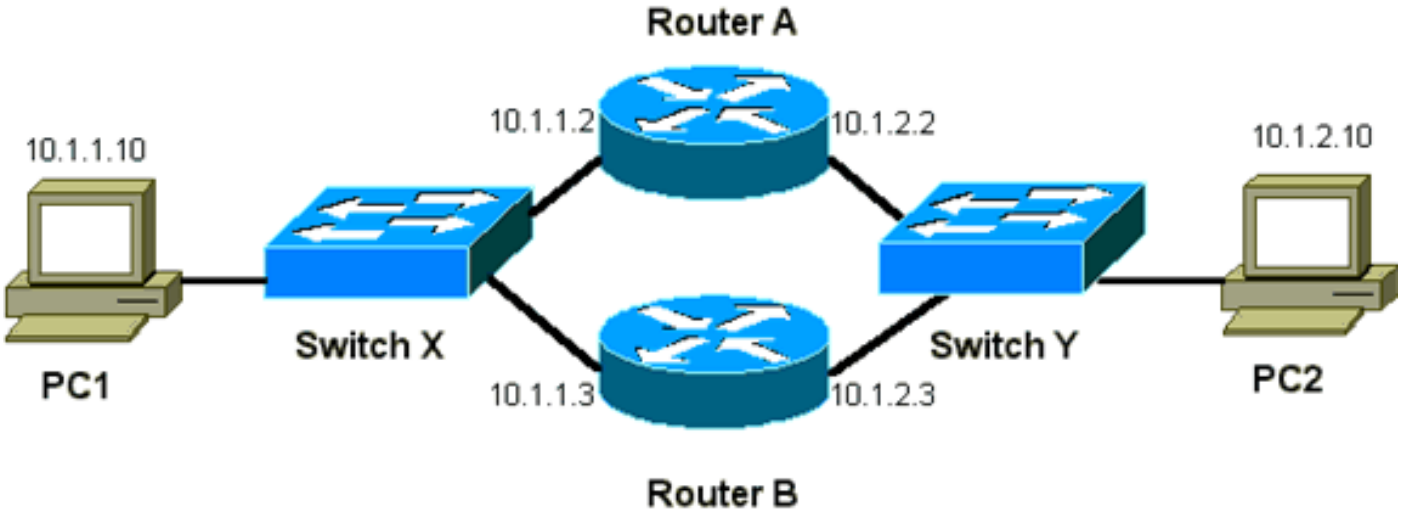
Tableau des états HSRP

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 schéma est détaillé et n'est pas nécessaire à des fins de dépannage général.

Pour obtenir une image à haute résolution du diagramme, voir les opérations d'états HSRP.



Flux des paquets



Périphérique	Adresse MAC :	Adresse IP	Subnet Mask (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 GigabitEthernet 0/0
 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 GigabitEthernet 0/1 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 GigabitEthernet 0/0
    ip address 10.1.1.3 255.255.225.0
    mac-address 4000.0000.0020
    standby 1 ip 10.1.1.1

interface GigabitEthernet 0/1 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 des adresses MAC statiques à des fins d'illustration uniquement. Ne configurez pas les adresses MAC statiques à moins que vous deviez le faire.

Vous devez comprendre le concept derrière le flux de paquets lorsque vous obtenez des traces de renifleur pour dépanner des 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 source	MAC de destination	Adresse IP source	Adresse IP de destination
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	10.1.2.10
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	10.1.1.10
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 adresse IP en double

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 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

Lorsque vous dépannez ces messages d'erreur, consultez les étapes de dépannage dans la section Dépannage de HSRP dans les commutateurs Catalyst de ce document. Tous les modules de dépannage sont applicables à cette section, qui inclut les modules de 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 GigabitEthernet 0/0
 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 : HSRP change d'état en continu (actif, veille, parler) 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
```

Jul 29 14:03:19.441: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active Jul 29 16:27:04.133: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak Jul 29 16:31:49.035: %HSRP-5-STATECHANGE: Vlan10 Grp 110 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 dans l'étude de cas n° 1, tous les modules de dépannage sont applicables à la résolution des changements d'état HSRP, en particulier le débogage HSRP de couche 3.

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.

Pour augmenter la taille du SPD (Selective Packet Discard), passez en mode de configuration et exécutez les commandes suivantes 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 la file d'attente, aller au mode d'interface du VLAN et exécuter cette commande :

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

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

Étude de cas #3 : HSRP ne reconnaît pas les homologues

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 State Changes and Switch Reports SYS-4-P2_WARN: 1/Host <mac_address> Is Flapping Between Port <port_1> and Port <port_2> in Syslog

Ces messages d'erreur peuvent apparaître :

```
2001 Jan 03 14:18:43 %SYS-4-P2_WARN: 1/Host 00:00:0c:14:9d:08
  is flapping between port 2/4 and port 2/3
```

Feb 4 07:17:44 AST: %SW_MATM-4-MACFLAP_NOTIF: Host 0050.56a9.1f28 in vlan 1027 is flapping between port Te1/0/7 and port Te2/0/2

Dans les commutateurs Catalyst, le commutateur signale une adresse MAC hôte qui se déplace si l'adresse MAC hôte se déplace deux fois en 15 secondes. Une cause possible 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** : suivez également les étapes de la section Dépannage de HSRP dans les commutateurs Catalyst de ce document.

1. Déterminez la source correcte (port) de l'adresse MAC hôte.
2. Déconnectez le port qui ne doit pas fournir 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 #5 : Asymmetric Routing and HSRP (Excessise Flooding of Unicast Traffic in Network with Routers that run HSRP)

Avec le routage asymétrique, les paquets de transmission et de réception utilisent des chemins différents entre un hôte et l'homologue avec lequel il communique. 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 définit le HSRP sur actif ou en veille. 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.

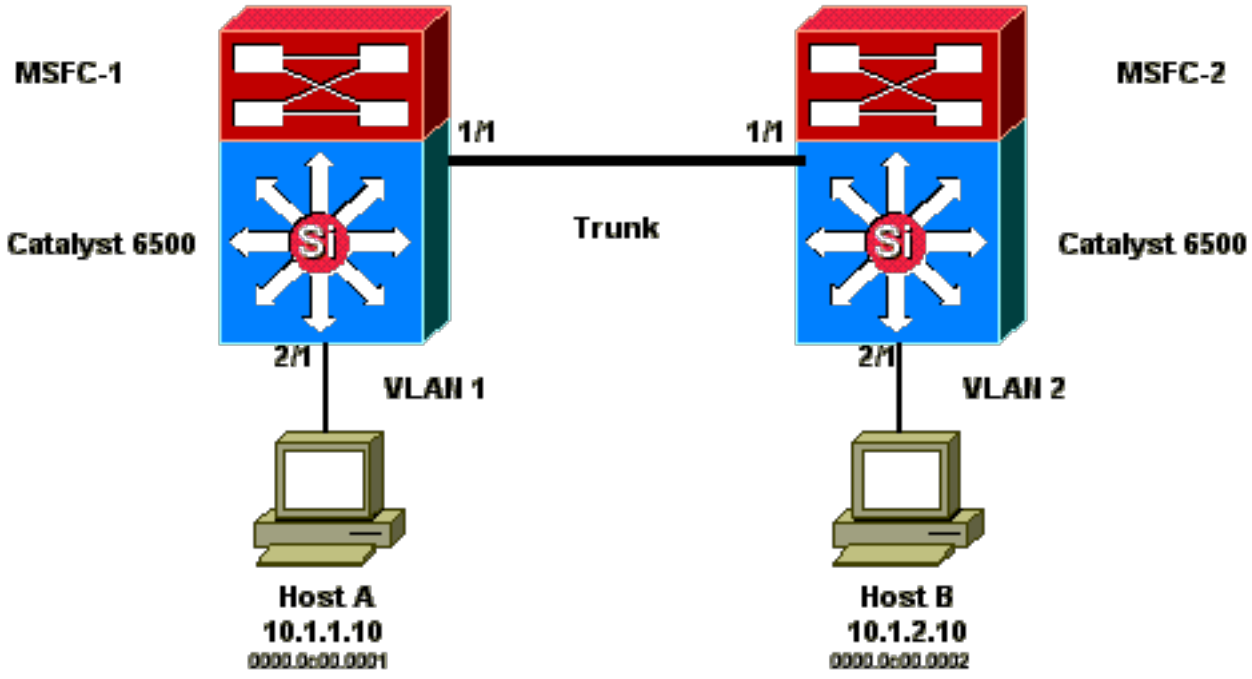
Les symptômes du routage asymétrique incluent :

- 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 : la durée d'expiration 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 temps de vieillissement ARP des stations de travail hôtes n'est pas significatif pour cette discussion. mais, l'exemple définit le temps 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 données de sortie sont des extraits de la commande **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, VLAN 1 est à l'état `actif` HSRP et VLAN 2 est à l'état de `veille` HSRP. 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** : par souci de concision, l'adresse MAC du commutateur Switch1 pour le routeur HSRP et l'adresse MAC ne sont pas incluses dans les autres tables 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 transfère le paquet à l'hôte B. Afin de réécrire le paquet, MSFC1 envoie une requête ARP pour l'hôte B, car l'hôte se trouve sur une interface connectée directement. 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. Comme l'hôte A réside sur un autre VLAN, l'hôte B transfère la réponse via 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. MSFC2 envoie une requête ARP pour l'hôte A, car il est directement connecté au VLAN 1. Le commutateur 2 remplit sa table d'adresses 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

Considérons le cas de la requête ping continue de l'hôte B par l'hôte A. N'oubliez pas que l'hôte A envoie le paquet écho à MSFC1 et que l'hôte B envoie la réponse écho à MSFC2, ce qui crée un routage asymétrique. 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	Commutateur 1	Table ARP	Table ARP	Commutateur 2	Table ARP

Hôte A	Tableau d'adresses MAC Port du VLAN MAC	MSFC1	MSFC2	Tableau d'adresses MAC Port du VLAN MAC	Hôte B
10.1.1.1 : 000.0c07.ac01 10.1.1.3 : 0003.6bf1.2a0	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001 10.1.2.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002 10.1.1.10 0000.0c00.0001	0000.0c00.0002 2 2/1	10.1.2.2 : 003.6bf1.2a01 10.1.2.1 : 000.0c07.ac01

Les paquets de réponse d'écho provenant de l'hôte B rencontrent le même problème après l'entrée d'adresse MAC pour les âges de l'hôte A sur le commutateur 2. L'hôte B transfère la réponse d'écho à MSFC2, qui à son tour achemine 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 :

- Logiciel Cisco IOS :**mac address-table aging-time <seconds> vlan <vlan_id>**

Étude de cas #6 : l'adresse IP virtuelle HSRP est signalée comme 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 emprunté par les paquets entre les noeuds 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 #7 : HSRP provoque une violation 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 #9 : %Interface Hardware Ne Peut Pas Prendre En Charge Plusieurs Groupes

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

```
%Interface hardware cannot support multiple groups
```

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.**

Dépannage de HSRP dans les commutateurs Catalyst

A. Vérification de la configuration du routeur HSRP

1. Vérification de l'adresse IP unique de l'interface du 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. Vérification des adresses IP et des numéros de groupe de secours (HSRP)

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 110 State is Active 2 state changes, last state change 00:01:34 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.144 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec) Priority 110 (configured 110) Group name is "hsrp-Vl10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:00:27 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.096 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec) Priority 110 (configured 110) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1 Router_2#show standby Vlan10 - Group 110 State is Standby 1 state change, last state change 00:03:15 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.088 secs Preemption disabled Active router is 192.168.10.1, priority 110 (expires in 11.584 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-Vl10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Standby 1 state change, last state change 00:02:53 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.352 secs Preemption disabled Active router is 192.168.11.1, priority 110 (expires in 9.120 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1

3. Vérifiez que l'adresse IP de secours (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 110 State is Active 2 state changes, last state change 00:01:34 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.144 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec) Priority 110 (configured 110) Group name is "hsrp-Vl10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:00:27 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.096 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec) Priority 110 (configured 110) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1 Router_2#show standby Vlan10 - Group 110 State is Standby 1 state change, last state change 00:03:15 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.088 secs Preemption disabled Active router is 192.168.10.1, priority 110 (expires in 11.584 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-Vl10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Standby 1 state change, last state change 00:02:53 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.352 secs Preemption disabled Active router is 192.168.11.1, priority 110 (expires in 9.120 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1

4. Quand utiliser la commande standy 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. Vérifier la configuration de la liste de contrôle 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 10.19.0.0, 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)
```

B. Vérification de la configuration de Catalyst Fast EtherChannel et de l’agrégation

1. Vérifier la configuration de trunking

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 :

- activé
- souhaitable
- auto
- désactivé
- 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 l’agrégation sont configurés pour utiliser le même VLAN natif et la même encapsulation. 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 interfaces <interface> trunk** pour une référence rapide qui montre ces informations. Voici un exemple :

L2Switch_1#show interfaces gigabitEthernet1/0/13 trunk Port Mode Encapsulation Status Native vlan Gi1/0/13 on 802.1q trunking

1 Port Vlans allowed on trunk Gi1/0/13 1-4094 Port Vlans allowed and active in management domain Gi1/0/13 1,10-11,70,100,300-309 Port Vlans in spanning tree forwarding state and not pruned Gi1/0/13 1,10-11,70,100,300-309
Router_1#show interfaces gigabitEthernet1/0/1 trunk Port Mode Encapsulation Status Native vlan Gi1/0/1 on 802.1q trunking 1 Port Vlans allowed on trunk Gi1/0/1 1-4094 Port Vlans allowed and active in management domain Gi1/0/1 1,10-11,100,206,301,307,401,900,3001-3002 Port Vlans in spanning tree forwarding state and not pruned Gi1/0/1 1,10-11,100,206,301,307,401,900,3001-3002

2. Vérification de la configuration de Fast EtherChannel (Port Channeling)

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 :

- activé
- souhaitable
- auto

Cependant, dans cet exemple, les interfaces ne sont pas membres d'un port-channel :

Router_1#show etherchannel summary Flags: D - down P - bundled in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable for bundling w - waiting to be aggregated d - default port A - formed by Auto LAG Number of channel-groups in use: 0 Number of aggregators: 0 Group Port-channel Protocol Ports ------+-------------+-----------+---------- Router_1#
Router_2#show etherchannel summary Flags: D - down P - bundled in port-channel I - stand-alone s - suspended H - Hot-standby (LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable for bundling w - waiting to be aggregated d - default port A - formed by Auto LAG Number of channel-groups in use: 0 Number of aggregators: 0 Group Port-channel Protocol Ports ------+-------------+-----------+---------- Router_2#

3. Examinez la table de transfert des adresses MAC du 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 Vlan10 - Group 110 State is Active 2 state changes, last state change 00:37:03 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.768 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.368 sec) Priority 110 (configured 110) Group name is "hsrp-Vl10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:35:56 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.472 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.336 sec) Priority 110 (configured 110) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1

Router_1#show interfaces vlan 10 Vlan10 is up, line protocol is up , Autostate Enabled Hardware is Ethernet SVI, address is d4e8.801f.4846 (bia d4e8.801f.4846) Internet address is 192.168.10.1/24 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:01, output hang never Last clearing of "show interface" counters never Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 9258 packets input, 803066 bytes, 0 no buffer Received 0 broadcasts (0 IP multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 3034 packets output, 368908 bytes, 0 underruns Output 0 broadcasts (0 IP multicasts) 0 output errors, 2 interface resets 0 unknown protocol drops 0 output buffer failures, 0 output buffers swapped out

L2Switch_1#show mac address-table address 0000.0c07.ac6e Mac Address Table ---------- Vlan Mac Address Type Ports ---- ----------- -------- ----- 10 0000.0c07.ac6e DYNAMIC Gi1/0/13 Total Mac Addresses for this criterion: 1
L2Switch_1#show mac address-table address 0000.0c07.ac6f Mac Address Table ---------- Vlan Mac

Address Type Ports ---- ----------- -------- ----- 11 0000.0c07.ac6f DYNAMIC Gi1/0/13 Total Mac Addresses for this criterion: 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 :

L2Switch_1#show mac address-table aging-time vlan 10 Global Aging Time: 300 Vlan Aging Time ---- ---------- 10 300
L2Switch_1#show mac address-table aging-time vlan 11 Global Aging Time: 300 Vlan Aging Time ---- ---------- 11 300

C. Vérification de la connectivité de la 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 110 State is Active 2 state changes, last state change 00:54:03 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.848 secs Preemption enabled Active router is local Standby router is unknown Priority 110 (configured 110) Group name is "hsrp-Vl10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:52:56 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.512 secs Preemption enabled Active router is local Standby router is unknown Priority 110 (configured 110) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1

Router_2#show standby Vlan10 - Group 110 State is Init (interface down) 2 state changes, last state change 00:00:42 Virtual IP address is 192.168.10.100 Active virtual MAC address is unknown (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Preemption disabled Active router is unknown Standby router is unknown Priority 109 (configured 109) Group name is "hsrp-Vl10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Init (interface down) 2 state changes, last state change 00:00:36 Virtual IP address is 192.168.11.100 Active virtual MAC address is unknown (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Preemption disabled Active router is unknown Standby router is unknown Priority 109 (configured 109) Group name is "hsrp-Vl11-111" (default) FLAGS: 0/1

1. Vérifier le statut 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 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 administratively down down Vlan11 192.168.11.2 YES manual administratively 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_2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router_2(config)#interface vlan 10
Router_2(config-if)#no shutdown
Router_2(config-if)#end
```

Router_2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router_2(config)#interface vlan 11 Router_2(config-if)#no shutdown Router_2(config-if)#end

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 down Vlan11 192.168.11.2 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: Vlan10 state Active-> Speak
3d04h: %LINK-5-CHANGED: Interface Vlan10, changed state to down
3d04h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, 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_2#show interface vlan 10 Vlan10 is down, line protocol is down , Autostate Enabled Hardware is Ethernet SVI, address is 1880.90d8.5946 (bia 1880.90d8.5946) Internet address is 192.168.10.2/24 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:10, output 00:00:08, output hang never Last clearing of "show interface" counters never Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 1243 packets input, 87214 bytes, 0 no buffer Received 0 broadcasts (0 IP multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 23 packets output, 1628 bytes, 0 underruns Output 0 broadcasts (0 IP multicasts) 0 output errors, 2 interface resets 0 unknown protocol drops 0 output buffer failures, 0 output buffers swapped out

2. Modification de liaison et erreurs de port

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

- **show logging**
- **show interfaces <interface> counters**
- **show interfaces <interface> status**

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` :

L2Switch_1#show logging Syslog logging: enabled (0 messages dropped, 5 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled) No Active Message Discriminator. No Inactive Message Discriminator. Console logging: level informational, 319 messages logged, xml disabled, filtering disabled Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled Buffer logging: level debugging, 467 messages logged, xml disabled, filtering disabled Exception Logging: size (4096 bytes) Count and timestamp logging messages: disabled File logging: disabled Persistent logging: disabled No active filter modules. Trap logging: level informational, 327 message lines logged Logging Source-Interface: VRF Name: Log Buffer (10000 bytes): *Jul 26 17:52:07.526: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up *Jul 26 17:52:09.747: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down *Jul 26 17:57:11.716: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307. *Jul 26 17:57:11.716: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type. *Jul 26 17:57:13.583: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up *Jul 26 17:57:16.237: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down *Jul 26 18:02:16.481: %SPANTREE-7-

RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307. *Jul 26 18:02:16.481: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type. *Jul 26 18:02:18.367: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up *Jul 26 18:02:20.561: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down

Émettez la commande **show interfaces <interface> status** afin de déterminer l'état général d'un port. Voici un exemple :

L2Switch_1#show interfaces gigabitEthernet 1/0/13 status Port Name Status Vlan Duplex Speed Type Gi1/0/13 connected trunk a-full a-1000 10/100/1000BaseTX

L'état de l'interface 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 Récupérer l'état de port Errdisable sur les plates-formes Cisco IOS 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.

L2Switch_1#show interfaces gi1/0/13 counters errors Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize OutDiscards Gi1/0/13 **0 0 0 0 0 0** `Port Single-Col Multi-Col Late-Col Excess-Col Carri-Sen Runs Gi1/0/13` **0 0 0 0 0 0**

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 `In` et `Out` indiquent le nombre de paquets de monodiffusion, de 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.`

`L2Switch_1`#show interfaces gi1/0/13 counters Port InOctets InUcastPkts InMcastPkts InBcastPkts Gi1/0/13 304933333 1180453 1082538 14978 Port OutOctets OutUcastPkts OutMcastPkts OutBcastPkts Gi1/0/13 282752538 276716 824562 588960

3. Vérification de la connectivité IP

Vérifiez la connectivité IP. Envoyez une requête ping IP depuis le routeur associé vers le périphérique HSRP distant. 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#show run interface vlan 10 Building configuration... Current configuration : 141 bytes ! interface Vlan10 ip address 192.168.10.1 255.255.255.0 standby 110 ip 192.168.10.100 standby 110 priority 110 standby 110 preempt end Router_2#show run interface vlan 10 Building configuration... Current configuration : 120 bytes ! interface Vlan10 ip address 192.168.10.2 255.255.255.0 standby 110 ip 192.168.10.100 standby 110 priority 109 end Router_1#ping 192.168.10.2 repeat 1500 Type escape

sequence to abort. Sending 1500, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!
!! !!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/9 ms

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

4. Recherchez la 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. 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. Voici des exemples de sorties de commande :

> **Remarque** : accédez au lien suivant pour Comprendre et configurer la fonctionnalité UDLD Cela dépend de la plate-forme utilisée.

Une autre option qui peut aider à vérifier une liaison unidirectionnelle si UDLD n'est pas disponible est l'utilisation du 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.

Router_1#show cdp Global CDP information: Sending CDP packets every 60 seconds Sending a holdtime value of 180 seconds Sending CDPv2 advertisements is enabled Router_1#show cdp neighbors gi1/0/1 detail ------------------------- Device ID: L2Switch_1.cisco.com Entry address(es): IP address: 192.168.70.1 IPv6 address: 2001:420:140E:2101::1 (global unicast) IPv6 address: FE80::2FE:C8FF:FED3:86C7 (link-local) Platform: cisco WS-C3650-12X48UR, Capabilities: Router Switch IGMP Interface: GigabitEthernet1/0/1, Port ID (outgoing port): GigabitEthernet1/0/13 Holdtime : 173 sec Version : Cisco IOS Software [Denali], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 16.3.8, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2019 by Cisco Systems, Inc. Compiled Wed 13-Feb-19 03:00 by mcpre advertisement version: 2 VTP Management Domain: 'CALOnet' Native VLAN: 1 Duplex: full Management address(es): IP address: 192.168.70.1 Spare Pair PoE: Yes, Spare Pair Detection Required: No Spare Pair PD Config: Disable, Spare Pair PSE Operational: No Total cdp entries displayed : 1

5. Références supplémentaires de dépannage de la 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
- Récupérer l'état du port Errdisable sur les plates-formes Cisco IOS

- 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 HSRP de couche 3

Si les changements d'état HSRP sont fréquents, utilisez les commandes de débogage HSRP (en mode enable) sur le routeur afin de surveiller l'activité 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 HSRP standard

Dans Cisco IOS, activez la fonctionnalité de débogage de HSRP avec la commande **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 Jul 29 16:12:16.889: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100 Jul 29 16:12:16.996: HSRP: Vl11 Grp 111 Hello in 192.168.11.2 Standby pri 109 vIP 192.168.11.100 Jul 29 16:12:17.183: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100 Jul 29 16:12:17.366: HSRP: Vl11 Grp 111 Hello out 192.168.11.1 Active pri 110 vIP 192.168.11.100 Jul 29 16:12:18.736: HSRP: Vl10 Interface adv in, Passive, active 0, passive 1, from 192.168.10.2 Jul 29 16:12:19.622: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
```

2. Débogage HSRP conditionnel (limitation du résultat basé sur le groupe de secours 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 10 110
Condition 1 set
Router_1#
Jul 29 16:16:20.284: Vl10 HSRP110 Debug: Condition 1, hsrp Vl10 HSRP110 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
Jul 29 16:16:44.797: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:45.381: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:16:47.231: HSRP: Vl10 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:48.248: HSRP: Vl10 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
```

3. Débogage HSRP amélioré

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 événeme et tous les paquets de HSRP
debug standby errors	Affiche les erreurs HSRP
debug standby events [[all] | [hsrp | redondance | piste]] [détail]	Affiche les évènements HSRP
debug standby packets [[all | abrégé] | [annoncer | coup d'Etat | bonjour | démissionner]] [détail]	Affiche les paquets HSRP
debug standby terse	Afficher une plage limitée d'erreurs, d'événements et de 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 (protocol, neighbor, redundancy, track, ha, arp, interface) HSRP Packets debugging is on (Coup, Resign) Router_2# *Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Resign in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Standby: i/Resign rcvd (110/192.168.10.1) *Jul 29 16:49:35.416: HSRP: Vl10 Grp 110 Active router is local, was 192.168.10.1 *Jul 29 16:49:35.416: HSRP: Vl10 Nbr 192.168.10.1 no longer active for group 110 (Standby) *Jul 29 16:49:35.417: HSRP: Vl10 Nbr 192.168.10.1 Was active or standby - start passive holddown *Jul 29 16:49:35.417: HSRP: Vl10 Grp 110 Standby router is unknown, was local *Jul 29 16:49:35.417: HSRP: Vl10 Grp 110 Standby -> Active *Jul 29 16:49:35.418: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active *Jul 29 16:49:35.418: HSRP: Peer not present *Jul 29 16:49:35.418: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Standby -> Active *Jul 29 16:49:35.419: HSRP: Vl10 Grp 110 Added 192.168.10.100 to ARP (0000.0c07.ac6e) *Jul 29 16:49:35.420: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" standby, local -> unknown *Jul 29 16:49:35.421: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Standby -> Active *Jul 29 16:49:38.422: HSRP: Vl10 IP Redundancy "hsrp-Vl10-110" update, Active -> Active

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 :

Rotuer_2#debug condition standby vlan 10 110 Condition 1 set Router_2#debug condition interface gigabitEthernet 1/0/1 vlan-id 10 Condition 2 set Router_2#debug standby HSRP debugging is on Router_2# *Jul 29 16:54:12.496: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:15.122: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:17.737: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:18.880: HSRP: Vl10 Nbr 192.168.10.1 is passive *Jul 29 16:54:20.316: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Active pri 109 vIP 192.168.10.100 *Jul 29 16:54:20.322: HSRP: Vl10 Grp 110 Coup in 192.168.10.1 Listen pri 110 vIP 192.168.10.100 *Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active: j/Coup rcvd from higher pri router (110/192.168.10.1) *Jul 29 16:54:20.323: HSRP: Vl10 Grp 110 Active router is 192.168.10.1, was local *Jul 29 16:54:20.323: HSRP: Vl10 Nbr 192.168.10.1 is no longer passive *Jul 29 16:54:20.324: HSRP: Vl10 Nbr 192.168.10.1 active for group 110 *Jul 29 16:54:20.324: HSRP: Vl10 Grp 110 Active -> Speak *Jul 29 16:54:20.325: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak *Jul 29 16:54:20.325: HSRP: Peer not present *Jul 29 16:54:20.325: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Active -> Speak *Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Removed 192.168.10.100 from ARP *Jul 29 16:54:20.326: HSRP: Vl10 Grp 110 Deactivating MAC 0000.0c07.ac6e *Jul 29 16:54:20.327: HSRP: Vl10 Grp 110 Removing 0000.0c07.ac6e from MAC address filter *Jul 29 16:54:20.328: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:20.328: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:23.104: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:23.226: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:25.825: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:25.952: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:28.427: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:28.772: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Speak pri 109 vIP 192.168.10.100 *Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Speak: d/Standby timer expired (unknown) *Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Standby router is local *Jul 29 16:54:30.727: HSRP: Vl10 Grp 110 Speak -> Standby *Jul 29 16:54:30.727: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby *Jul 29 16:54:30.728: HSRP: Peer not present *Jul 29 16:54:30.728: HSRP: Vl10 Grp 110 Redundancy "hsrp-Vl10-110" state Speak -> Standby *Jul 29 16:54:30.728: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:31.082: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:33.459: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:33.811: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:36.344: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:36.378: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.856: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.876: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.688: HSRP: Vl10 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.717: HSRP: Vl10 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100

E. Dépannage du protocole 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. Vérification de la configuration 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 spanning-tree** afin de voir toutes ces informations. Par défaut, la commande affiche ces informations pour tous les VLAN. Cependant, vous pouvez également filtrer d'autres informations VLAN si vous fournissez le numéro 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 spanning-tree** sont appris à partir 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, qu'il y ait ou non des liaisons redondantes sur le réseau. 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 spanning-tree** :

L2Switch_1#show spanning-tree vlan 10 VLAN0010 Spanning tree enabled protocol rstp Root ID Priority 32778 Address 00fe.c8d3.8680 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32778 (priority 32768 sys-id-ext 10) Address 00fe.c8d3.8680 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 300 sec Interface Role Sts Cost Prio.Nbr Type ---------- ---- --- --------- -------- -------------------------------- Gi1/0/3 Desg FWD 4 128.3 P2p Gi1/0/10 Desg FWD 4 128.10 P2p Edge Gi1/0/11 Desg FWD 4 128.11 P2p Gi1/0/13 Desg FWD 4 128.13 P2p Gi1/0/14 Desg FWD 4 128.14 P2p Gi1/0/15 Desg FWD 4 128.15 P2p Gi1/0/16 Desg FWD 4 128.16 P2p Gi1/0/35 Desg FWD 4 128.35 P2p L2Switch_1#show spanning-tree vlan 11 VLAN0011 Spanning tree enabled protocol rstp Root ID Priority 32779 Address 00fe.c8d3.8680 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32779 (priority 32768 sys-id-ext 11) Address 00fe.c8d3.8680 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 300 sec Interface Role Sts Cost Prio.Nbr Type ---------- ---- --- --------- -------- -------------------------------- Gi1/0/3 Desg FWD 4 128.3 P2p Gi1/0/10 Desg FWD 4 128.10 P2p Edge Gi1/0/11 Desg FWD 4 128.11 P2p Gi1/0/13 Desg FWD 4 128.13 P2p Gi1/0/14 Desg FWD 4 128.14 P2p Gi1/0/15 Desg FWD 4 128.15 P2p Gi1/0/16 Desg FWD 4 128.16 P2p Gi1/0/35 Desg FWD 4 128.35 P2p

Le commutateur L2Switch_1 est la racine des VLAN 10 et 11.

2. Conditions de boucle 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

Un seul VLAN avec une condition de boucle STP peut congestionner une liaison et priver les autres VLAN de bande passante. La commande **show interfaces <interface> controller** note quels ports 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. 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 BPDU (Bridge Protocol Data Unit) STP qui sont reçues et transmises sous forme de 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.

Router_2#show interfaces gi1/0/1 controller GigabitEthernet1/0/1 is up, line protocol is up (connected) Hardware is Gigabit Ethernet, address is 1880.90d8.5901 (bia 1880.90d8.5901) Description: PNP STARTUP VLAN MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX input flow-control is on, output flow-control is unsupported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:04, output hang never Last clearing of "show interface" counters never Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 33000 bits/sec, 31 packets/sec 5 minute output rate 116000 bits/sec, 33 packets/sec 9641686 packets input, 1477317083 bytes, 0 no buffer Received 1913802 broadcasts (1151766 multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 1151766 multicast, 0 pause input 0 input packets with dribble condition detected 10702696 packets output, 4241534645 bytes, 0 underruns Output 3432 broadcasts (0 multicasts) 0 output errors, 0 collisions, 2 interface resets 9582 unknown protocol drops 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier, 0 pause output 0 output buffer failures, 0 output buffers swapped out Transmit GigabitEthernet1/0/1 Receive 4241534645 Total bytes 1477317083 Total bytes 10562003 Unicast frames 7727884 Unicast frames 4229489212 Unicast bytes 1291270617 Unicast bytes 137261 Multicast frames 1151766 Multicast frames 11812065 Multicast bytes 91096867 Multicast bytes 3432 Broadcast frames 762036 Broadcast frames 233368 Broadcast bytes 94949599 Broadcast bytes 0 System FCS error frames 0 IpgViolation frames 0 MacUnderrun frames 0 MacOverrun frames 0 Pause frames 0 Pause frames 0 Cos 0 Pause frames 0 Cos 0 Pause frames 0 Cos 1 Pause frames 0 Cos 1 Pause frames 0 Cos 2 Pause frames 0 Cos 2 Pause frames 0 Cos 3 Pause frames 0 Cos 3 Pause frames 0 Cos 4 Pause frames 0 Cos 4 Pause frames 0 Cos 5 Pause frames 0 Cos 5 Pause frames 0 Cos 6 Pause frames 0 Cos 6 Pause frames 0 Cos 7 Pause frames 0 Cos 7 Pause frames 0 Oam frames 0 OamProcessed frames 0 Oam frames 0 OamDropped frames 38144 Minimum size frames 4165201 Minimum size frames 4910833 65 to 127 byte frames 3126489 65 to 127 byte frames 1237675 128 to 255 byte frames 750243 128 to 255 byte frames 1029126 256 to 511 byte frames 1279281 256 to 511 byte frames 2205966 512 to 1023 byte frames 103668 512 to 1023 byte frames 1280952 1024 to 1518 byte frames 205229 1024 to 1518 byte frames 0 1519 to 2047 byte frames 11575 1519 to 2047 byte frames 0 2048 to 4095 byte frames 0 2048 to 4095 byte frames 0 4096 to 8191 byte frames 0 4096 to 8191 byte frames 0 8192 to 16383 byte frames 0 8192 to 16383 byte frames 0 16384 to 32767 byte frame 0 16384 to 32767 byte frame 0 > 32768 byte frames 0 > 32768 byte frames 0 Late collision frames 0 SymbolErr frames 0 Excess Defer frames 0 Collision fragments 0 Good (1 coll) frames 0 ValidUnderSize frames 0 Good (>1 coll) frames 0 InvalidOverSize frames 0 Deferred frames 0 ValidOverSize frames 0 Gold frames dropped 0 FcsErr frames 0 Gold frames truncated 0 Gold frames successful 0 1 collision frames 0 2 collision frames 0 3 collision frames 0 4 collision frames 0 5 collision frames 0 6 collision frames 0 7 collision frames 0 8 collision frames 0 9 collision frames 0 10 collision frames 0 11 collision frames 0 12 collision frames 0 13 collision frames 0 14 collision frames 0 15 collision frames 0 Excess collision frames LAST UPDATE 2384 msecs AGO

3. Notification de changement de topologie

La commande **show spanning-tree detail** est une autre commande essentielle au diagnostic des problèmes STP. 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 spanning-tree <interface> detail** pour les ports connectés au commutateur. La `dernière` entrée de `modification` indique l'heure à laquelle le dernier 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 `Number of topology changes` 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.

Autres informations utiles :

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

Voici un exemple de sortie de commande :

L2Switch_1#show spanning-tree vlan 10 detail VLAN0010 is executing the rstp compatible Spanning Tree protocol Bridge Identifier has priority 32768, sysid 10, address 00fe.c8d3.8680 Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6 We are the root of the spanning tree Topology change flag not set, detected flag not set Number of topology changes 8 last change occurred 03:21:48 ago from GigabitEthernet1/0/35 Times: hold 1, topology change 35, notification 2 hello 2, max age 20, forward delay 15 Timers: hello 0, topology change 0, notification 0, aging 300 Port 3 (GigabitEthernet1/0/3) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.3. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.3, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 0 Port 10 (GigabitEthernet1/0/10) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.10. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.10, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 The port is in the portfast mode by portfast trunk configuration Link type is point-to-point by default BPDU: sent 6063, received 0 Port 11 (GigabitEthernet1/0/11) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.11. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.11, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 0 Port 13 (GigabitEthernet1/0/13) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.13. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.13, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 3 Port 14 (GigabitEthernet1/0/14) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.14. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.14, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 3 Port 15 (GigabitEthernet1/0/15) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.15. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.15, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0 Port 16 (GigabitEthernet1/0/16) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.16. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.16, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0 Port 35 (GigabitEthernet1/0/35) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.35. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.35, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0

Ce résultat montre que la dernière modification de topologie s'est produite à partir d'un périphérique connecté à l'interface GigabitEthernet1/0/35. Ensuite, émettez la même commande **show spanning-tree detail** à partir de ce périphérique afin d'essayer de suivre le problème. Si ce commutateur qui génère les TCN est uniquement connecté à un PC ou à des terminaux, assurez-vous que STP PortFast est activé sur ces ports. 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) :

- Utilisation de PortFast et d'autres commandes pour remédier aux délais de connectivité lors du démarrage de la station de travail
- Comprendre le protocole Spanning Tree rapide (802.1w)
- Problèmes STP et considérations concernant la 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. Lorsque vous dépannez STP ou HSRP, vous pouvez supprimer la configuration de toutes les connexions FEC. Une fois que les modifications de configuration sont en place, émettez la commande **show spanning-tree 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.

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

- Comprendre l'équilibrage de charge et la redondance EtherChannel sur les commutateurs Catalyst
- Configuration des EtherChannels

5. Suppression de la 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 :

L2Switch_1#show run interface TenGigabitEthernet1/1/5 Building configuration... Current configuration : 279 bytes ! interface TenGigabitEthernet1/1/5 switchport trunk allowed vlan 300-309 switchport mode trunk storm-control broadcast level 30.00 storm-control multicast level 30.00 storm-control unicast level 30.00 spanning-tree guard root end L2Switch_1#show storm-control broadcast Key: U - Unicast, B - Broadcast, M - Multicast Interface Filter State Upper Lower Current Action Type --------- ------------- --------- ----------- ---------- --------- ---- Te1/1/5 Forwarding 30.00% 30.00% 0.00% None B Te1/1/7 Link Down 30.00% 30.00% 0.00% None B Te1/1/8 Forwarding 10.00% 10.00% 0.00% None B L2Switch_1#show storm-control multicast Key: U - Unicast, B - Broadcast, M - Multicast Interface Filter State Upper Lower Current Action Type --------- ------------- ----------- ----------- ---------- ---------- ---- Te1/1/5 Forwarding 30.00% 30.00% 0.00% None M Te1/1/7 Link Down 30.00% 30.00% 0.00% None M

6. Accès console et Telnet

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. Fonctionnalités 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 quelques documents pour vous aider à comprendre et à configurer ces fonctions :

Configurer Spanning Tree PortFast, la protection BPDU, le filtre BPDU, UplinkFast, BackboneFast et la protection contre les boucles

Comprendre et configurer la fonction Cisco UplinkFast

8. Protection BPDU

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 les périphériques reflètent les paquets ou injectent des BPDU STP dans le réseau. Lorsque vous dépannez des problèmes STP, vous pouvez activer cette fonctionnalité pour aider à isoler le problème STP.

```
L2Switch_1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. L2Switch_1(config)#spanning-tree portfast bpduguard L2Switch_1(config)#end
```

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. Diviser et conquérir

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 certaines 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.

Problèmes identifiés

État HSRP instable/instable lorsque vous utilisez Cisco 2620/2621, Cisco 3600 avec Fast Ethernet

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	Régler	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.		Une mise à niveau logicielle ; référez-vous au bogue pour les détails de révision.	Active Spanning Tree Portfast sur le port de commutateur connecté.
Cisco 2620/2621	L'état de HSRP s'affole sur 2600 avec Fast Ethernet.		Logiciel Cisco IOS® Version 12.1.3	Active Spanning Tree Portfast sur le port de commutateur 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 Spanning Tree Portfast sur le port de commutateur connecté.
Cisco 4500 avec l'interface Fast Ethernet	L'état de HSRP s'affole sur 4500 Fast Ethernet.	ID de bogue Cisco CSCds16055	Logiciel Cisco IOS® Version 12.1.5	Active Spanning Tree Portfast sur le port de commutateur connecté.

1NM-1FE-TX = module de réseau Fast Ethernet à un port (interface 10/100Base-TX).

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 <object> decrement 15
```

Où 15 est la valeur de décrément lorsque l'objet s'affale. Afin d'en savoir plus sur la commande track, veuillez naviguer vers le document Track Option dans HSRPv2 Configuration Example.

Informations connexes

- Commutateurs Catalyst LAN de campus - Accès
- Commutation LAN
- Assistance et documentation techniques - Cisco Systems

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

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