Dépanner les problèmes courants de HSRP

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Comprendre HSRP
- Informations générales
  - Fonctionnement de base
  - Termes HSRP
  - Adressage HSRP
    - Communication du routeur HSRP
    - Communication d'adresse IP de secours HSRP sur tous les supports sauf Token Ring
  - Redirections ICMP
  - Matrice de fonctionnalités HSRP
  - Fonctionnalités HSRP
  - Format de paquet
  - États HSRP
  - Minuteurs HSRP
  - Événements HSRP
  - Actions HSRP
  - Table d'état HSRP
  - Flux de paquets
    - Configuration du routeur A (routeur actif)
    - Configuration du routeur B (routeur de secours)
- Dépannage des études de cas HSRP
  - Étude de cas #1 : L'adresse IP de secours HSRP est signalée comme adresse IP en double
  - Étude de cas #2 : L'état du protocole HSRP change continuellement (actif, veille, parole) ou %HSRP-6-STATECHANGE
  - Étude de cas #3 : HSRP ne reconnaît pas l'homologue
  - Étude de cas #4 : Rapports sur les changements d'état et les commutateurs HSRP SYS-4-P2_WARN : 1/Hôte Bascule Entre Les Ports et port dans Syslog
  - Étude de cas #5 : Routage asymétrique et HSRP (inondation excessive du trafic de monodiffusion dans le réseau avec des routeurs qui exécutent HSRP)
    - MSFC1
    - MSFC2
    - Tables d'adresses ARP et MAC avant le lancement de la commande ping
    - Tables d'adresses ARP et MAC après que l'hôte A a envoyé ARP pour la passerelle par défaut
    - Tables d'adresses ARP et MAC après que l'hôte B a envoyé ARP pour sa passerelle par défaut
    - Tables d'adresses ARP et MAC après réception du paquet d'écho par l'hôte A
    - Conséquences du routage asymétrique
    - Tables d'adresses ARP et MAC après 5 minutes de ping continu de l'hôte B par l'hôte A
  - Étude de cas #6 : L'adresse IP virtuelle HSRP est signalée comme une adresse IP différente

Étude de cas #7 : HSRP provoque une violation MAC sur un port sécurisé
Solution de contournement
Étude de cas #8 : %Interface Le Matériel Ne Peut Pas Prendre En Charge Plusieurs Groupes
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
2. Vérification des adresses IP et des numéros de groupe de secours (HSRP)
3. Vérifiez que l'adresse IP de secours (HSRP) est différente par interface
4. Quand utiliser la commande standy use-bia
5. Vérifier la configuration de la liste de contrôle d'accès
B. Vérification de la configuration de Catalyst Fast EtherChannel et de l'agrégation
1. Vérifier la configuration de trunking
2. Vérification de la configuration EtherChannel
3. Examinez la table de transfert des adresses MAC du commutateur
C. Vérification de la connectivité de la couche physique
1. Vérifier le statut de l'interface
2. Modification de liaison et erreurs de port
3. Vérification de la connectivité IP
4. Recherchez la liaison unidirectionnelle
5. Références supplémentaires de dépannage de la couche physique
D. Débogage HSRP de couche 3
1. Débogage HSRP standard
2. Débogage HSRP conditionnel (limitation du résultat basé sur le groupe de secours et/ou le VLAN)
3. Débogage HSRP amélioré
E. Dépannage du protocole Spanning Tree
1. Vérification de la configuration Spanning Tree
2. Conditions de boucle Spanning Tree
3. Notification de modification de topologie
4. Suppression de diffusion
5. Accès console et Telnet
6. Fonctionnalités Spanning Tree : Portfast, UplinkFast et BackboneFast
7. Protection BPDU
8. Élagage VTP
F. Diviser et conquérir
Informations connexes

Introduction

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

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document inclut des exemples de plusieurs versions du logiciel Cisco IOS® et plates-formes matérielles. La disponibilité et le comportement des commandes varient selon la plate-forme et la version.

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.

Comprendre HSRP

Informations générales

Ce document couvre les problèmes les plus courants qui concernent le protocole HSRP :

- Rapport de routeur d'une adresse IP de secours HSRP dupliquée
- Changements d'état HSRP constants (actif, veille, parler)
- Homologues HSRP absents
- Messages d'erreur de commutateur liés à HSRP
- Diffusion de monodiffusion réseau excessive vers la configuration HSRP

Remarque : Ce document explique comment dépanner HSRP dans les environnements de commutateurs Catalyst. Le document contient de nombreuses références aux versions logicielles et à la conception de la topologie du réseau. Néanmoins, le seul objectif de ce document est de faciliter et de guider les ingénieurs sur la façon de dépanner HSRP. Ce document n'est pas conçu pour être un guide de conception, un document de recommandations logicielles ou un document de meilleures pratiques.

Les entreprises et les particuliers qui dépendent des services intranet et Internet pour leurs communications critiques ont besoin de leurs réseaux et applications et s'attendent à ce qu'ils

soient disponibles en permanence. Les clients peuvent satisfaire leurs demandes de temps de fonctionnement du réseau proche de 100 % s'ils utilisent le protocole HSRP dans le logiciel Cisco IOS®. Le protocole HSRP, qui est unique aux plates-formes Cisco, assure la redondance réseau pour les réseaux IP de manière à garantir que le trafic utilisateur récupère immédiatement et de manière transparente des pannes au premier saut dans les périphériques de périphérie du réseau ou les circuits d'accès.

Deux routeurs ou plus peuvent agir en tant que routeur virtuel unique s’ils partagent une adresse IP et une adresse MAC (couche 2 [L2]). L’adresse est nécessaire pour la redondance de la passerelle par défaut de la station de travail hôte. La plupart des stations de travail hôtes ne contiennent pas de tables de routage et n’utilisent qu’une seule adresse IP et MAC de tronçon suivant. Cette adresse est appelée passerelle par défaut. Avec HSRP, les membres du groupe de routeurs virtuels échangent continuellement des messages d'état. Un routeur peut assumer la responsabilité du routage d’un autre si un routeur est mis hors service pour des raisons planifiées ou non. Les hôtes sont configurés avec une seule passerelle par défaut et continuent à transférer des paquets IP vers une adresse IP et MAC cohérente. Le basculement des périphériques qui effectuent le routage est transparent pour les stations de travail finales.



Remarque : Vous pouvez configurer des stations de travail hôtes qui exécutent Microsoft OS pour plusieurs passerelles par défaut. Mais les passerelles par défaut multiples ne sont pas dynamiques. Le système d'exploitation utilise une seule passerelle par défaut à la fois. Le système ne sélectionne une passerelle par défaut configurée supplémentaire au démarrage que si la première passerelle par défaut configurée est jugée inaccessible par le protocole ICMP (Internet Control Management Protocol).

Fonctionnement de base

Un ensemble de routeurs qui exécutent HSRP fonctionne de concert pour présenter l'illusion d'un routeur de passerelle par défaut unique aux hôtes sur le LAN. Cet ensemble de routeurs est appelé 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 sous le nom de routeur actif. Un autre routeur est choisi comme routeur de secours. Si le routeur actif tombe en panne, le routeur en veille assume les fonctions de transfert 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 minimiser le trafic réseau, seuls les routeurs actif et en veille envoient des messages HSRP périodiques une fois que le protocole a terminé le processus de sélection. 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 tombe en panne ou devient le routeur actif, un autre routeur est sélectionné comme routeur de secours.

Chaque groupe de secours émule un seul routeur virtuel (passerelle par défaut). Pour chaque groupe, une seule adresse MAC et IP connue est attribuée à ce groupe. Plusieurs groupes de secours peuvent coexister et se chevaucher sur un réseau local, et des routeurs individuels peuvent participer à plusieurs groupes. Dans ce cas, le routeur conserve un état et des minuteurs distincts pour chaque groupe.

Termes HSRP

Terme	Définition
Routeur actif	Le routeur qui transfère actuellement les paquets pour le routeur virtuel
Routeur de secours	Le routeur de secours principal
Groupe de secours	Ensemble de routeurs qui participent au protocole HSRP et émulent conjointement un routeur virtuel
Heure Hello	Intervalle entre les messages Hello HSRP successifs d'un routeur donné
Temps d'attente	Intervalle entre la réception d'un message Hello et la présomption d'échec du routeur émetteur

Adressage HSRP

Communication du routeur HSRP

Les routeurs qui exécutent le protocole HSRP communiquent via des paquets HSRP. HSRPv1 utilise l'adresse de multidiffusion IPv4 224.0.0.2 et HSRPv2 utilise l'adresse de multidiffusion IPv4 224.0.0.102. Les deux versions utilisent le port UDP (User Datagram Protocol) 1985 (l'adressage et les exemples de ce document utilisent HSRPv1 sauf indication contraire). L’adresse de multidiffusion IP 224.0.0.2 est une adresse de multidiffusion réservée utilisée pour communiquer avec tous les routeurs. Le routeur actif fournit des paquets Hello à partir de son adresse IP configurée et de l'adresse MAC virtuelle HSRP. Le routeur de secours crée des paquets Hello à partir de son adresse IP configurée et de l'adresse MAC gravée (BIA). Cette utilisation de l'adressage source est nécessaire pour que les routeurs HSRP puissent s'identifier correctement les uns les autres.

Dans la plupart des cas, lorsque vous configurez des routeurs pour qu'ils fassent partie d'un groupe HSRP, les routeurs écoutent l'adresse MAC HSRP pour ce groupe ainsi que leur propre BIA. La seule exception à ce comportement concerne les routeurs Cisco 2500, 4000 et 4500. Ces routeurs possèdent un matériel Ethernet qui ne reconnaît qu’une seule adresse MAC. Par conséquent, ces routeurs utilisent l'adresse MAC HSRP lorsqu'ils servent de routeur actif. Les routeurs utilisent leur BIA lorsqu'ils servent de routeur de secours.

Communication d'adresse IP de secours HSRP sur tous les supports sauf Token Ring

Étant donné que les stations de travail hôtes sont configurées avec leur passerelle par défaut comme adresse IP de secours HSRP, les hôtes doivent communiquer avec l'adresse MAC associée à l'adresse IP de secours HSRP. Cette adresse MAC est une adresse MAC virtuelle composée de 0000.0c07.ac**. ** est le numéro de groupe HSRP au format hexadécimal, basé sur l'interface respective. Par exemple, le groupe HSRP 1 utilise l'adresse MAC virtuelle HSRP 000.0c07.ac01. Les hôtes sur le segment LAN adjacent utilisent le processus ARP (Address Resolution Protocol) normal afin de résoudre les adresses MAC associées.

Redirections ICMP

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

Plus tard, le logiciel Cisco IOS a introduit une méthode pour permettre les redirections ICMP avec HSRP. Cette méthode filtre les messages de redirection ICMP sortants via HSRP. L'adresse IP du tronçon suivant est remplacée par une adresse virtuelle HSRP. L'adresse IP de la passerelle dans le message de redirection ICMP sortant est comparée à une liste de routeurs actifs HSRP 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 virtuelle de ce groupe. Cette solution permet aux hôtes d'apprendre des routes optimales vers des réseaux distants et, en même temps, de maintenir la résilience fournie par HSRP.

Matrice de fonctionnalités HSRP

Référez-vous à la section Matrice des fonctionnalités de la version de Cisco IOS® et de HSRP de Comprendre les fonctionnalités du protocole de routeur de secours automatique afin d'en savoir plus sur les fonctionnalités et les versions du logiciel Cisco IOS qui prennent en charge HSRP.

Fonctionnalités HSRP

Ce document fournit des informations sur ces fonctionnalités HSRP :

- Préemption

- Suivi des interfaces
- Utilisation d'un BIA
- Plusieurs groupes HSRP
- Adresses MAC configurables
- Support Syslog
- Débogage HSRP
- Débogage HSRP amélioré
- Authentification
- Redondance IP
- Base MIB SNMP (Simple Network Management Protocol)
- HSRP pour MPLS (Multiprotocol Label Switching)

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

Format de paquet

Ce tableau indique le format de la partie données de la trame UDP HSRP :

Version	Code Op	Province	Hellotime (temps du message Hello)
Temps D'Attente	Priorité	Groupe	Réservé
Données d'authentification			
Données d'authentification			
Adresse IP virtuelle			

Ce tableau décrit chacun des champs dans le paquet HSRP :

Champ Paquet	Description
Code Op (1 octet)	Le code d'opération décrit le type de message contenu dans le paquet. Les valeurs possibles sont : 0 - bonjour, 1 - coup d'état, et 2 - démissionner. Des messages Hello sont envoyés pour indiquer qu'un routeur exécute HSRP et peut devenir le routeur actif. Les messages Coup sont envoyés lorsqu'un routeur souhaite devenir le routeur actif. Des messages de démission sont envoyés lorsqu'un routeur ne souhaite plus être le routeur actif.

État (1 octet)	Chaque routeur du groupe de secours implémente 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 - apprentissage, 2 - écoute, 4 - parole, 8 - veille et 16 - actif.
Hellotime (1 octet)	Ce champ n'a de sens que dans les messages Hello. Il contient la période approximative entre les messages Hello que le routeur envoie. Le temps est donné en secondes.
Holdtime (1 octet)	Ce champ n'a de sens que dans les messages Hello. Il indique la durée pendant laquelle les routeurs attendent un message Hello avant de lancer un changement d'état.
Priorité (1 octet)	Ce champ permet de sélectionner les routeurs actif et de secours. En comparant les priorités de deux routeurs, le routeur dont la valeur est la plus élevée devient le routeur actif. L'élément de rupture de connexion est le routeur dont l'adresse IP est la plus élevée.
Groupe (1 octet)	Ce champ identifie le groupe de secours.
Données d'authentification (8 octets)	Ce champ contient un mot de passe en clair de huit caractères.
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 acquise que si aucune adresse IP de secours HSRP n'a été configurée et que le message Hello est authentifié (si l'authentification est configurée).

États HSRP

Province	Définition
`Initialement`	C'est l'état au début. Cet état indique que HSRP ne s'exécute pas. Cet état est entré lors d'une modification de la configuration ou lorsqu'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 de 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 il n'est ni le routeur actif ni le routeur de secours. Il écoute les messages Hello de ces routeurs.
`Parler`	Le routeur envoie des messages Hello périodiques et participe activement à la sélection du routeur actif et/ou en veille. Un routeur ne peut pas passer en état `vocal` à moins qu'il ne dispose de l'adresse IP virtuelle.
`En veille`	Le routeur est candidat pour devenir le prochain routeur actif et envoie régulièrement des messages Hello. À l'exclusion des conditions transitoires, il y a, au plus, un routeur dans le groupe à l'état `veille`.
`Actif`	Le routeur transfère actuellement les paquets qui sont envoyés à l'adresse MAC virtuelle du groupe. Le routeur envoie des messages Hello périodiques. À l'exclusion des conditions transitoires, un routeur doit être, au maximum, à l'état `actif` dans le groupe.

Minuteurs HSRP

Chaque routeur utilise trois minuteurs HSRP. Les minuteurs contrôlent la transmission Hello et l'expiration des homologues. La convergence HSRP après une panne dépend de la façon dont les minuteurs hello et de maintien HSRP sont configurés. Par défaut, ces minuteurs sont définis sur 3 et 10 secondes, respectivement, ce qui signifie qu'un paquet Hello est envoyé entre les périphériques du groupe de secours HSRP toutes les 3 secondes, et le périphérique de secours devient actif lorsqu'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.



Remarque : Utilisez les valeurs de minuteur HSRP prises en charge par la plate-forme et la version logicielle. Certaines plates-formes et versions plus récentes prennent en charge les minuteurs HSRP millisecondes. Vérifiez la plage de minuteurs prise en charge et évaluez la charge du processeur, les conditions du réseau et l'échelle HSRP avant le déploiement.



Remarque : Si vous utilisez le suivi d'objet HSRP et que l'objet suivi change d'état, HSRP applique immédiatement l'action de décrément de priorité ou d'arrêt configurée. Un changement de rôle se produit uniquement lorsque les priorités HSRP, les états et la configuration de préemption qui en résultent en déclenchent un. Lorsqu'un compteur expire, le routeur passe à un nouvel état HSRP. Les compteurs peuvent être modifiés avec cette commande : standby <group-number> timers <hello-interval> <hold-time>. Par exemple, standby 1 timers 5 15.

Ce tableau fournit plus d'informations sur ces compteurs :

Minuteur	Description
Temporisateur actif	Ce minuteur est utilisé pour surveiller le routeur actif. Ce minuteur démarre chaque fois qu'un routeur actif reçoit un paquet Hello. Ce minuteur expire conformément à la valeur de temps d'attente qui est définie dans le champ associé du message Hello HSRP.
Minuteur de veille	Ce minuteur est utilisé afin de surveiller le routeur de secours. Le minuteur démarre chaque fois que le routeur de secours reçoit un paquet Hello. Ce minuteur expire en fonction de la valeur de temps d'attente définie dans le paquet Hello correspondant.
Minuteur Hello	Ce minuteur est utilisé pour synchroniser les paquets Hello. Les routeurs HSRP dans les états Speak, Standby et Active génèrent un paquet Hello lorsque le minuteur Hello expire.

Événements HSRP

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

Key (Clé)	Événements
1	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 fonction du 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 de priorité supérieure d'un routeur en état `parler`
7	Réception d'un message Hello de priorité supérieure du routeur actif
8	Réception d'un message Hello de 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 de priorité supérieure en provenance du routeur de secours
12	Réception d'un message Hello de priorité inférieure du routeur de secours

Actions HSRP

Ce tableau spécifie les actions à effectuer dans le cadre de l'automate fini :

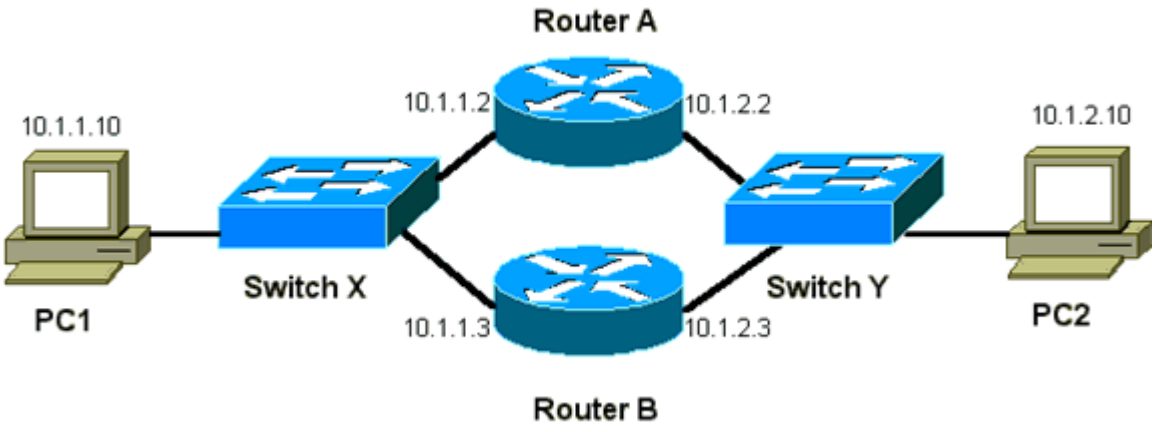
Lettre	Action
A	Start active timer : si cette action se produit suite à la réception d'un message Hello authentifié du routeur actif, le minuteur actif est défini sur le champ de durée d'attente dans le message Hello. Dans le cas contraire, le minuteur actif est défini sur la valeur de temps d'attente actuelle utilisée par ce routeur. Le minuteur 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 message Hello. Dans le cas contraire, le minuteur de veille est défini sur la valeur de temps d'attente actuelle utilisée par ce routeur. Le minuteur 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 actif. Si l'adresse IP virtuelle de ce groupe n'est pas configurée manuellement, l'adresse IP virtuelle peut être apprise à partir du message. Le routeur peut apprendre des

	valeurs de temps Hello et de temps d'attente à partir du message.
F	Send hello message : le routeur envoie un message Hello avec son état actuel, sa durée Hello et sa durée d'attente.
G	Send coup message : le routeur envoie un message coup afin d'informer le routeur actif qu'un routeur de priorité supérieure est disponible.
H	Send resign message : le routeur envoie un message de démission afin de permettre à un autre routeur de devenir le routeur actif.
I	Send gratuitous ARP message : le routeur diffuse un paquet de réponse ARP qui annonce les adresses IP et MAC virtuelles du groupe. Le paquet est envoyé avec l'adresse MAC virtuelle comme adresse MAC source dans l'en-tête de couche liaison, ainsi que dans le paquet ARP.

Table d'état HSRP

Le schéma de cette section montre les transitions d'état de la machine d'état HSRP. Chaque fois qu'un événement se produit, l'action associée se produit et le routeur passe à l'état HSRP suivant. Dans le schéma, les chiffres désignent les événements et les lettres désignent l'action associée. Le tableau de la section Événements HSRP définit les nombres, et le tableau de la section Actions HSRP définit les lettres. Utilisez ce schéma uniquement comme référence. Le schéma est détaillé et n'est pas nécessaire à des fins de dépannage général.

Flux de 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 10.1.1.3 255.255.255.0
    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 d'adresses MAC statiques à moins d'y être obligé.

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 destinés à une station de travail hôte ont l'adresse MAC source de l'adresse MAC physique (BIA) du routeur. Les paquets des machines hôtes qui sont destinés à l'adresse IP HSRP ont l'adresse MAC de destination de l'adresse MAC virtuelle HSRP. Notez que les adresses MAC ne sont pas identiques pour chaque flux entre le routeur et l'hôte.

Ce tableau présente les informations d'adresses MAC et IP respectives par flux sur la base d'une trace de renifleur qui est prise à partir du commutateur X.

Flux de paquets	MAC source	MAC de destination	Adresse IP source	Adresse IP de destination
Paquets de PC1 destinés à PC2	PC1 (0000.0c00.0001)	Adresse MAC virtuelle HSRP de l'interface Ethernet 0 du routeur A (0000.0c07.ac01)	10.1.1.10	10.1.2.10
Paquets renvoyés	Routeur A Ethernet 0	PC1 (0000.0c00.0001)	10.1.2.10	10.1.1.10

par le routeur A depuis PC2 et destinés à PC1	BIA (4000.000.0010)			
Paquets de PC1 destinés à l'adresse IP de secours HSRP (ICMP, Telnet)	PC1 (0000.0c00.0001)	Adresse MAC virtuelle HSRP de l'interface Ethernet 0 du routeur A (0000.0c07.ac01)	10.1.1.10	10.1.1.1
Paquets destinés à l'adresse IP réelle du routeur actif (ICMP, Telnet)	PC1 (0000.0c00.0001)	Routeur A Ethernet 0 BIA (4000.000.0010)	10.1.1.10	10.1.1.2
Paquets destinés à l'adresse IP réelle du routeur de secours (ICMP, Telnet)	PC1 (0000.0c00.0001)	Routeur B Ethernet 0 BIA (4000.000.0020)	10.1.1.10	10.1.1.3

Dépannage des 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 HSRP. Les messages d'erreur indiquent plutôt un problème possible de boucle STP (Spanning Tree Protocol) ou de configuration de routeur/commutateur. Les messages d'erreur ne sont que les symptômes d'un autre problème.

En outre, ces messages d'erreur n'empêchent pas le bon fonctionnement de HSRP. Le paquet HSRP en double est ignoré. Ces messages d'erreur sont limités à des intervalles de 30 secondes. Cependant, la lenteur des performances du réseau et la perte de paquets peuvent résulter de l'instabilité du réseau qui provoque les messages d'erreur `STANDBY-3-DUPADDR` de l'adresse HSRP.

Ces messages indiquent spécifiquement que le routeur a reçu un paquet de données provenant 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 retour, soit les deux routeurs dans le groupe HSRP sont passés à l'état `actif`. Comme le routeur a reçu son propre paquet, le problème vient probablement du réseau plutôt que du routeur. Divers problèmes peuvent provoquer ce comportement. Parmi les problèmes de réseau susceptibles d'être à l'origine des messages d'erreur, citons :

- Boucles STP momentanées
- Problèmes de configuration EtherChannel
- Trames en double

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. De plus, notez toute erreur dans le journal du commutateur et référencez d'autres études de cas si nécessaire.

Vous pouvez utiliser une liste d’accès afin d’empêcher le routeur actif de recevoir son propre paquet Hello de multidiffusion. Mais, il ne s'agit que d'une solution de contournement pour les messages d'erreur et cache en fait le symptôme du problème. La solution de contournement consiste à appliquer une liste d'accès entrante étendue aux interfaces HSRP. La liste d’accès bloque tout le trafic provenant de l’adresse IP physique et destiné à l’adresse de multidiffusion 224.0.0.2 de tous les 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 : L'état du protocole HSRP change continuellement (actif, veille, parole) 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 de paquets Hello HSRP de son homologue avant l'expiration du minuteur de mise en attente actif. Le résultat montre que le routeur en veille passe de l'état `veille` à l'état `actif`. Peu de temps après, le routeur revient à l'état `standby`. À moins que ce message d'erreur ne se produise pendant l'installation initiale, un problème HSRP ne cause probablement pas le message d'erreur. Les messages d'erreur signifient la perte des paquets Hello HSRP entre les homologues. Lorsque vous dépannez ce problème, vous devez vérifier la communication entre les homologues HSRP. Une perte aléatoire et momentanée de la communication de données entre les homologues est le problème le plus courant qui entraîne ces messages. Les changements d'état HSRP sont souvent dus à une utilisation CPU élevée. Si le message d'erreur est dû à une utilisation élevée du CPU, placez un analyseur sur le réseau et tracez le système qui provoque l'utilisation élevée du CPU.

Il y a plusieurs causes possibles pour la perte de paquets HSRP entre les homologues. Les problèmes les plus courants sont les problèmes de couche physique , le trafic réseau excessif provoqué par les problèmes de Spanning Tree ou le trafic excessif provoqué par chaque VLAN. Comme avec l'étude de cas #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 homologues est due à un trafic excessif causé par chaque VLAN comme mentionné, vous pouvez régler ou augmenter le SPD et maintenir la taille de la file d'attente pour surmonter le problème de suppression 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 Catalyst 6500 :

<#root>

```
(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 :

```
<#root>

(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 clear counters <interface>.

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

Le résultat du routeur dans cette section montre un routeur qui est configuré pour HSRP mais qui ne reconnaît pas ses homologues HSRP. Pour que cela se produise, le routeur doit échouer à recevoir les messages Hello HSRP du routeur voisin. Lorsque vous dépannez ce problème, consultez les sections Vérification de la connectivité de la couche physique et Vérification de la configuration du routeur HSRP de ce document. Si la connectivité de la couche physique est correcte, recherchez les modes VTP incompatibles.

```
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 : Rapports sur les changements d'état et les commutateurs HSRP

SYS-4-P2_WARN : 1/L’hôte <mac_address> oscille entre le port <port_1> et le port <port_2> dans 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, si le commutateur signale une adresse MAC hôte qui se déplace entre les ports, et 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 cet hôte pendant environ 15 secondes afin de minimiser l'impact d'une boucle STP. Si l'adresse MAC signalée qui se déplace entre deux ports est l'adresse MAC virtuelle HSRP, le problème est très probablement un problème dans lequel les deux routeurs HSRP passent à l'état `actif`.

Si l'adresse MAC qui est signalée n'est pas l'adresse MAC virtuelle HSRP, le problème peut indiquer la boucle, la duplication ou la réflexion des paquets dans le réseau. Ces types de conditions peuvent contribuer aux problèmes de HSRP. Les causes les plus courantes du déplacement des adresses MAC sont les problèmes de Spanning Tree ou de couche physique .

Lorsque vous dépannez ce message d'erreur, procédez comme suit :

1. Déterminez la source (port) correcte de l’adresse MAC hôte.
2. Déconnectez le port qui ne doit pas fournir l'adresse MAC hôte.
3. Documentez la topologie STP par VLAN et recherchez les défaillances STP.
4. Vérifiez la configuration de la canalisation des ports.
    1. Une configuration de canal de port incorrecte peut entraîner l'affolement des messages d'erreur par l'adresse MAC de l'hôte. Ceci est dû à la nature d'équilibrage de charge de la transmission de port.

Étude de cas #5 : Routage asymétrique et HSRP (inondation excessive du trafic de monodiffusion dans le réseau avec des routeurs qui exécutent 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 entraîner une diffusion de monodiffusion inconnue excessive. En outre, les entrées MLS (Multilayer Switching) peuvent être absentes. Une inondation de monodiffusion inconnue se produit lorsque le commutateur inonde un paquet de monodiffusion hors de tous les ports. Le commutateur inonde le paquet car il n'y a pas d'entrée pour l'adresse MAC de destination. Ce comportement n'interrompt pas la connectivité car les paquets sont toujours transférés. Cependant, le comportement ne tient pas compte du flux de paquets supplémentaires sur les ports hôtes. Ce cas étudie le comportement du routage asymétrique et la raison pour laquelle l'inondation de monodiffusion se produit.

Les symptômes du routage asymétrique sont les suivants :

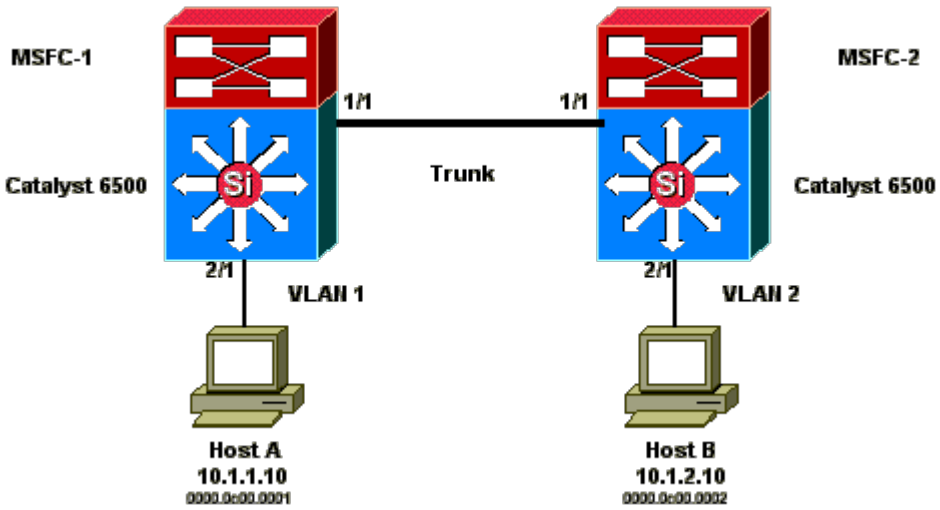
- Diffusion excessive de paquets monodiffusion
- Entrée MLS absente pour les flux
- Trace d'analyseur qui indique que les paquets sur le port hôte ne sont pas destinés à l'hôte
- Latence accrue du réseau grâce aux moteurs de réécriture de paquets de couche 2, tels que les équilibreurs de charge de serveur, les périphériques de cache Web et les appliances réseau

  Cisco LocalDirector et Cisco Cache Engine en sont des exemples.
- Paquets abandonnés sur les hôtes et les stations de travail connectés qui ne peuvent pas gérer la charge de trafic supplémentaire de diffusion de monodiffusion

---

Remarque : La durée de vieillissement du cache ARP par défaut sur un routeur est de quatre heures. Le temps de vieillissement par défaut de l'entrée de mémoire associative (CAM) 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 la durée de vieillissement ARP sur quatre heures.

Ce schéma illustre ce problème. Cet exemple de topologie inclut des Catalyst 6500 avec des cartes MSFC (Multilayer Switch Feature Cards) dans chaque commutateur. Bien que cet exemple utilise des cartes MSFC, vous pouvez utiliser n'importe quel routeur à la place de la carte MSFC. Les exemples de routeurs que vous pouvez utiliser sont le module de commutation de routage (RSM), le routeur de commutation Gigabit (GSR) et le Cisco 7500. Les hôtes sont directement connectés aux ports du commutateur. Les commutateurs sont interconnectés via une agrégation qui achemine le trafic pour VLAN 1 et VLAN 2.



Ces sorties sont des extraits de la sortie de la commande show standby de chaque MSFC.

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 `veille` HSRP. Sur MSFC2, VLAN 2 est à l'état `actif` HSRP et VLAN 1 est à l'état `veille` HSRP. La passerelle par défaut de chaque hôte est l'adresse IP de secours correspondante.

1. Au départ, tous les caches sont vides. L’hôte A utilise MSFC1 comme passerelle par défaut. L’hôte B utilise MSFC2.

   Tables d’adresses ARP et MAC avant le lancement de la commande ping

Table ARP de l’hôte A	Commutateur 1 Tableau d’adresses MAC Port du VLAN MAC	Table ARP MSFC1	Table ARP MSFC2	Commutateur 2 Tableau d’adresses MAC Port du VLAN MAC	Table ARP Hôte B
	0003.6bf1.2a01 1 15/1			0003.6bf1.2a02 1 15/1	
	0003.6bf1.2a01 2 15/1			0003.6bf1.2a02 2 15/1	

	0000.0c07.ac01 1 15/1			0000.0c07.ac01 1/1	
	0000.0c07.ac02 2 1/1			0000.0c07.ac02 2 15/1	
	0003.6bf1.2a02 1 1/1			0003.6bf1.2a01 1/1	
	0003.6bf1.2a02 2 1/1			0003.6bf1.2a01 2 1/1	

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. L'hôte A envoie une requête ping à l'hôte B, ce qui signifie que l'hôte A envoie un paquet d'écho ICMP. Étant donné que chaque hôte réside sur un VLAN distinct, l'hôte A transfère ses paquets destinés à l'hôte B vers sa passerelle par défaut. Pour que ce processus se produise, l'hôte A doit envoyer un protocole 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 a envoyé ARP pour la passerelle par défaut

Table ARP de l'hôte A	Commutateur 1 Tableau d'adresses MAC Port du VLAN MAC	Table ARP MSFC1	Table ARP MSFC2	Commutateur 2 Tableau d'adresses MAC Port du VLAN MAC	Table ARP Hôte B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001			

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 n'a pas encore reçu de paquets dans ce flux. Lorsque MSFC1 reçoit la réponse ARP de l'hôte B, les deux commutateurs apprennent le port source associé à l'hôte B.

   Tables d'adresses ARP et MAC après que l'hôte A a envoyé le paquet à la passerelle par défaut et que MSFC1 a envoyé ARP à l'hôte B

Table ARP de l'hôte A	Commutateur 1 Tableau d'adresses MAC Port du VLAN MAC	Table ARP MSFC1	Table ARP MSFC2	Commutateur 2 Tableau d'adresses MAC Port du VLAN MAC	Table ARP Hôte B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001		0000.0c00.0002 2/1	10.1.2.2 : 0003.6bf1.2a01
	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0002			

4. L'hôte B reçoit le paquet d'écho de l'hôte A, via 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. Pour transférer le paquet, 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 a envoyé ARP pour sa passerelle par défaut

Table ARP de l'hôte A	Commutateur 1 Tableau d'adresses MAC Port du VLAN MAC	Table ARP MSFC1	Table ARP MSFC2	Commutateur 2 Tableau d'adresses MAC Port du VLAN MAC	Table ARP Hôte B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2/1	10.1.2.2 (0003.6bf1.2a01
	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0001			10.1.2.1 (0000.0c07.ac02

5. L'hôte B transfère maintenant le paquet de réponse d'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 réception du paquet d'écho par l'hôte A

Table ARP de l'hôte A	Commutateur 1 Tableau d'adresses MAC Port du VLAN MAC	Table ARP MSFC1	Table ARP MSFC2	Commutateur 2 Tableau d'adresses MAC Port du VLAN MAC	Table ARP Hô B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2/1	10.1.2.2 (0003.6bf1.2a01
10.1.1.3 : 0003.6bf1.2a0	0000.0c00.0002 2 1/1	10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001	0000.0c00.00001 1 1/1	10.1.2.1 (0000.0c07.ac0

6. La réponse d'écho atteint l'hôte A et le flux est terminé.

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. Le seul moment où le commutateur 1 apprend l'adresse MAC source de l'hôte B est lorsque l'hôte B répond à une requête ARP de MSFC1. En effet, l'hôte B utilise MSFC2 comme passerelle par défaut et n'envoie pas de paquets à MSFC1 et, par conséquent, au commutateur 1. Comme le délai d'attente ARP est de quatre heures par défaut, le commutateur 1 vieillit l'adresse MAC de l'hôte B au bout de cinq minutes par défaut. Le commutateur 2 vieillit

l’hôte A après cinq minutes. Par conséquent, le commutateur 1 doit traiter tout paquet dont l’adresse MAC de destination est celle de l’hôte B comme une monodiffusion inconnue. Le commutateur inonde le paquet provenant de l’hôte A et destiné à l’hôte B sur tous les ports. En outre, comme il n’y a pas d’entrée d’adresse MAC hôte B 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 de l’hôte A	Commutateur 1 Tableau d’adresses MAC Port du VLAN MAC	Table ARP MSFC1	Table ARP MSFC2	Commutateur 2 Tableau d’adresses MAC Port du VLAN MAC	Table ARP Hôte B
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2/1	10.1.2.2 : 0003.6bf1.2a01
10.1.1.3 : 0003.6bf1.2a0		10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001		10.1.2.1 : 0000.0c07.ac02

Les paquets de réponse d’écho provenant de l’hôte B rencontrent le même problème après que l’entrée d’adresse MAC de l’hôte A a expiré 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 d’hôte d’entrée A dans la table d’adresses MAC et doit diffuser le paquet sur tous les ports du VLAN 1.

Les problèmes de routage asymétrique n’interrompent pas la connectivité. Cependant, le routage asymétrique peut provoquer une diffusion de monodiffusion excessive et des entrées MLS manquantes. Trois modifications de configuration peuvent remédier à cette situation :

- Réglez la durée de vieillissement MAC sur les commutateurs respectifs sur 14 400 secondes (quatre heures) ou plus.
- Réglez le délai d’attente ARP sur les routeurs sur cinq minutes (300 secondes).
- Modifiez le délai d'expiration MAC et le délai d'expiration ARP sur la même valeur.

La méthode préférable consiste à modifier le temps de vieillissement MAC à 14 400 secondes. Voici les consignes 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 » indique qu'un routeur a reçu un paquet HSRP pour le même groupe avec une adresse IP virtuelle différente. Vérifiez la configuration HSRP incohérente, les fuites inter-VLAN et les boucles de couche 2.

Si vous obtenez ce message d'erreur et qu'il y a une fuite interVLAN 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 existe un routeur sur ce chemin, procédez comme suit :

   1. Dépannez le chemin du premier commutateur au routeur.
   2. Dépannez le chemin entre le routeur et le deuxième commutateur.

2. Connectez-vous à chaque commutateur sur le chemin et vérifiez l'état des ports qui sont utilisés sur le chemin entre les noeuds d'extrémité.

Étude de cas #7 : HSRP provoque une violation MAC sur un port sécurisé

Lorsque la sécurité des ports est configurée sur les ports de commutation qui sont connectés aux routeurs compatibles HSRP, cela provoque une violation MAC, car vous ne pouvez pas avoir la même adresse MAC sécurisée sur plusieurs interfaces. Une violation de la sécurité se produit sur un port sécurisé dans l'une des situations suivantes :

- Le nombre maximal d’adresses MAC sécurisées est ajouté à la table d’adresses et une station dont l’adresse MAC ne figure pas dans la table d’adresses tente d’accéder à l’interface.
- Une adresse apprise ou configurée sur une interface sécurisée est vue sur une autre interface sécurisée du même VLAN.

Par défaut, une violation de sécurité de port entraîne la désactivation des erreurs et l'arrêt immédiat de l'interface du commutateur, ce qui bloque les messages d'état HSRP entre les routeurs.

Solution de contournement

- Exécutez la commande standby use-bia sur les routeurs. Cela force les routeurs à utiliser

une adresse intégrée pour HSRP au lieu de l'adresse MAC virtuelle.

- Désactivez la sécurité des ports sur les ports de commutateur qui se connectent aux routeurs compatibles HSRP.

Étude de cas #8 : %Interface Le Matériel Ne Peut Pas Prendre En Charge Plusieurs Groupes

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

<#root>

%Interface hardware cannot support multiple groups

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

La solution de contournement consiste à utiliser la commande de configuration d'interface standby use-bia, qui utilise l'adresse intégrée (BIA) de l'interface comme adresse MAC virtuelle, au lieu de l'adresse MAC préattribuée.

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 possède une adresse IP unique pour chaque sous-réseau, par interface. Vérifiez également que le protocole de ligne est `activé sur` chaque interface. Afin de vérifier rapidement l'état actuel de chaque interface, émettez la commande show ip interface brief. Voici un exemple :

<#root>

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 et les numéros de groupe de secours configurés correspondent à chaque routeur HSRP participant. Une non-correspondance des groupes de secours ou des adresses de secours HSRP peut causer des problèmes HSRP. La commande show standby détaille la configuration du groupe de secours et de l'adresse IP de secours de chaque interface. Voici un exemple :

<#root>

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 de secours (HSRP) est unique par rapport à l'adresse IP configurée sur chaque interface. La commande show standby est une référence rapide afin d'afficher ces informations. Voici un exemple :

<#root>

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

À moins que HSRP ne soit configuré sur une interface Token Ring, utilisez seulement la commande standby use-bia dans des circonstances spéciales. Cette commande indique au routeur d'utiliser son BIA au lieu de l'adresse MAC HSRP virtuelle pour le groupe HSRP. Sur un réseau Token Ring, si SRB (Source-Route Bridging) est utilisé, la commande standby use-bia permet au nouveau routeur actif de mettre à jour le cache RIF (Routing Information Field) de l'hôte avec un ARP gratuit. Cependant, toutes les implémentations d'hôtes ne gèrent pas correctement le protocole ARP gratuit. Une autre mise en garde pour la commande standby use-bia concerne le proxy ARP. Un routeur de secours ne peut pas couvrir la base de données ARP proxy perdue du 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 HSRP ne filtrent pas les adresses HSRP qui sont configurées sur leurs interfaces. Plus précisément, vérifiez l'adresse de multidiffusion utilisée pour envoyer le trafic à tous les routeurs d'un sous-réseau (224.0.0.2). Vérifiez également que le trafic UDP destiné au port HSRP 1985 n'est pas filtré. HSRP utilise cette adresse et ce port pour envoyer des paquets Hello entre homologues. Émettez la commande show access-lists comme référence rapide pour noter les listes d'accès qui sont configurées sur le routeur. Voici un exemple :

<#root>

```
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 des homologues HSRP communiquent sur une ou plusieurs liaisons trunk, vérifiez que chaque liaison trunk est opérationnelle et transporte le VLAN HSRP. Exécutez la commande show interfaces <interface> trunk sur chaque commutateur applicable et vérifiez les conditions suivantes :

- L’interface fonctionne comme une agrégation IEEE 802.1Q.
- Le VLAN natif est cohérent aux deux extrémités.
- Le VLAN HSRP est autorisé et actif sur l'agrégation.
- Le VTP ou un autre mécanisme d'élagage VLAN ne supprime pas le VLAN HSRP.
- Le protocole STP place l'agrégation dans l'état de transmission pour le VLAN HSRP.
- Le commutateur ne signale pas d'incohérence de type de port, d'encapsulation ou de VLAN natif.

Configurez les deux extrémités avec des paramètres d'agrégation compatibles. Pour une agrégation statique de commutateur à commutateur, configurez le mode d’agrégation explicitement aux deux extrémités. Sur les plates-formes qui prennent en charge le protocole DTP (Dynamic Trunking Protocol), utilisez la négociation de liaison dynamique uniquement lorsque la conception du réseau l’exige. La commande switchport nonegotiate désactive la négociation DTP ; il ne configure pas indépendamment l’interface en tant qu’agrégation.

<#root>

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 G
```

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 Gi
```

2. Vérification de la configuration EtherChannel

Si un port-channel est utilisé afin de connecter les routeurs HSRP, vérifiez la configuration EtherChannel sur les routeurs et les commutateurs. Configurez les deux extrémités d'un EtherChannel avec des modes compatibles. Utilisez desirable avec desirable ou auto pour le protocole PAgP (Port Aggregation Protocol), active avec active ou passive pour le protocole LACP (Link Aggregation Control Protocol), ou on aux deux extrémités pour un EtherChannel statique.

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

<#root>

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 HSRP pour l'adresse MAC virtuelle 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 quelques exemples de résultats :

<#root>

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
```

Assurez-vous de vérifier le temps de vieillissement du CAM afin de déterminer la vitesse à laquelle les entrées sont vieillies. Si le temps est égal à la valeur configurée pour le délai de transmission 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 :

<#root>

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 d'un groupe HSRP deviennent actifs, ces routeurs ne reçoivent pas systématiquement les paquets Hello des homologues HSRP. Les problèmes de couche physique peuvent empêcher le passage cohérent du trafic entre les homologues et provoquer ce scénario. Assurez-vous de vérifier la connectivité physique et la connectivité IP entre les homologues HSRP lorsque vous dépannez HSRP. Émettez la commande show standby afin de vérifier la connectivité. Voici un exemple :

<#root>

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

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

<#root>

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, passez en mode de configuration sur le routeur et émettez la commande no shutdown spécifique à l'interface. Voici un exemple :

<#root>

```
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`, consultez le journal pour les notifications de modification d'interface. Pour les commutateurs basés sur le logiciel Cisco IOS, ces messages apparaissent pour les situations `de liaison active/inactive` :

```
<#root>

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

Router_1#

show logging

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 situés entre les homologues HSRP. Quelqu'un a-t-il supprimé ou desserré des connexions ? Y a-t-il des interfaces qui perdent une liaison à plusieurs reprises ? Les types de câbles appropriés sont-ils utilisés ? Recherchez les erreurs sur les interfaces, comme le montre cet exemple :

```
<#root>

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

Vérifiez les modifications de liaison des ports du commutateur et les autres erreurs. Exécutez ces commandes et consultez le résultat :

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

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

Ces messages sont normaux pour les situations `de liaison active/inactive` :

<#root>

L2Switch_1#

show logging

```
Syslog logging: enabled (0 messages dropped, 5 messages rate-limited, 0 flushes, 0 overruns, xml disabl

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
*Jul 26 17:57:11.716: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsis
*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
*Jul 26 18:02:16.481: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsis
*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
```

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

<#root>

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 n'est `pas connect`, vérifiez que le câble est branché des deux côtés. Vérifiez que le câble approprié est utilisé. Si l'état est `errdisable`, vérifiez les compteurs pour les 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 ? Assurez-vous que l'autre côté de la connexion est configuré pour le même VLAN. Si la liaison est configurée en tant qu'agrégation, assurez-vous

que les deux côtés de l’agrégation transportent les mêmes VLAN.

Quelle est la configuration du débit et du mode bidirectionnel ? Si le paramètre est précédé d'un-, le port est configuré pour négocier automatiquement le débit et le duplex. Dans le cas contraire, l’administrateur réseau a prédéterminé cette configuration. Pour configurer la vitesse et le mode bidirectionnel d’une liaison, les paramètres des deux côtés de la liaison doivent correspondre. Si un port de commutateur est configuré pour la négociation automatique, l'autre côté de la liaison doit également être configuré pour la négociation automatique. Si un côté est codé en dur selon une vitesse et un mode duplex spécifiques, l'autre côté doit également être codé en dur. Si vous laissez une partie négocier automatiquement alors que l'autre est codée en dur, vous interrompez le processus de négociation automatique.

<#root>

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

Existe-t-il de nombreux `Align-Err`, `FCS-Err` ou `Runs` ? Ils peuvent indiquer une incompatibilité de vitesse ou de mode duplex, une défaillance de câblage, une défaillance d’émetteur-récepteur ou un autre problème de couche physique. Modifiez les paramètres de vitesse et de duplex de ce port afin de corriger ces erreurs.

Exécutez la commande show interfaces <interface> counters afin de vérifier que le port transmet 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 le nombre de paquets rejetés ou perdus et si ces paquets font partie du trafic entrant ou sortant. **`Lrn-Discrd`**, **`In-Lost`** et **`Out-Lost`** comptent le nombre de paquets transférés ou abandonnés par erreur en raison de mémoires tampons insuffisantes.

<#root>

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. Cela permet d'exposer toute perte momentanée de connectivité. Une requête ping étendue n’est disponible qu’en mode enable. Voici un exemple de sortie de commande :

<#root>

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
```

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

4. Recherchez la liaison unidirectionnelle

Recherchez des liaisons unidirectionnelles entre les homologues HSRP sur le commutateur. Une liaison unidirectionnelle se produit chaque fois que le trafic transmis par un périphérique local sur une liaison est reçu par le voisin, mais que le trafic transmis par le voisin n'est pas reçu par le périphérique local. Cette fonctionnalité est appelée mode agressif UniDirectional Link Detection (UDLD). L'utilisation d'UDLD n'est possible que si les deux côtés de la connexion prennent en charge la fonction. Le mode UDLD agressif fonctionne au niveau de L2 pour déterminer si une liaison est connectée correctement et si le trafic circule de manière bidirectionnelle entre les voisins droits. Voici des exemples de résultats de commande :

Remarque : Accédez au lien suivant pour Configurer la fonctionnalité de protocole 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 du protocole CDP est un autre moyen de détecter l'existence d'une liaison unidirectionnelle. Si un seul côté d'une liaison peut voir son périphérique voisin, remplacez le câble entre les périphériques et vérifiez les interfaces défectueuses.

<#root>

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

Reportez-vous à ces documents :

- Configurer et vérifier la négociation automatique Ethernet 10/100/1000 Mo duplex intégral/semi-duplex
- Récupérer l'état du port Errdisable sur les plateformes Cisco IOS
- La section Présentation des erreurs de liaison de données de Dépannage des problèmes de compatibilité des commutateurs Catalyst avec les cartes réseau

- Dépannage des problèmes de ports et d’interfaces du 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 quels paquets HSRP sont reçus et envoyés par le routeur. Collectez ces informations si vous créez une demande de service auprès de l'assistance technique Cisco. Le résultat du débogage montre également des informations d'état HSRP, ainsi que des comptes de paquets Hello HSRP détaillés.

1. Débogage HSRP standard

Dans Cisco IOS, activez la fonctionnalité de débogage de HSRP avec la commande debug standby. Ces informations sont utiles lorsque les problèmes sont intermittents et n’affectent que quelques interfaces. Le débogage vous permet de déterminer si le routeur HSRP en question reçoit et transmet des paquets Hello HSRP à des intervalles spécifiques. Si le routeur ne reçoit pas de paquets Hello, vous pouvez en déduire que l'homologue ne transmet pas les paquets Hello ou que le réseau les abandonne.

Commande	Objectif
debug standby	Active le débogage HSRP

Voici un exemple de sortie de commande :

<#root>

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 le filtrage de la sortie de la commande debug standby en fonction de l'interface et du numéro de groupe. La commande utilise le paradigme de condition de débogage qui a été 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 pouvant prendre en charge HSRP. Le groupe peut être n'importe quel groupe, de 0 à 255. Une condition de débogage peut être définie pour les groupes qui n'existent pas. Cela permet de capturer les débogages lors de l'initialisation d'un nouveau groupe. Debug standby doit être activé afin de produire toute sortie de débogage. S'il n'existe aucune condition de débogage de secours, la sortie de débogage est produite pour tous les groupes sur toutes les interfaces. Si au moins une condition de débogage de secours existe, 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 le débogage amélioré de HSRP. Afin d'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 lorsque vous travaillez avec un ingénieur du support technique Cisco si vous créez une demande de service.

Commande	Objectif
debug standby	Affiche toutes les erreurs, événements et paquets HSRP
debug standby errors	Affiche les erreurs HSRP
debug standby events [all] | [hsrp | redondance | piste]] [détail]	Affiche les événements 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 :

<#root>

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 d'interface et/ou de groupe HSRP afin de filtrer cette sortie de débogage.

Commande	Objectif
debug condition interface interface	Active le débogage conditionnel des interfaces
debug condition standby <interface> <group>	Active le débogage conditionnel HSRP

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

<#root>

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

Les conditions de boucle STP ou l'instabilité dans un réseau peuvent empêcher la communication

correcte des homologues HSRP. En raison de cette communication incorrecte, chaque homologue devient un routeur actif. Les boucles STP peuvent provoquer des tempêtes de diffusion, des trames dupliquées et une incohérence de la table MAC. Tous ces problèmes affectent l'ensemble du réseau, et en particulier le protocole HSRP. Les messages d'erreur HSRP peuvent être la première indication d'un problème STP.

Lorsque vous dépannez le protocole 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 en mode de blocage et de transfert. Étant donné que chaque VLAN possède sa propre topologie STP, ces informations sont très importantes sur chaque VLAN.

1. Vérification de la configuration Spanning Tree

Assurez-vous que le protocole STP est configuré sur chaque commutateur et périphérique de pontage du réseau. Notez l’emplacement estimé du pont racine par chaque commutateur. Notez également les valeurs de ces compteurs :

- **Âge max. racine**
- **Heure 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 lorsque vous dépannez des problèmes STP.

Ces trois temporisateurs que vous notez dans la sortie show spanning-tree sont appris à partir du pont racine. Ces minuteurs n'ont pas besoin de correspondre aux minuteurs qui sont définis sur ce pont spécifique. Cependant, assurez-vous que les minuteurs correspondent au pont racine dans le cas où ce commutateur deviendrait le pont racine à tout moment. Cette correspondance entre les minuteurs et le pont racine permet de maintenir la continuité et la facilité d’administration. La correspondance empêche également un commutateur avec des minuteurs 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 le protocole STP dans des réseaux non redondants, vous empêchez une rupture. Une rupture peut se produire si quelqu’un établit un pont entre des commutateurs et des concentrateurs ou d’autres commutateurs et crée accidentellement une boucle physique. Le protocole STP est également très utile pour isoler des problèmes spécifiques. Si l'activation du protocole STP affecte le fonctionnement d'un

---

élément du réseau, il peut y avoir un problème existant que vous devez isoler.

Voici un exemple de sortie de la commande show spanning-tree :

<#root>

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 se produise, il doit y avoir une redondance physique de couche 2 dans le réseau. Une boucle 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 les suivants :

- Indisponibilité totale du réseau
- Perte de connectivité
- Rapport par équipement réseau d'une utilisation élevée des processus et du système

Un VLAN unique qui connaît une condition de boucle STP peut encombrer 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 faisant partie d'une boucle STP. Soupçonnez une boucle STP lorsque le trafic de diffusion ou de multidiffusion augmente fortement au-delà de la ligne de base établie et coïncide avec des trames dupliquées, une instabilité MAC, des modifications de topologie, un encombrement ou une utilisation CPU élevée.

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 dans l'état de blocage STP transmet et reçoit toujours des BPDU STP.

<#root>

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               416501 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 modification de topologie

La commande show spanning-tree detail est une autre commande essentielle au diagnostic des problèmes STP. Cette commande assure le suivi des messages TCN (Topology Change Notification) renvoyés à l'expéditeur. Ces messages, envoyés en tant que BPDU spéciaux entre les commutateurs, indiquent qu'il y a eu une modification de topologie sur un commutateur. Ce commutateur envoie un TCN à son port racine. Le TCN se déplace en amont vers le pont racine. Un pont qui reçoit une trame BPDU TCN la reconnaît en définissant l'indicateur TCA (Topology Change Acknowledgement) dans une trame BPDU de configuration sur le port qui a reçu la trame TCN. Si le pont récepteur n'est pas le pont racine, il envoie également une trame BPDU TCN via son port racine. Lorsque le pont racine reçoit la trame BPDU TCN, il définit l'indicateur TC (Topology Change) dans les trames BPDU de configuration qu'il envoie via le domaine Spanning Tree. Ceci amène tous les ponts non-racine à définir leur compteur d'obsolescence de table d'adresses MAC sur le délai de transfert STP de 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 tard pour voir qui a émis les TCN qui peuvent avoir causé la boucle STP possible. L'entrée **`Number of topology changes`** vous donne une idée du nombre de TCN qui se produisent. Pendant une boucle STP, ce compteur peut s'incrémenter toutes les minutes. Référez-vous à Dépannage des problèmes STP et considérations de conception connexes pour plus d'informations.

Voici d'autres renseignements utiles :

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

Voici un exemple de sortie de commande :

<#root>

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 du 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 STP lorsqu'un port passe à l'état .

Référez-vous à ces documents pour des informations sur le STP et comment dépanner les transitions de liaison qui sont associées aux cartes d'interface réseau (NIC) :

- Utilisation de PortFast et d'autres commandes pour corriger les retards de connectivité de démarrage des stations de travail
- Comprendre le protocole Spanning Tree rapide (802.1w)
- Dépannage des problèmes STP et considérations de conception associées

4. Suppression de diffusion

Activez la suppression de diffusion afin de réduire l'impact 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.



Remarque : Envisagez le contrôle des tempêtes afin de limiter l'impact d'une tempête de diffusion, de multidiffusion ou de monodiffusion inconnue. Définissez des seuils à partir du trafic normal mesuré et validez l'action configurée avant le déploiement.

<#root>

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
```

5. Accès console et Telnet

Le trafic de console ou Telnet vers le commutateur devient souvent trop lent pour suivre correctement un périphérique incriminé pendant une boucle STP. Pendant une fenêtre de maintenance approuvée et avec un accès hors bande disponible, isolez les liaisons redondantes suspectées une par une après avoir vérifié que le chemin restant conserve la connectivité requise. Autorisez STP à reconverger et vérifiez la stabilité avant de restaurer chaque liaison. Si la boucle STP revient après l'ajout d'un segment particulier, vous avez identifié les périphériques en cause.

6. Fonctionnalités Spanning Tree : Portfast, UplinkFast et BackboneFast

Vérifiez que PortFast, UplinkFast et BackboneFast sont configurés correctement. Lorsque vous dépannez des problèmes STP, vérifiez si UplinkFast ou BackboneFast hérités est configuré et si le mode Spanning Tree actif utilise ces fonctionnalités. Modifier la configuration uniquement pendant une fenêtre de maintenance contrôlée après une évaluation de l'impact. En outre, vérifiez que STP PortFast est uniquement activé sur les ports qui sont directement connectés à des hôtes non pontés. Les hôtes non pontés incluent les stations de travail utilisateur et les routeurs sans groupes de pontage. N’activez pas PortFast sur les ports connectés à des concentrateurs ou à d’autres commutateurs. Voici quelques documents pour vous aider à comprendre et à configurer ces fonctions :

Comprendre l'amélioration de la protection BPDU PortFast Spanning Tree

Comprendre et configurer la fonction Cisco UplinkFast

7. Protection BPDU

Lorsque vous activez la protection BPDU PortFast, un port activé PortFast non agrégé passe à 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.

```
<#root>

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
```

8. Élagage VTP

Lorsque l'élagage VTP est activé sur le réseau, les périphériques d'un groupe HSRP peuvent devenir actifs. Cela entraîne des conflits d'adresses IP entre les passerelles et des problèmes de trafic. Assurez-vous que VTP n'élague pas le VLAN d'un groupe HSRP des agrégations requises dans le réseau.

F. Diviser et conquérir

Si toutes les autres tentatives d'isolation ou de résolution de HSRP échouent, la méthode « diviser et conquérir » est la prochaine approche. Cette méthode permet d’isoler le réseau et les composants qui le composent. Diviser et conquérir implique l'une des directives de cette liste :

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

- Créez un VLAN de test pour HSRP et un VLAN isolé pour commuter avec les routeurs HSRP.
- Déconnectez tous les ports redondants.

- Divisez les ports FEC en ports connectés uniques.
- Réduisez les membres du groupe HSRP à seulement deux membres.
- Élaguez les ports trunk de sorte que seuls les VLAN nécessaires se propagent à travers ces ports.
- Déconnectez les commutateurs connectés sur le réseau jusqu'à ce que les problèmes cessent.

Informations connexes

- 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.