Implémentation de HSRP sur LANE

Contenu

Introduction

Le but de ce document est de tracer les grandes lignes des questions qui peuvent être produites en mettant en application le Protocole HSRP (Hot Standby Router Protocol) dans un environnement d'Émulation LAN (LANE). Il décrit plusieurs des particularités du HSRP au-dessus de la RUELLE et fournit des conseils de dépannage pour différents scénarios.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

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

Informations générales

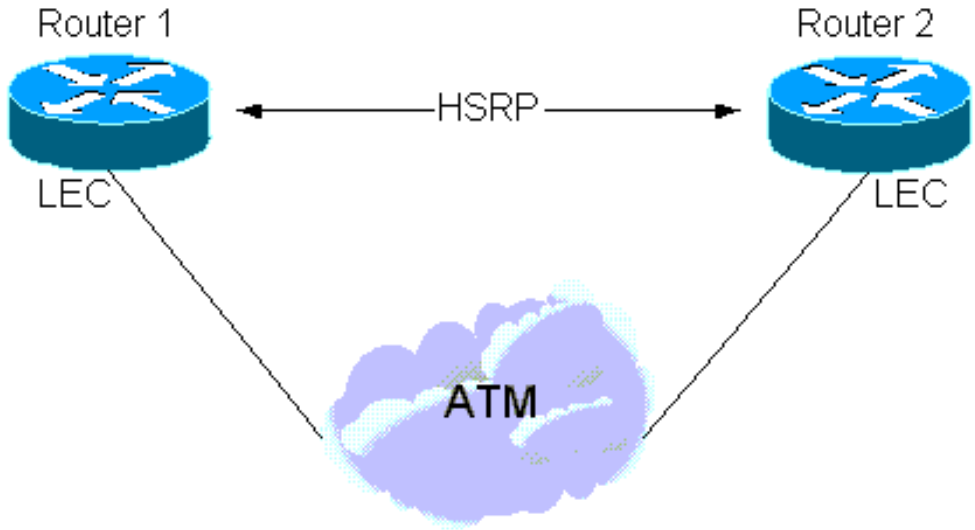
En résumé, le but du HSRP est de permettre à des hôtes dans un sous-réseau pour utiliser un

routeur « virtuel » simple comme passerelle par défaut – les plusieurs routeurs participent au protocole de HSRP afin d'élire le routeur actif, qui assume le rôle de la passerelle par défaut et d'un routeur de sauvegarde au cas où l'actif échouerait. Le résultat est que la passerelle par défaut semblera toujours être même si l'examen médical sautent à cloche-pied d'abord des modifications de routeur. Une description complète de HSRP peut être trouvée dans RFC 2281 .

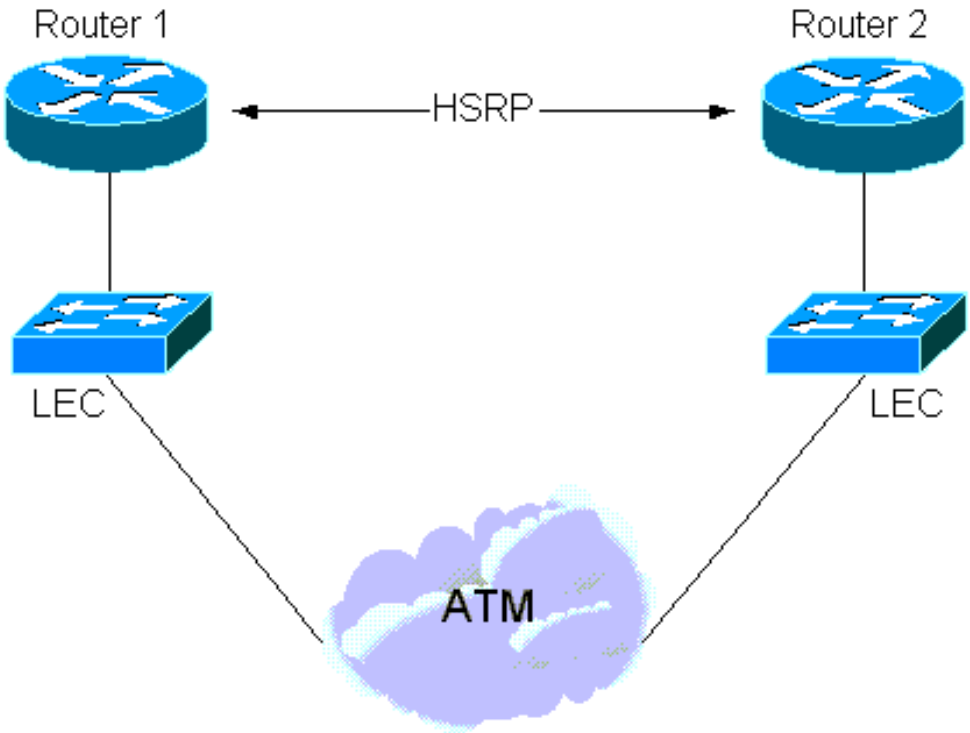
Le HSRP a été conçu pour l'usage au-dessus d'à plusieurs accès, Multidiffusion, ou annoncez les réseaux locaux capables (typiquement Ethernets, Anneau à jeton, ou Fiber Distributed Data Interface [FDDI]). Par conséquent, le HSRP devrait fonctionner bien plus de l'ATM LANE.

Plusieurs situations impliquant l'interaction de HSRP et de RUELLE peuvent surgir :

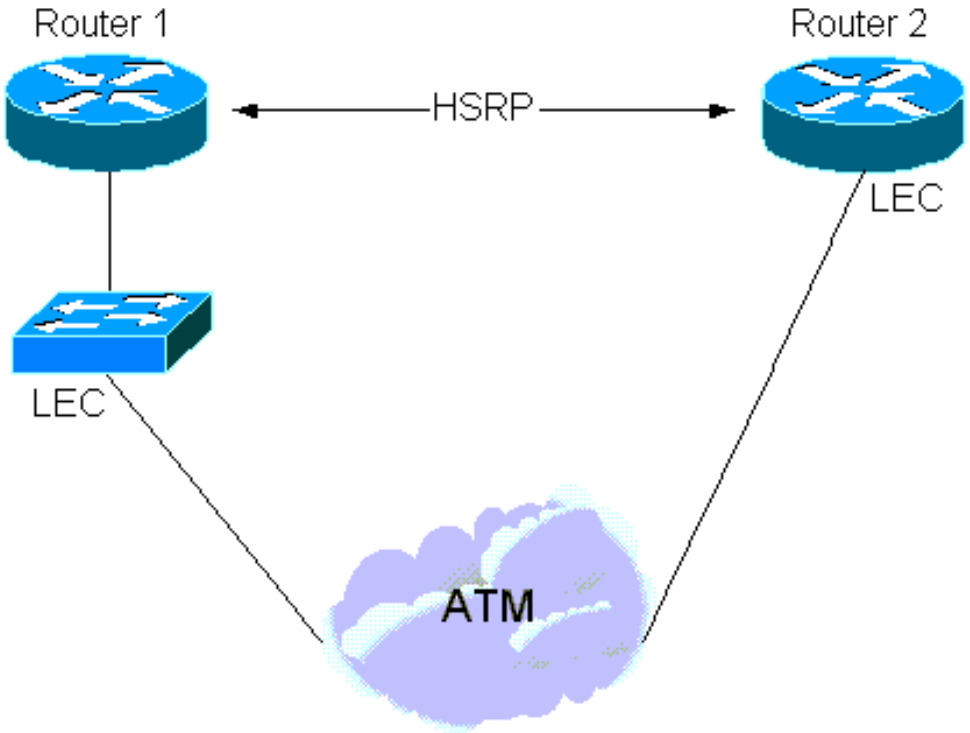
1. Depuis la version de logiciel 11.2 de Cisco IOS®, le HSRP peut fonctionner « à la façon des indigènes » au-dessus de la RUELLE. Dans ce cas, les commandes **de réserve** sont configurées directement sur les sous-interfaces atmosphère où les clients d'émulation LAN (LECs) résident. Voyez l'illustration
   suivante.



2. Il y a également un exemple où le HSRP est configuré sur des interfaces de RÉSEAU LOCAL, mais une partie du sous-réseau répartit une entité LANE. Ceci est accompli par l'intermédiaire d'un commutateur de RÉSEAU LOCAL avec une interface ATM (telle que Cisco Catalyst 5000 avec un module LANE). Voyez l'illustration
   suivante.



3. En conclusion, il y a une situation « hybride » où quelques Routeurs de HSRP Ruelle-sont reliés et d'autres sont sur un RÉSEAU LOCAL derrière un commutateur de RÉSEAU LOCAL.



Études de cas

1) HSRP indigène au-dessus de RUELLE

Les Routeurs participant au HSRP envoient « bonjour » des paquets au-dessus du support de diffusion afin de se renseigner sur l'un l'autre et élire les Routeurs actifs et de réserve. Ces paquets sont envoyés à l'adresse de multidiffusion 224.0.0.2 avec un Time to Live (TTL) de 1 et une adresse MAC de destination de Multidiffusion de 0100 5E00 0002.

La RUELLE n'introduit aucune nouvelle question ici ainsi les détails décrits dans RFC 2281 s'appliquent toujours – par l'échange de bonjour, le coup, et démissionnent des paquets, l'actif et des Routeurs de réserve sont élus.

Bonjour les paquets sont envoyés au-dessus du serveur de diffusion et inconnu (BUS) et ce qui suit est ce qui un **paquet atmosphère de débogage** (sur le circuit virtuel en avant de Multidiffusion [circuit virtuel]) et un **debug standby** indiquerait :

```
Medina#show run [snip]interface ATM3/0.1 multipoint ip address 1.1.1.3 255.255.255.0 no ip
redirects no ip directed-broadcast lane client ethernet HSRP standby 1 ip 1.1.1.1 [snip]
Medina#show lane client LE Client ATM3/0.1 ELAN name: HSRP Admin: up State: operational Client
ID: 2 LEC up for 14 minutes 34 seconds ELAN ID: 0 Join Attempt: 7 Last Fail Reason: Config VC
being released HW Address: 0050.a219.5c54 Type: ethernet Max Frame Size: 1516 ATM Address:
47.00918100000000604799FD01.0050A2195C54.01 VCD rxFrames txFrames Type ATM Address 0 0 0
configure 47.00918100000000604799FD01.00604799FD05.00 12 1 3 direct
47.00918100000000604799FD01.00604799FD03.01 13 2 0 distribute
47.00918100000000604799FD01.00604799FD03.01 14 0 439 send
47.00918100000000604799FD01.00604799FD04.01 15 453 0 forward
47.00918100000000604799FD01.00604799FD04.01 Medina#show atm vc 15 ATM3/0.1: VCD: 15, VPI: 0, VCI:
40 UBR, PeakRate: 149760 LANE-LEC, etype:0xE, Flags: 0x16C7, VCmode: 0x0 OAM frequency: 0
second(s) InARP DISABLED Transmit priority 4 InPkts: 601, OutPkts: 0, InBytes: 48212, OutBytes:
0 InPRoc: 0, OutPRoc: 0, Broadcasts: 0 InFast: 0, OutFast: 0, InAS: 0, OutAS: 0 InPktDrops: 0,
OutPktDrops: 0 CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0 OAM cells received: 0 OAM cells
sent: 0 Status: UP TTL: 0 interface = ATM3/0.1, call remotely initiated, call reference =
8388610 vcnum = 15, vpi = 0, vci = 46, state = Active(U10) , multipoint call Retry count:
Current = 0 timer currently inactive, timer value = 00:00:00 Root Atm Nsap address:
47.00918100000000604799FD01.00604799FD04.01 , VC owner: ATM_OWNER_UNKNOWN
```

D'importance le regarde ce que le client d'émulation LAN (LEC) reçoit au-dessus du BUS (par exemple, par la Multidiffusion en avant) :

```
Medina#debug atm packet interface atm 3/0.1 vcd 15 ATM packets debugging is on Displaying
packets on interface ATM3/0.2 VPI 0, VCI 46 only Medina#debug standby Hot standby protocol
debugging is on *Feb 18 06:36:05.443: SB1:ATM3/0.1 Hello in 1.1.1.2 Active pri 110 hel 3 hol 10
ip 1.1.1.1 *Feb 18 06:36:08.007: SB1:ATM3/0.1 Hello out 1.1.1.3 Standby pri 100 hel 3 hol 10 ip
1.1.1.1 *Feb 18 06:36:08.439: ATM3/0.1(I): VCD:0xF VPI:0x0 VCI:0x40 Type:0xE, LANE, ETYPE:0x000E
LECID:0x0004 Length:0x4A *Feb 18 06:36:08.439: 0004 0100 5E00 0002 0000 0C07 AC01 0800 45C0 0030
0000 0000 0111 D6F8 0101 *Feb 18 06:36:08.443: 0102 E000 0002 07C1 07C1 001C AAEE 0000 1003 0A6E
0100 6369 7363 6F00 0000 *Feb 18 06:36:08.443: 0101 0101 0001 0001 000C
```

Ce vidage hexadécimal se traduit à ce qui suit :

```
VCD:0xF VPI:0x0 VCI:0x28: VCD number 15, VPI=0 and VCI=400
004: LECID from the sender of the packet
0100 5E00 0002: Destination MAC address for HSRP hellos
0000 0C07 AC01: Virtual MAC address of HSRP (the last octet is actually the standby group
number) 0800: Type = IP 45C0 0030 0000 0000 0111 D6F8: IP header - UDP packet 0101 0102: Source
IP = 1.1.1.2 E000 0002: Destination IP = 224.0.0.2 07C1 07C1 001C AAEE: UDP header - Source &
Destination ports = 1985 00: HSRP version 0 00: Hello packet (type 0) 10: State (of the sender)
is Active (16) 03: Hellotime (3 sec) 0A: Holdtime (10 sec) 6E: Priority = 110 01: Group 00:
Reserved 6369 7363 6F00 0000: Authentication Data 0101 0101: Virtual IP address = 1.1.1.1
```

Ce qui est remarquable est que bonjour les paquets sont originaires par le routeur actif avec l'adresse MAC virtuelle (VMAC) comme adresse MAC source – c'est desirable parce que les ponts auto-adaptatifs (Commutateurs) qui expédient ces paquets mettront à jour leur table de mémoire de contenu adressable (CAM) avec la localisation adaptée du VMAC.

La clé au HSRP se trouve en dessous du mappage entre une adresse IP et une adresse MAC.

Dans l'expression la plus simple, l'adresse IP virtuelle est de manière permanente liée à une adresse MAC virtuelle et le seul aspect à s'inquiéter pour est que les Commutateurs savent

toujours où cette adresse MAC virtuelle se trouve. Ceci est assuré parce que les hellos sont originaires par le VMAC.

```
Medina#show standby ATM3/0.1 - Group 1 Local state is Standby, priority 100 Hellotime 3 holdtime
10 Next hello sent in 00:00:00.006 Hot standby IP address is 1.1.1.1 configured Active router is
1.1.1.2 expires in 00:00:08 Standby router is local Standby virtual mac address is
0000.0c07.ac01
```

Une autre option est que les Routeurs utilisent le leur graver-dans des adresses (de **standby use-bia**) tracées à l'adresse IP virtuelle. Dans ce cas, le mappage entre l'IP virtuel et l'adresse MAC change au fil du temps – nouvellement le routeur actif envoie un Protocole ARP (Address Resolution Protocol) afin d'annoncer la nouvelle reproduction d'adresses virtuelle d'IP-à-MAC. Un ARP est simplement une réponse non sollicitée d'ARP. -

Remarque: Certaines piles (plus anciennes) IP peuvent ne pas comprendre des ARPs.

```
Medina#show standby ATM3/0.1 - Group 1 Local state is Standby, priority 100, use bia Hellotime 3
holdtime 10 Next hello sent in 00:00:02.130 Hot standby IP address is 1.1.1.1 configured Active
router is 1.1.1.2 expires in 00:00:09 Standby router is local Standby virtual mac address is
0050.a219.5c54
```

Remarque: Pour introduire la RUELLE, la clé est celle sur la reproduction d'adresses virtuelle d'IP-à-MAC, là doit expliquer la reproduction d'adresses (NSAP) VMAC à Réseau Service Access point. Ce mappage est simplement résolu par le processus de Resolution Protocol d'Émulation-adresse de RÉSEAU LOCAL (LE-ARP) : un LEC souhaitant envoyer le trafic à la passerelle active utilisera LE-ARP pour le VMAC (ou le MAC physique si utilisation graver-dans adresse MAC [BIA]).

Considérez maintenant ce qui se produit quand un nouveau routeur devient actif : pour que le LECs soit informé du nouveau emplacement de la passerelle active (nouveau VMAC--NSAP au mappage), la table LE-ARP doit être modifiée. Par défaut, les entrées LE-ARP chronomètrent toutes les cinq minutes mais, dans la plupart des cas, compter sur ce délai d'attente est inacceptable – la convergence doit être plus rapide. La solution dépend de si le LEC assumant le nouvel état active est la version LANE courante 1 ou la version 2 (voir l'atmosphère Forum.com pour les spécifications LANE) :

- **Version LANE 1**Quand un routeur devient actif, en plus des étapes décrites dans RFC 2281 , il envoie un LE-NARP afin de faire le nouveau VMAC--NSAP à la liaison d'adresse connue. Selon les spécifications LANE, à la réception d'un LE-NARP, un LEC peut choisir d'effacer ou mettre à jour l'entrée LE-ARP correspondant à l'adresse MAC. La tendance au sein de Cisco est d'adopter plus d'approche prudente et de choisir d'effacer l'entrée LE-ARP – ceci entraînera le LEC immédiatement au re-LE-ARP sans devoir attendre le délai d'attente de cinq-minute.**Remarque:** Cette solution peut entraîner le problème de compatibilité décrit ci-dessous.
- **Version LANE 2**Dans la version LANE 2, certains défauts de la version LANE 1 ont été allégés : le LE-NARP a été remplacé par le LE-ARP targetless et la NO--source LE-NARP. Le LE-ARP targetless peut être vu comme véhicule pour annoncer de nouvelles attaches tandis que le but de la NO--source le LE-NARP est de rendre Désuet(e) exister MAC--NSAP à la liaison d'adresse. La manière que ceci est mis en application est que si un routeur change du standby en l'Active, elle envoie un LE-ARP targetless (ceci est utilisée pour annoncer a MAC--NSAP au mappage) et s'il change de l'Active en le standby, c'envoie une NO--source LE-NARP (ceci est utilisée pour rendre a MAC--NSAP à lier Désuet(e)).

Problème - Interopérabilité

Il y a un problème qui surgit assez souvent pour mériter un examen plus en profondeur. Les caractéristiques de la version LANE 1 déclarent que le LE-NARP doit spécifier la « vieille attache, » qui est rendu Désuet(e) en spécifiant (la vieille) adresse de la cible NSAP (T-NSAP). Typiquement, les Routeurs participant au HSRP ne mettent pas à jour des accès directs aux données entre l'un l'autre.

Par conséquent, nouvellement le routeur actif ne sait pas que les ces informations et elles choisiront de ne pas se terminer ce champ puisqu'elles ne savent pas mieux. C'est une violation douce des caractéristiques et quelques constructeurs ignoreront ces paquets si la zone adresse T-NSAP est tous les zéros. Malheureusement, il n'y a aucun contournement pour ceci – si le LE-NARP est ignoré, comptez sur le délai d'attente LE-ARP (en général cinq minutes) avant que l'attache correcte soit apprise.

Quand un LE-ARP ou un LE-NARP est envoyé avec une zone adresse T-NSAP de tous les zéros, elle s'appelle « targetless. » Comme vu ci-dessus, avec l'arrivée de la version LANE 2 (et atmosphère finie multiprotocole [MPOA]), ceci a la norme devenue et le problème cesse d'exister.

C'est ce qui est fait dans la version LANE 1 où les problèmes peuvent surgir :

- Si le routeur connaît la « vieille attache, » elle pourrait aussi bien obéir les caractéristiques. Ceux-ci met au point sont maintenant pris sur le contrôle distribuent le circuit virtuel

```
:ATM0/0.1(I):
VCD:0xD Type:0x6, LANE, ETYPE:0x0006 LECID:0xFF00 Length:0x70
FF00 0101 0008 0000 0000 0018 0003 0000 0000 0000 0000 0000 0001 0000 0C07
AC01 4700 9181 0000 0000 101F 2D68 0100 50A2 195C 5401 0000 0000 4700 9181
0000 0000 101F 2D68 0100 102F FBA4 0101 0000 0000 0000 0000 0000 0000 0000
FF00: Marker = Control Frame
0101: ATM LANE version 10
008: Op-code = LE_NARP_REQUEST
0000: Status
0000 0018: Transaction ID0003: Requester LECID0000: Flags
0000 0000 0000 0000: Source LAN destination
(not used for an LE-NARP)
0001 0000 0C07 AC01: Target LAN destination
(the 0001 indicates a MAC address as opposed to a route descriptor)
4700 9181 0000 0000 101F 2D68 0100 50A2 195C 5401: Source NSAP address
(new NSAP address to be bound)
0000 0000: Reserved
4700 9181 0000 0000 101F 2D68 0100 102F FBA4 0101: Target NSAP address
(old NSAP address to be rendered obsolete)
```

- S'il ne connaît pas la « vieille attache, » il fait son meilleur et annonce au moins le neuf

```
:ATM0/0.1(I):
VCD:0xD Type:0x6, LANE, ETYPE:0x0006 LECID:0xFF00 Length:0x70
FF00 0101 0008 0000 0000 0014 0003 0000 0000 0000 0000 0000 0001 0000 0C07
AC01 4700 9181 0000 0000 101F 2D68 0100 50A2 195C 5401 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

Remarque: Cette fois l'adresse T-NSAP est vide.

De nouveau, le comportement est complètement dans les caractéristiques en utilisant des clients de la version LANE 2.

Remarque: Le logiciel qui prend en charge MPOA également prend en charge la version LANE 2.

Conseils de dépannage

Le HSRP indigène au-dessus de la RUELLE ne devrait pas engendrer trop de problèmes autres

que le problème d'interopérabilité potentiel dû au LE-NARP exempt du T-NSAP.

Si les Routeurs ont la difficulté en établissant s'ils sont en activité ou de réserve, utilisez la commande de **debug standby** de voir si les hellos sont vus des deux côtés. Sinon, alors le BUS n'expédie pas probablement correctement les paquets.

2) HSRP au-dessus des Routeurs derrière la RUELLE

La situation devient plus compliquée quand le HSRP est configuré sur des interfaces de RUELLE des Routeurs situés derrière une entité LANE, comme illustré dans la figure 2.

Remarque: Cette figure dépeint logiquement le fait que le routeur est non-atmosphère reliée. Il ne doit pas nécessairement être dans un périphérique distinct au commutateur de RÉSEAU LOCAL (un module de route switch [RSM] dans Cisco Catalyst 5000 tombe sous ce cas).

De nouveau, la difficulté surgit en raison du mappage de MAC-adresse-à-NSAP-adresse imposé par la RUELLE. Comme remarquable ci-dessus, quand le VMAC commute à un périphérique (quand un nouveau routeur devient actif) qui correspond à une autre adresse NSAP, tous les périphériques reliés à l'entité LANE doivent être au courant. Ceci est assez facilement mis en application dans un HSRP indigène au-dessus d'environnement LANE à l'aide du LE-NARP (ou de LE-ARP targetless).

Le problème dans ce deuxième cas est que le LECs ne se rendent pas compte d'aucune informations de la couche 3 (IP), ils sont seulement conçus pour jeter un pont sur des paquets entre deux supports différents (le RÉSEAU LOCAL et l'atmosphère).

Par exemple, dans la figure 2, si le Router2 devenait soudainement actif, puis il serait desirable que le commutateur 2 réseau local informe tous les périphériques connectés au nuage atmosphère (RUELLE) au sujet du nouveau VMAC--NSAP à la cartographie. Le LEC dans le commutateur 2 de RÉSEAU LOCAL est dit proxying pour toutes les adresses MAC qui sont derrière lui. Les périphériques à travers la RUELLE souhaitant envoyer le trafic à ces adresses MAC doivent faire ainsi par un accès direct aux données installé vers ce LEC. Intuitivement, on pourrait penser que ce ne sera pas un grand problème puisque, dès que le Router2 assumera l'état active, il commencera des hellos d'approvisionnement avec le VMAC comme adresse MAC source. Ces informations seraient alors apprises par tous les Commutateurs de RÉSEAU LOCAL et tout convergerait rapidement. C'est vrai dans des environnements de non-RUELLE, mais la RUELLE est spéciale pour la raison suivante :

Dans la RUELLE, un paquet de données peut habituellement être transmis par deux chemins :

- L'accès direct aux données si ce paquet est un unicast pour lequel la destination a été tracée à un NSAP connu et si l'accès direct aux données a été déjà établi.
- Le BUS pour les unicasts et les Multidiffusions inconnus.

Par conséquent, une même adresse MAC les paquets de source qui seront reçus par un commutateur de RÉSEAU LOCAL plus de deux différents chemins. Les Multidiffusions et les unicasts inconnus arriveront par le BUS tandis que les unicasts connus arrivent par des accès directs aux données. Si aucun effort particulier n'avait été fait, un commutateur de RÉSEAU LOCAL continuerait à apprendre cette adresse MAC au-dessus d'un accès direct aux données ou au-dessus du BUS selon le dernier paquet reçu. C'est indésirable parce que le BUS devrait seulement être utilisé pour envoyer des paquets pour les unicasts ou les Multidiffusions inconnus. À ce stade, rien n'est appris au-dessus du BUS, mais en réalité, choisissez de faire ce qui suit :

Packets received over the BUS are marked with the Conditional Learn (CL) bit set to 1(this bit is in a control overhead specific to Cisco LAN switches). The LAN switch will only update its CAM table with this entry if it does not already have an entry for this MAC address (in this VLAN). The idea is that if a switch receives a packet from a source that it does not know about, at least it will now know that it is located somewhere across the LANE cloud. Future packets for that MAC address will be forwarded to the BUS only as opposed to being flooded in the entire VLAN.

Pour retourner à l'exemple, il est sûr de supposer que tout le LECs dans cet ELAN se rendent déjà compte du mappage VMAC-NSAP pour le routeur 1 avant quand le Router2 devient actif. Tous les Commutateurs de RÉSEAU LOCAL savent également que le VMAC est derrière le commutateur 1. de RÉSEAU LOCAL. Quand le Router2 devient Active et sources bonjour les paquets, ceux-ci sont expédiés à l'entité LANE au-dessus du BUS. Par conséquent, aucun des Commutateurs de RÉSEAU LOCAL ne mettra à jour leurs tables de CAM avec ces nouvelles informations et tous les paquets envoyés à ce VMAC seront mal dirigés jusqu'à ce que les Commutateurs de RÉSEAU LOCAL « oublient » cette entrée (le vieillissement par défaut étant de cinq minutes).

Remarque: La Connectivité globale pourrait être perdue réellement pendant jusqu'à 10 minutes puisque le temporisateur d'obsolescence LE-ARP sur le LECs sont également de cinq minutes par défaut. La réduction du temporisateur d'obsolescence pour des adresses MAC aidera, mais ne résout pas réellement le problème.

Il y a deux solutions pour ceci :

1. Si les Commutateurs de RÉSEAU LOCAL sont non-Cisco, retournez à une méthode décrite ci-dessus : utilisant l'adresse fixe. Si les Routeurs utilisent seulement leur adresse MAC à la source bonjour les paquets et cela l'adresse virtuel-IP change le mappage toutes les fois qu'un commuté se produit, il n'y a aucune confusion possible quant à où ces adresses MAC se trouvent.
2. Si les Commutateurs de RÉSEAU LOCAL sont des Catalyst de Cisco, alors continuez à utiliser le VMAC dû aux modifications fournies par le système de recherche réparti de défaut (DDTS) couvert dans les id de bogue Cisco CSCdj58719 (clients enregistrés seulement) et CSCdj60431 (clients enregistrés seulement).Essentiellement, quand un routeur assume l'état active, en plus de l'ARP (réponse non sollicitée d'ARP) ce il envoie selon RFC 2281 , le routeur envoie un deuxième ARP avec une adresse MAC de destination de 0100.0CCD.CDCD. Quand Cisco Catalyst reçoit ce paquet il fait deux choses :Il efface l'entrée LE-ARP qu'il a pour le VMAC.Il apprend le VMAC au-dessus du BUS.

Pour cette raison, il n'y ont plus d'entrées éventées LE-ARP dans le divers LECs et le nouveau emplacement du VMAC est propagé à tous les Commutateurs (par exemple, au delà de l'entité LANE). Pour que ceci fonctionne correctement, les configurations logicielles requises minimales suivantes doivent être répondues :

- Les Routeurs doivent avoir au moins le Logiciel Cisco IOS version 11.1(24), la version 11.2(13), ou toute la version 12.0.
- Les modules LANE doivent avoir au moins la version 3.2(8). les versions 11.3W4 et sont plus tard acceptables.

Cisco recommande utilisant le dernier logiciel.

3) Environnement mixte

Il y a une question finale qui peut surgir dans les environnements mixtes. Prenant le scénario ci-

dessus et ajoutant un fin-périphérique directement connecté de RUELLE (routeur ou poste de travail), le fin-périphérique doit être informé au sujet d'une modification de l'emplacement de la passerelle active la même manière que dans le scénario 1. Si nouvellement le routeur actif est connecté derrière un commutateur, la seule solution est pour le commutateur lui-même pour envoyer le LE-NARP au nom du routeur et est exactement ce ce qui à faire.

En plus des étapes décrites ci-dessus, si Cisco Catalyst prend un paquet destiné à 0100 0CCD CDCD, il envoie un LE-NARP (NO--source LE-NARP si exécutant version LANE 2), qui son objectif unique est d'effacer les caches LE-ARP pour le VMAC.

Conclusion

Comme expliqué, le HSRP au-dessus de la RUELLE fonctionne bien en principe mais, sous certaines circonstances, les utilisateurs peuvent perdre des périodes de Connectivité pour faire court si tombant dans une des échappatoires décrites ci-dessus.

Important ! : Afin d'assurer le succès avec le HSRP au-dessus de la RUELLE, suivez au moins ces deux recommandations :

- Pour être sûr, améliorez au moins à la dernière version du logiciel Cisco IOS 12.0.
- Dans des environnements de mult-constructeur, il est le meilleur d'employer la version LANE 2 ou l'adresse fixe afin d'éviter des problèmes.

Informations connexes

- Pages de support technologique atmosphère
- Support technique - Cisco Systems