Implémentation de HSRP sur LANE

Contenu

Introduction

L'objectif de ce document est de décrire les problèmes qui peuvent se poser lors de la mise en oeuvre du protocole HSRP (Hot Standby Router Protocol) dans un environnement d'émulation de réseau local (LANE). Il décrit de nombreuses caractéristiques de HSRP sur LANE et fournit des conseils de dépannage pour différents scénarios.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

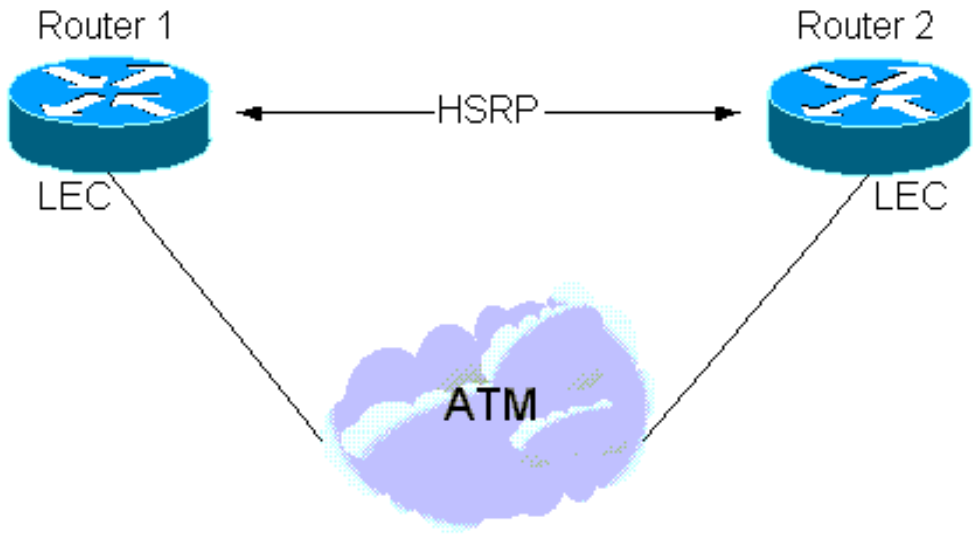
En résumé, l'objectif de HSRP est de permettre aux hôtes d'un sous-réseau d'utiliser un seul

routeur « virtuel » comme passerelle par défaut : les routeurs multiples participent au protocole HSRP afin de sélectionner le routeur actif, qui assume le rôle de passerelle par défaut et de routeur de secours en cas de défaillance du routeur actif. Il en résulte que la passerelle par défaut apparaît toujours active même si le routeur physique du premier saut change. Une description complète de HSRP est disponible dans RFC 2281 .

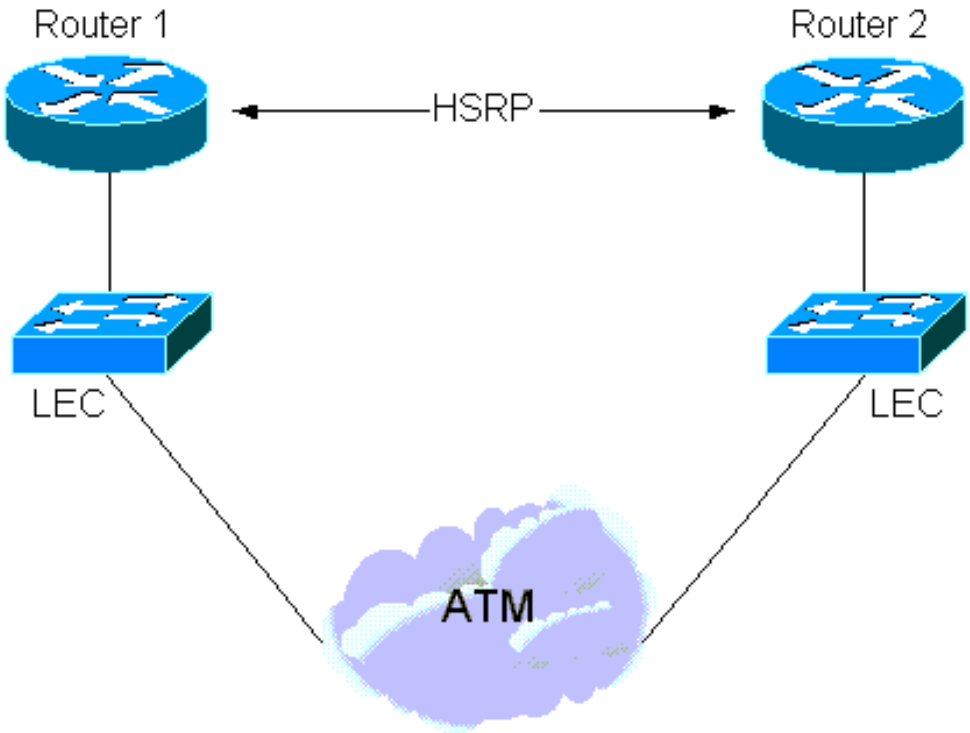
Le protocole HSRP a été conçu pour être utilisé sur des réseaux locaux à accès multiple, multidiffusion ou de diffusion (généralement Ethernet, Token Ring ou FDDI). Par conséquent, HSRP doit fonctionner correctement sur ATM LANE.

Plusieurs situations impliquant une interaction HSRP et LANE peuvent survenir :

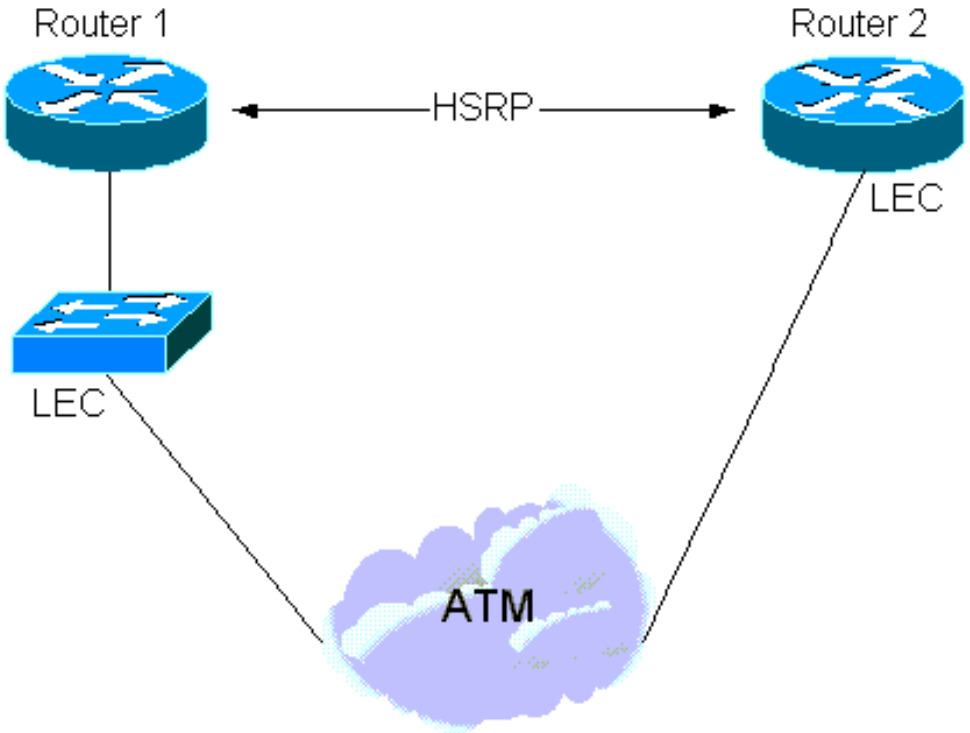
1. Depuis la version 11.2 du logiciel Cisco IOS®, HSRP peut exécuter « nativement » sur LANE . Dans ce cas, les commandes **standby** sont configurées directement sur les sous-interfaces ATM où résident les LEC (LAN Emulation Clients). Reportez-vous à l'illustration suivante.



2. Il existe également une instance où HSRP est configuré sur les interfaces LAN, mais une partie du sous-réseau couvre un nuage LANE. Pour ce faire, vous devez utiliser l'intermédiaire d'un commutateur LAN avec une interface ATM (par exemple, un commutateur Cisco Catalyst 5000 avec un module LANE). Reportez-vous à l'illustration suivante.



3. Enfin, il y a une situation « hybride » où certains routeurs HSRP sont connectés à un LAN et d'autres se trouvent sur un LAN derrière un commutateur
   LAN.



Études de cas

1) HSRP natif sur LANE

Les routeurs participant au protocole HSRP envoient des paquets « hello » sur le support de diffusion afin d'apprendre les uns des autres et de sélectionner les routeurs actifs et de secours. Ces paquets sont envoyés à l'adresse de multidiffusion 224.0.0.2 avec une durée de vie (TTL) de 1 et une adresse MAC de destination de multidiffusion de 0100 5E00 0002.

LANE n'introduit aucun nouveau problème ici, donc les détails décrits dans RFC 2281 s'appliquent toujours - par l'échange de paquets Hello, coup d'état et de démission, les routeurs actifs et de secours sont élus.

Les paquets Hello sont envoyés sur le serveur de diffusion et d'inconnu (BUS) et voici ce qu'un **paquet debug atm** (sur le circuit virtuel Multicast Forward [VC]) et un **débogage standby** révéleraient :

```
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: 47.009181000000000604799FD01.0050A2195C54.01
VCD  rxFrames  txFrames  Type      ATM Address
  0        0         0  configure  47.009181000000000604799FD01.00604799FD05.00
 12        1         3  direct     47.009181000000000604799FD01.00604799FD03.01
 13        2         0  distribute 47.009181000000000604799FD01.00604799FD03.01
 14        0       439  send       47.009181000000000604799FD01.00604799FD04.01
 15      453         0  forward    47.009181000000000604799FD01.00604799FD04.01

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: 47.009181000000000604799FD01.00604799FD04.01
, VC owner: ATM_OWNER_UNKNOWN
```

Il est important d'examiner ce que le client d'émulation de réseau local (LEC) reçoit sur le BUS

(par exemple, par le biais de la multidiffusion vers l'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 par 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, c'est que les paquets HELLO sont fournis par le routeur actif avec l'adresse MAC virtuelle (VMAC) comme adresse MAC source. C'est souhaitable car les ponts d'apprentissage (commutateurs) qui transmettent ces paquets mettront à jour leur table CAM avec l'emplacement approprié du VMAC.

La clé de HSRP réside dans le mappage entre une adresse IP et une adresse MAC.

Dans l'expression la plus simple, l'adresse IP virtuelle est liée de manière permanente à une adresse MAC virtuelle et le seul aspect qui vous préoccupe est que les commutateurs savent toujours où se trouve cette adresse MAC virtuelle. Ceci est garanti car les HELLO sont fournis 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 leurs adresses brûlées (**standby use-bia**) mappées à l'adresse IP virtuelle. Dans ce cas, le mappage entre l'adresse IP virtuelle et l'adresse MAC change au fil du temps. Le routeur nouvellement actif envoie un protocole ARP (Address Resolution Protocol) afin d'annoncer le nouveau mappage d'adresse IP virtuelle vers MAC. Un ARP est simplement une réponse ARP non sollicitée.-

Remarque : certaines piles IP (plus anciennes) peuvent ne pas comprendre les ARP.

```
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 le LANE, la clé est qu'en plus du mappage d'adresses IP à MAC virtuelles, il doit y avoir une comptabilité pour le mappage d'adresses NSAP (VMAC-to-Network-Service-Access Point). Ce mappage est simplement résolu par le processus LE-ARP (Emulation-Address Resolution Protocol) LAN : une LEC souhaitant envoyer le trafic à la passerelle active utilisera LE-ARP pour la VMAC (ou MAC physique si elle utilise l'adresse MAC intégrée [BIA]).

Maintenant, réfléchissez à ce qui se passe lorsqu'un nouveau routeur devient actif : pour que les LEC soient informés du nouvel emplacement de la passerelle active (nouveau mappage VMAC-NSAP), la table LE-ARP doit être modifiée. Par défaut, les entrées LE-ARP expirent toutes les cinq minutes mais, dans la plupart des cas, compter sur ce délai est inacceptable - la convergence doit être plus rapide. La solution dépend du fait que le LEC supposant le nouveau statut actif exécute LANE version 1 ou version 2 (voir ATM Forum.com pour les spécifications LANE) :

- **LANE version 1**Lorsqu'un routeur devient actif, en plus des étapes décrites dans la RFC 2281 , il envoie un LE-NARP afin de faire connaître la nouvelle liaison d'adresse VMAC à NSAP. Selon les spécifications LANE, à la réception d'un LE-NARP, une ESL peut choisir d'effacer ou de mettre à jour l'entrée LE-ARP correspondant à l'adresse MAC. La tendance de Cisco est d'adopter une approche plus prudente et de choisir de supprimer l'entrée LE-ARP. Cela entraînera la réactivation immédiate du protocole LE-ARP par le LEC sans avoir à attendre le délai de cinq minutes.**Remarque :** Cette solution peut provoquer le problème de compatibilité décrit ci-dessous.
- **LANE version 2**Dans LANE version 2, certaines lacunes de LANE version 1 ont été atténuées : le LE-NARP a été remplacé par le LE-ARP sans cible et le LE-NARP sans source. Le protocole LE-ARP sans cible peut être considéré comme un moyen d'annoncer de nouvelles liaisons, tandis que le protocole LE-NARP sans source a pour objectif de rendre obsolète une liaison d'adresse MAC à NSAP existante. La mise en oeuvre de cette méthode consiste à ce que si un routeur passe de Standby à Active, il envoie un LE-ARP sans cible (utilisé pour annoncer un mappage MAC-NSAP) et s'il passe d'Active à Standby, il envoie un LE-NARP

sans source (utilisé pour rendre obsolète une liaison MAC-NSAP).

Problème - Interopérabilité

Il y a un problème qui se pose assez souvent pour mériter un examen plus approfondi. Les spécifications LANE version 1 indiquent que le LE-NARP doit spécifier l'ancienne liaison, rendue obsolète en spécifiant l'adresse (ancienne) du NSAP cible (T-NSAP). En règle générale, les routeurs participant au protocole HSRP ne gèrent pas les directions de données entre eux.

Par conséquent, le nouveau routeur actif ne connaît pas ces informations et il choisira de ne pas remplir ce champ car il ne sait pas mieux. Il s'agit d'une légère violation des spécifications et certains fournisseurs ignoreront ces paquets si le champ d'adresse T-NSAP est uniquement composé de zéro. Malheureusement, il n'y a aucune solution de contournement pour cela-si le LE-NARP est ignoré, comptez sur le délai d'attente LE-ARP (généralement cinq minutes) avant d'apprendre la liaison correcte.

Lorsqu'un LE-ARP ou LE-NARP est envoyé avec un champ d'adresse T-NSAP de tous les zéros, il est appelé « sans cible ». Comme nous l'avons vu plus haut, avec l'avènement de la version 2 de LANE (et du protocole multiprotocole sur ATM [MPOA]), cela est devenu une norme et le problème cesse d'exister.

Voici ce qui se passe dans LANE version 1 où des problèmes peuvent survenir :

- Si le routeur connaît l'ancienne liaison, il peut tout aussi bien respecter les spécifications. Ces débogages sont maintenant pris sur Control Distribute VC :

```
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 liaison », il fait de son mieux et au moins annonce la nouvelle :

```
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.

Encore une fois, le comportement est entièrement conforme aux spécifications lors de l'utilisation de clients LANE version 2.

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

Conseils de dépannage

Le protocole HSRP natif sur LANE ne doit pas engendrer trop de problèmes autres que le problème potentiel d'interopérabilité dû au protocole LE-NARP dépourvu du protocole T-NSAP.

Si les routeurs ont de la difficulté à déterminer s'ils sont actifs ou en veille, utilisez la commande **debug standby** pour voir si les HELLO sont visibles des deux côtés. Sinon, le BUS ne transmet probablement pas correctement les paquets.

2) HSRP sur les routeurs derrière LANE

La situation devient plus compliquée lorsque HSRP est configuré sur les interfaces LANE des routeurs situés derrière un nuage LANE, comme illustré à la Figure 2.

Remarque : cette figure illustre de manière logique le fait que le routeur n'est pas connecté à un ATM. Il ne doit pas nécessairement se trouver dans un périphérique distinct du commutateur LAN (un module de commutation de route [RSM] d'un Cisco Catalyst 5000 relève de ce cas).

Là encore, la difficulté provient du mappage adresse MAC/adresse NSAP imposé par LANE. Comme indiqué ci-dessus, lorsque le VMAC passe à un périphérique (lorsqu'un nouveau routeur devient actif) qui correspond à une autre adresse NSAP, tous les périphériques connectés au nuage LANE doivent être informés. Cela est assez facile à mettre en oeuvre dans un environnement HSRP sur LANE natif en utilisant LE-NARP (ou LE-ARP sans cible).

Le problème dans ce deuxième cas est que les LEC ne connaissent aucune information de couche 3 (IP), ils sont uniquement conçus pour relier des paquets entre deux supports différents (LAN et ATM).

Par exemple, dans la Figure 2, si le routeur 2 devient soudainement actif, il serait souhaitable que le commutateur LAN 2 informe tous les périphériques connectés au nuage ATM (LANE) du nouveau mappage VMAC-NSAP. Le LEC dans le commutateur LAN 2 est censé fournir un proxy pour toutes les adresses MAC qui se trouvent derrière. Les périphériques de l’ensemble du réseau local souhaitant envoyer du trafic à ces adresses MAC doivent le faire au moyen d’une configuration directe des données vers ce LEC. Intuitivement, on pourrait penser que ce ne sera pas un gros problème car, dès que le routeur 2 assume l’état Actif, il commence à fournir des paquets Hello avec le VMAC comme adresse MAC source. Ces informations seraient ensuite apprises par tous les commutateurs LAN et tout convergerait rapidement. Ceci est vrai dans les environnements non LANE, mais LANE est spécial pour la raison suivante :

Dans LANE, un paquet de données peut généralement être transmis via deux chemins :

- La liaison de données si ce paquet est une monodiffusion pour laquelle la destination a été mappée à un NSAP connu et si la liaison de données a déjà été établie.
- Le BUS pour les monodiffusions et multidiffusions inconnues.

Par conséquent, une même adresse MAC source les paquets qui seront reçus par un commutateur LAN sur deux chemins différents. Les multidiffusions et les monodiffusions inconnues arriveront par le biais du BUS tandis que les monodiffusions connues arriveront par le biais de directions de données. Si aucun effort particulier n’avait été fait, un commutateur LAN continuerait d’apprendre cette adresse MAC soit via une liaison de données, soit via le BUS, en fonction du dernier paquet reçu. Cela n'est pas souhaitable car le BUS ne doit être utilisé que pour envoyer des paquets pour des monodiffusions ou des multidiffusions inconnues. À ce stade, rien n'est appris sur le 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 revenir à l'exemple, il est possible de supposer que tous les LEC de cet ELAN sont déjà au courant du mappage VMAC-NSAP pour le routeur 1 avant que le routeur 2 ne devienne actif. Tous les commutateurs LAN savent également que le VMAC est derrière le commutateur LAN 1. Lorsque le routeur 2 devient actif et qu'il source les paquets Hello, ceux-ci sont transférés vers le nuage LANE via le BUS. Par conséquent, aucun des commutateurs LAN ne mettra à jour ses tables CAM avec ces nouvelles informations et tous les paquets envoyés à ce VMAC seront mal dirigés jusqu'à ce que les commutateurs LAN « oublient » cette entrée (le vieillissement par défaut étant de cinq minutes).

Remarque : La connectivité globale peut être perdue pendant 10 minutes maximum, car le compteur de vieillissement LE-ARP sur les LEC est également de cinq minutes par défaut. La réduction du compteur de vieillissement pour les adresses MAC aidera, mais ne résout pas le problème.

Il existe deux solutions :

1. Si les commutateurs LAN ne sont pas Cisco, revenez à la méthode décrite ci-dessus : à l'aide de l'adresse gravée. Si les routeurs utilisent uniquement leur adresse MAC pour source les paquets Hello et que l'adresse IP virtuelle change de mappage chaque fois qu'un basculement se produit, il n'y a aucune confusion possible quant à l'emplacement de ces adresses MAC.
2. Si les commutateurs LAN sont des commutateurs Cisco Catalyst, continuez à utiliser le VMAC en raison des modifications fournies par le système DDTS (Distributed Defect Tracking System) couvert par les ID de bogue Cisco CSCdj58719 (clients enregistrés seulement) et CSCdj60431 ().Essentiellement, lorsqu'un routeur assume l'état Actif, en plus du protocole ARP (réponse ARP non sollicitée) qu'il envoie conformément à la RFC 2281 , il envoie un deuxième protocole ARP avec l'adresse MAC de destination 0100.0CCD.CDCD. Lorsqu'un 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 sur le BUS.

Pour cette raison, il n'y a plus d'entrées LE-ARP obsolètes dans les différentes LEC et le nouvel emplacement de VMAC est propagé à tous les commutateurs (par exemple, au-delà du nuage LANE). Pour que cela fonctionne correctement, les conditions minimales suivantes doivent être remplies :

- Les routeurs doivent avoir au moins la version 11.1(24) du logiciel Cisco IOS, la version 11.2(13) ou la version 12.0.
- Les modules LANE doivent avoir au moins la version 3.2(8). Les versions 11.3W4 et ultérieures sont acceptables.

Cisco recommande d'utiliser les logiciels les plus récents.

3) Environnement mixte

Un dernier problème peut survenir dans des environnements mixtes. En prenant le scénario ci-dessus et en ajoutant un périphérique final LANE directement connecté (routeur ou station de travail), le périphérique final doit être informé d'un changement d'emplacement de la passerelle active de la même manière que dans le scénario 1. Si le nouveau routeur actif est connecté derrière un commutateur, la seule solution est que le commutateur lui-même envoie le LE-NARP au nom du routeur et c'est exactement ce qu'il faut faire.

En plus des étapes décrites ci-dessus, si un Cisco Catalyst récupère un paquet destiné à un CDCD 0100 0CCD, il envoie un LE-NARP (LE-NARP non source s'il exécute LANE version 2), dont le seul objectif est de supprimer les caches LE-ARP pour le VMAC.

Conclusion

Comme nous l'avons démontré, le protocole HSRP sur LANE fonctionne bien en principe, mais dans certaines circonstances, les utilisateurs peuvent perdre la connectivité pendant de courtes périodes si ils tombent dans l'une des failles décrites ci-dessus.

Important ! : Afin d'assurer le succès de HSRP sur LANE, suivez au moins ces deux recommandations :

- Pour être sûr, mettez à niveau vers au moins la dernière version du logiciel Cisco IOS Version 12.0.
- Dans les environnements multifournisseurs, il est préférable d'utiliser LANE version 2 ou l'adresse gravée afin d'éviter les problèmes.

Informations connexes

- Pages d'assistance technique ATM
- Support technique - Cisco Systems