HSRP via LANE implementeren

Inhoud

Inleiding

Het doel van dit document is een overzicht te geven van de problemen die kunnen worden aangetroffen bij het implementeren van het Hot Standby Router Protocol (HSRP) in een LAN Emulation-omgeving (LANE). Het beschrijft veel van de specificaties van HSRP via LANE en biedt tips voor het oplossen van problemen voor verschillende scenario's.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

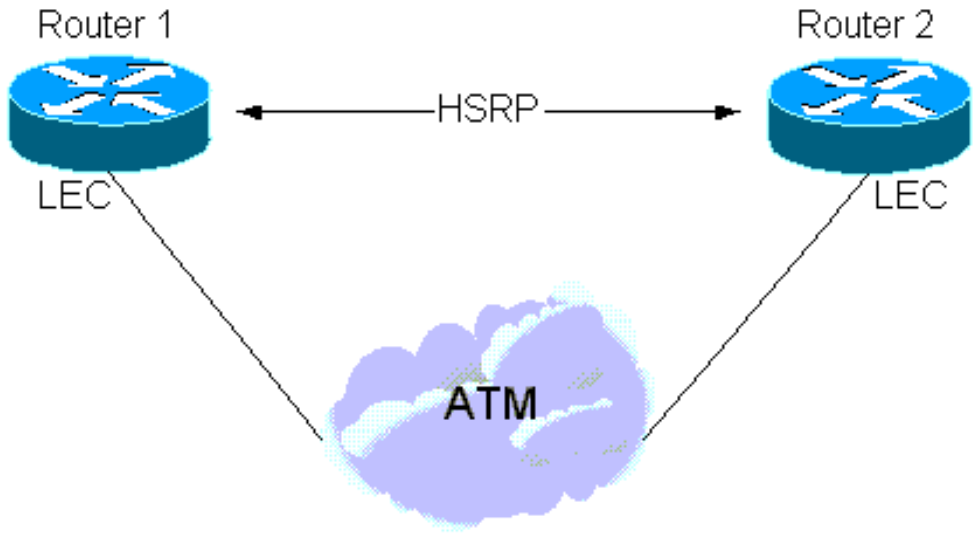
Samengevat, is het doel van HSRP om hosts in een netwerk toe te staan om één enkele "virtuele" router te gebruiken als de standaard gateway-meerdere routers deelnemen aan het HSRP-

protocol om de actieve router te selecteren, die de rol van standaardgateway en een backup router in acht neemt voor het geval dat het actieve fout gaat. Het resultaat is dat de standaardgateway altijd omhoog zal lijken zelfs als de fysieke eerste hoprouter verandert. Een volledige beschrijving van HSRP is te vinden in RFC 2281 .

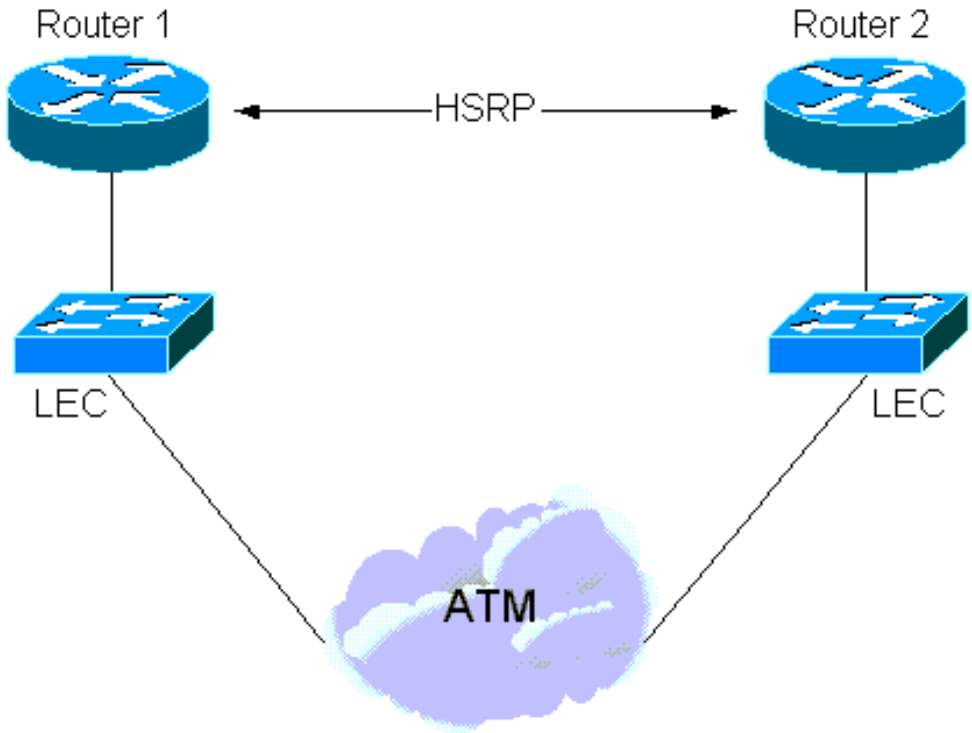
HSRP is ontworpen voor gebruik via multi-toegang, multicast of broadcast-enabled LAN's (doorgaans Ethernet, Token Ring of Fibre Distributed Data Interface [FDDI]). Daarom moet HSRP goed werken via ATM LANE.

Er kunnen zich verschillende situaties voordoen waarbij HSRP en LANE-interactie betrokken zijn:

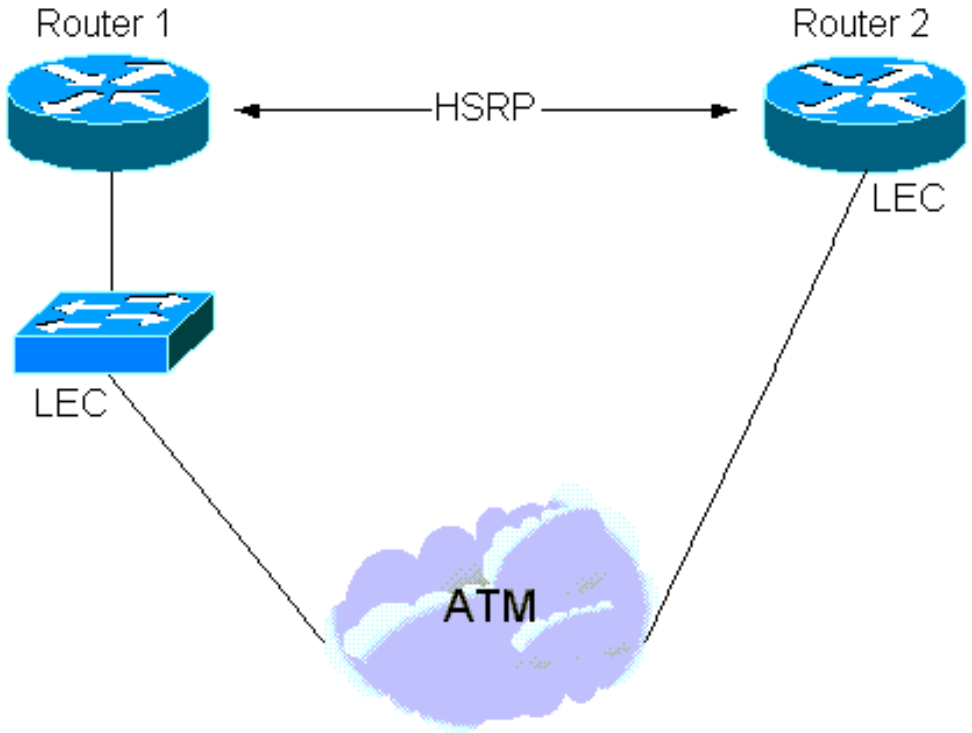
1. Sinds Cisco IOS® softwarerelease 11.2 kan HSRP "negatief" over LANE uitvoeren. In dit geval worden de **standby-**opdrachten direct ingesteld op ATM subinterfaces, waar LEC's (LAN Emulation Clients) aanwezig zijn. Raadpleeg de volgende illustratie.



2. Er is ook een geval waar HSRP op LAN interfaces wordt geconfigureerd, maar een deel van het netwerk spant een LANE-cloud door. Dit wordt gerealiseerd door het midden van een LAN switch met een ATM-interface (zoals een Cisco Catalyst 5000 met een LANE-module). Raadpleeg de volgende illustratie.



3. Tenslotte is er een "hybride" situatie waarin sommige HSRP-routers LANE-aangesloten zijn en andere LAN's achter een LAN-
   switch.



casestudy's

1) Native HSRP via LANE

Routers die aan HSRP deelnemen, verzenden "hallo"-pakketten over het omroepmedium om meer over elkaar te weten te komen en de actieve en standby routers te selecteren. Deze pakketten worden naar multicast adres 224.0.0.2 verzonden met een Tijd om te leven (TTL) van 1 en een multicast MAC-adres van 0100 5E00 002.

LANE introduceert hier geen nieuwe problemen, zodat de details die in RFC 2281 zijn beschreven, nog steeds van toepassing zijn door de uitwisseling van hallo, coup, en pakketten aftreden, de actieve en standby routers worden geselecteerd.

De hallo-pakketten worden verzonden over de uitzending en de onbekende server (BUS) en het volgende is wat een **debug ATM-pakket** (op de Multicast Forward Virtual Circuit [VC]) en een **debug-stand** zou onthullen:

```
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
```

Belangrijk is het kijken naar wat de LAN Emulation Client (LEC) via de BUS ontvangt (bijvoorbeeld

via de multicast forward):

```
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
```

Dit afvalwater vertaalt zich in het volgende:

```
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
```

Wat opmerkelijk is, is dat de hallo pakketten door de actieve router met het Virtuele adres van MAC (VMAC) als bron MAC adres-adres-dit wenselijk is omdat het leren van bruggen (switches) die deze pakketten verzenden hun content-adresseerbare geheugen (CAM) tabel met de aangewezen plaats van de VMAC zal bijwerken.

De sleutel tot HSRP ligt binnen het in kaart brengen tussen een IP adres en een MAC adres.

In de eenvoudigste expressie, is het virtuele IP-adres permanent gebonden aan een virtueel MAC-adres en is het enige aspect waar je zorgen over moet maken dat de switches altijd weten waar dit virtuele MAC-adres zich bevindt. Dit is gewaarborgd omdat de hellos afkomstig zijn van de 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
```

Een andere optie is dat de routers hun gebrand (**stand-by use-bia**) adressen gebruiken die aan het virtuele IP-adres zijn toegewezen. In dit geval, stuurt de mapping tussen virtuele IP- en MAC-adresveranderingen in de tijd-de nieuwe actieve router een Protocol voor adresresolutie (ARP) uit om de nieuwe virtuele IP-naar-MAC-adrestoewijzing aan te kondigen. Een ARP is gewoon een ongevraagde ARP-respons.

Opmerking: Bepaalde (oudere) IP-stapels begrijpen mogelijk geen 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
```

Opmerking: Om LANE te kunnen introduceren, is de sleutel dat er bovenop de virtuele IP-naar-MAC-adrestoewijzing een accounting moet zijn voor de VMAC-to-Network-Service-Access-Point (NSAP) adrestoewijzing. Deze mapping wordt eenvoudig opgelost via het LAN Emulation-Address Resolutie Protocol (LE-ARP)-proces: Een LEC die verkeer naar de actieve gateway wil verzenden zal LE-ARP voor de VMAC (of fysieke MAC) gebruiken als het gebrand MAC-adres [BIA] wordt gebruikt.

Bedenk nu wat er gebeurt wanneer een nieuwe router actief wordt: Om de LEC's op de hoogte te stellen van de nieuwe locatie van de actieve gateway (nieuwe VMAC-to-NSAP-mapping) moet de LE-ARP-tabel worden aangepast. Standaard zal LE-ARP-vermeldingen elke vijf minuten uitkomen, maar in de meeste gevallen is het vertrouwen op deze time-out onacceptabel. De conversie moet sneller zijn. De oplossing is afhankelijk van de vraag of de LEC ervan uitgaat dat de nieuwe actieve status LANE versie 1 of versie 2 (zie ATM Forum.com voor de LANE-specificaties) heeft:

- **LANE versie 1**Wanneer een router actief wordt, naast de stappen die in RFC 2281 worden beschreven , verstuurt deze een LE-NARP om de nieuwe VMAC-to-NSAP adresband bekend te maken. Volgens de LANE-specificaties kan een LEC bij ontvangst van een LE-NARP ervoor kiezen de LE-ARP-vermelding die overeenkomt met het MAC-adres, te wissen of bij te werken. De neiging binnen Cisco is de conservatievere benadering te volgen en te kiezen om de LE-ARP ingang-deze te ontruimen zal LEC onmiddellijk re-LE-ARP veroorzaken zonder te hoeven wachten op de time-out van vijf minuten.**Opmerking:** deze oplossing kan de compatibiliteit van de producten zoals hieronder beschreven veroorzaken.
- **LANE versie 2**In LANE versie 2 werden bepaalde tekortkomingen van LANE versie 1 verholpen: LE-NARP is vervangen door de doelloze LE-ARP en de geen-bron LE-NARP. Het doelloze LE-ARP kan worden gezien als een voertuig om nieuwe bindingen te adverteren, terwijl het doel van LE-NARP zonder bron is om een bestaande MAC-to-NSAP-adresbinding achterhaald te maken. Dit wordt ten uitvoer gelegd door te zeggen dat als een router van Standby- naar Active verandert, deze een doelloze LE-ARP verstuurt (dit wordt gebruikt om

een MAC-to-NSAP-mapping aan te geven) en als deze van Active in Standby verandert, dan wordt een geen-bron LE-NARP verzonden (dit wordt gebruikt om een MAC-to-NSAP-binding achterhaald te maken).

Probleem - interoperabiliteit

Er is een probleem dat zich vaak genoeg voordoet om een grondiger onderzoek te verdienen. De LANE versie 1 specificaties geven aan dat LE-NARP de "oude binding" moet specificeren, die verouderd wordt door het (oude) Target NSAP (T-NSAP) adres te specificeren. Routers die deelnemen aan HSRP onderhouden doorgaans geen gegevensverbindingen tussen elkaar.

Daarom kent de pas actieve router deze informatie niet en zal zij ervoor kiezen dit veld niet te voltooien omdat het niet beter weet. Dit is een milde schending van de specificaties en sommige verkopers zullen deze pakketten negeren als het T-NSAP adresveld alle nul is. Helaas is er geen tijdelijke oplossing voor dit-als LE-NARP genegeerd wordt, baseer dan op de LE-ARP tijd (gewoonlijk vijf minuten) voordat de juiste binding geleerd wordt.

Wanneer een LE-ARP of LE-NARP verzonden wordt met een T-NSAP adresveld van alle nullen, wordt het "doelloos" genoemd. Zoals hierboven is aangegeven, met de komst van LANE versie 2 (en Multiprotocol-over-ATM [MPOA]), is dit standaard geworden en bestaat het probleem niet meer.

Dit gebeurt in LANE versie 1 wanneer zich problemen kunnen voordoen:

- Als de router de "oude band" kent, zou het net zo goed de specificaties kunnen volgen. Deze debugs worden nu gebruikt op 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)
```

- Indien het de "oude" binding niet kent, doet het zijn best en adverteert het in ieder geval met de nieuwe:

```
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
```

  Opmerking: Dit keer is het T-NSAP-adres leeg.

Opnieuw is het gedrag volledig binnen de specificaties bij gebruik van LANE versie 2 clients.

Opmerking: Software die MPOA ondersteunt, ondersteunt ook LANE versie 2.

Tips bij het oplossen van problemen

Native HSRP via LANE mag niet leiden tot te veel problemen anders dan het potentiële interoperabiliteitsprobleem als gevolg van het LE-NARP-losgekoppeld van de T-NSAP.

Als de routers moeite hebben vast te stellen of zij Active of Standby zijn, gebruikt u de opdracht **debug standby** om te zien of de hellos aan beide zijden worden gezien. Als niet, dan zal de BUS waarschijnlijk niet correct de pakketten verzenden.

2) HSRP via routers achter LANE

De situatie wordt gecompliceerder wanneer HSRP wordt geconfigureerd op LANE-interfaces van routers achter een LANE-cloud, zoals in afbeelding 2 wordt geïllustreerd.

Opmerking: dit getal geeft logisch aan dat de router niet-ATM aangesloten is. Het hoeft niet per se in een apparaat te zijn dat gescheiden is van de LAN-switch (een routemodule Switch [RSM] in een Cisco Catalyst 5000-sleuf onder dit geval).

Opnieuw doet de moeilijkheid zich voor als gevolg van de MAC-Address-to-NSAP-Address mapping die door LANE wordt opgelegd. Zoals hierboven vermeld, wanneer de VMAC-switches op een apparaat (wanneer een nieuwe router actief wordt) dat correspondeert met een ander NSAP-adres, moeten alle apparaten die aan de LANE-cloud zijn gekoppeld op de hoogte worden gebracht. Dit wordt tamelijk eenvoudig geïmplementeerd in een native HSRP over LANE-omgeving door het LE-NARP (of doelloze LE-ARP) te gebruiken.

Het probleem in dit tweede geval is dat de LECs niet op de hoogte zijn van enige Layer 3 informatie (IP), ze zijn uitsluitend ontworpen om pakketten tussen twee verschillende media (LAN en ATM) te overbruggen.

In afbeelding 2 bijvoorbeeld, als router 2 plotseling actief wordt, is het wenselijk dat LAN switch 2 alle apparaten die aangesloten zijn op de ATM (LANE) cloud informeert over de nieuwe VMAC-to-NSAP mapping. LEC in LAN switch 2 zou proxy zijn voor alle MAC-adressen die erachter staan. Apparaten over LANE die verkeer naar deze MAC-adressen willen doorsturen, moeten dit doen door middel van een gegevensdirecte instelling naar deze LEC. Intuïtief zou je kunnen denken dat dit geen groot probleem zal zijn omdat, zodra Router 2 de Actieve Staat veronderstelt, het hellos zal gaan betrekken bij de VMAC als het bron-MAC-adres. Deze informatie zou dan door alle LAN switches worden geleerd en alles zou snel samenvallen. Dit is waar in niet-LANE omgevingen, maar LANE is speciaal om de volgende reden:

In LANE kan een gegevenspakket meestal door twee paden worden verzonden:

- De data-direct als dit pakket een unicast is waarvoor de bestemming aan een bekend NSAP in kaart is gebracht en als de data-direct reeds gevestigd is.
- De BUS voor onbekende eensten en multicast.

Daarom zal een zelfde MAC-adres pakketten bron die door een LAN switch over twee verschillende paden zullen worden ontvangen. Multicast en onbekende eensten zullen via de BUS komen, terwijl bekende eensten via gegevensdragers aankomen. Als er geen speciale inspanning was gedaan, zou een LAN switch dit MAC-adres blijven leren via een data-direct of via de BUS, afhankelijk van het laatste ontvangen pakket. Dit is ongewenst omdat de BUS alleen gebruikt mag

worden om pakketten naar onbekende unicast of multicast te verzenden. In dit stadium wordt er niets geleerd over de BUS, maar in werkelijkheid heeft de BUS de volgende keuze:

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.

Om terug te keren naar het voorbeeld, is het veilig om aan te nemen dat alle LECs in deze ELAN reeds bewust zijn van de VMAC-NSAP afbeelding voor router 1 voorafgaand aan wanneer router 2 Actief wordt. Alle LAN switches weten ook dat VMAC achter LAN switch 1 zit. Wanneer router 2 Actief wordt en bronnen de hallo pakketten ontvangt, worden deze naar de LANE wolk over de BUS verzonden. Om deze reden zal geen van de LAN switches hun CAM-tabellen met deze nieuwe informatie bijwerken en zullen alle pakketten die naar deze VMAC worden verzonden, verkeerd worden gericht tot de LAN-switches "vergeten" over deze ingang (de standaardveroudering is vijf minuten).

Opmerking: globale connectiviteit zou eigenlijk tot 10 minuten verloren kunnen zijn aangezien de LE-ARP verouderings-timer op de LECs ook vijf minuten standaard is. Het verminderen van de veroudering-timer voor de adressen van MAC zal helpen, maar lost eigenlijk het probleem niet op.

Hiervoor bestaan twee oplossingen:

1. Als LAN-switches niet-Cisco zijn, kies dan een van de hierboven beschreven methoden: gebruik van het ingebouwde adres. Als de routers alleen hun MAC-adres gebruiken om de hallo-pakketten te bronnen en dat het virtuele-IP-adres verandert in mapping wanneer een switch-over wordt uitgevoerd, is er geen verwarring mogelijk over de plaats waar deze MAC-adressen zich bevinden.
2. Als LAN-switches Cisco-katalysatoren zijn, moet u het VMAC blijven gebruiken vanwege de wijzigingen die zijn geleverd door het Distributed Defect Tracking System (DTS) dat is gedekt door Cisco bug ID's CSCdj58719 (alleen geregistreerde klanten) en CSCdj60431 (alleen) .In essentie, wanneer een router de Actieve staat veronderstelt, naast de ARP (ongevraagde ARP respons) die het in overeenstemming met RFC 2281 verstuurt , stuurt de router een tweede ARP met een bestemming MAC-adres van 100.0CCD.CDCD. Wanneer een Cisco Catalyst dit pakket ontvangt, doet het twee dingen:Hiermee wordt de LE-ARP-ingang die het voor de VMAC heeft, gewist.Het leert de VMAC over de BUS.

Daarom zijn er geen meer stabiele LE-ARP-waarden in de verschillende LEC's en wordt de nieuwe locatie van de VMAC verspreid naar alle switches (bijvoorbeeld buiten de LANE-cloud). Om dit correct te laten werken, moet aan de volgende minimale softwarevereisten worden voldaan:

- Routers moeten ten minste Cisco IOS-softwarerelease 11.1(24)E, versie 11.2(13) of alle versie 12.0 hebben.
- LANE-modules moeten ten minste versie 3.2(8) hebben. 11.3W4-versies en latere versies zijn aanvaardbaar.

Cisco raadt het gebruik van de nieuwste software aan.

3) Gemengde omgeving

Er is nog een laatste probleem dat kan ontstaan in gemengde omgevingen. Rekening houdend met het bovenstaande scenario en door een direct aangesloten LANE-eindapparaat (router of werkstation) toe te voegen, moet het eindapparaat op de hoogte worden gesteld van een verandering van locatie van de actieve gateway op dezelfde manier als in scenario 1. Als de nieuw actieve router achter een switch is aangesloten, is de enige oplossing voor de switch zelf om LE-NARP namens de router uit te sturen en dit is precies wat te doen.

Naast de stappen die hierboven worden beschreven, als Cisco Catalyst een pakket ophaalt dat is bestemd voor 1000CD CD, stuurt het een LE-NARP (geen-bron LE-NARP als LAN versie 2 wordt uitgevoerd), wat als enige doel heeft de LE-ARP-caches voor de VMAC te wissen.

Conclusie

Zoals aangetoond werkt HSRP via LANE in principe goed, maar onder bepaalde omstandigheden kunnen gebruikers connectiviteit voor korte perioden verliezen als ze in een van de hierboven beschreven mazen vallen.

Belangrijk!: Om succes met HSRP over LANE te verzekeren, volg ten minste deze twee aanbevelingen:

- Voor een veilige upgrade naar ten minste de nieuwste versie van Cisco IOS-softwarerelease 12.0.
- In omgevingen van meerdere leveranciers is het het beste om LANE versie 2 of het gebrand adres te gebruiken om problemen te voorkomen.

Gerelateerde informatie

- Ondersteuning van ATM-technologie
- Technische ondersteuning - Cisco-systemen