Implementierung von HSRP über LANE

Inhalt

Einführung

In diesem Dokument werden die Probleme beschrieben, die bei der Implementierung des Hot Standby Router Protocol (HSRP) in einer LAN Emulation (LANE)-Umgebung auftreten können. Er beschreibt viele der Besonderheiten von HSRP über LANE und enthält Tipps zur Fehlerbehebung für verschiedene Szenarien.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen

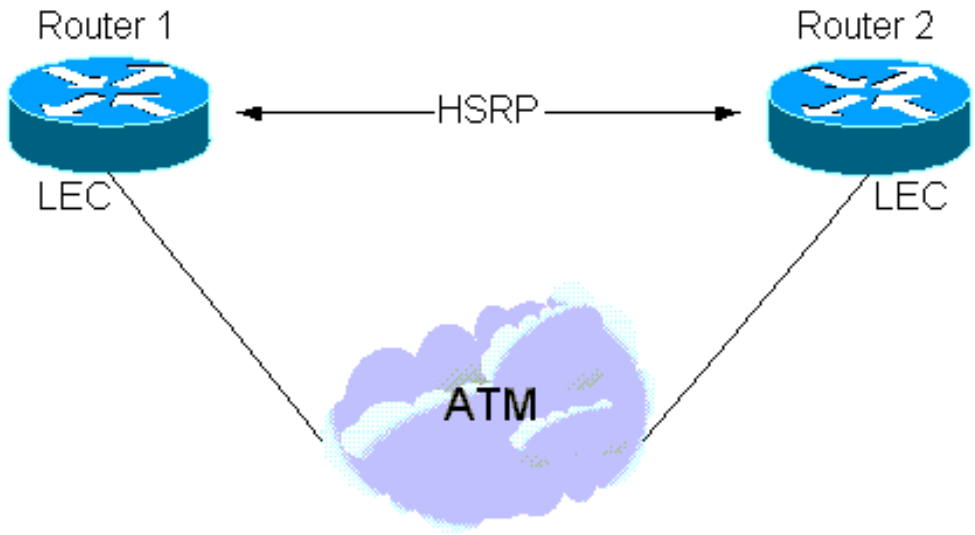
Zusammenfassend besteht der Zweck von HSRP darin, Hosts in einem Subnetz die Verwendung

eines einzelnen "virtuellen" Routers als Standard-Gateway zu ermöglichen. Mehrere Router nehmen am HSRP-Protokoll teil, um den aktiven Router auszuwählen, der die Rolle des Standard-Gateways und eines Backup-Routers übernimmt, falls der aktive Router ausfällt. Das Ergebnis ist, dass das Standard-Gateway immer eingeschaltet erscheint, auch wenn sich der physische First-Hop-Router ändert. Eine vollständige Beschreibung von HSRP finden Sie in RFC 2281 .

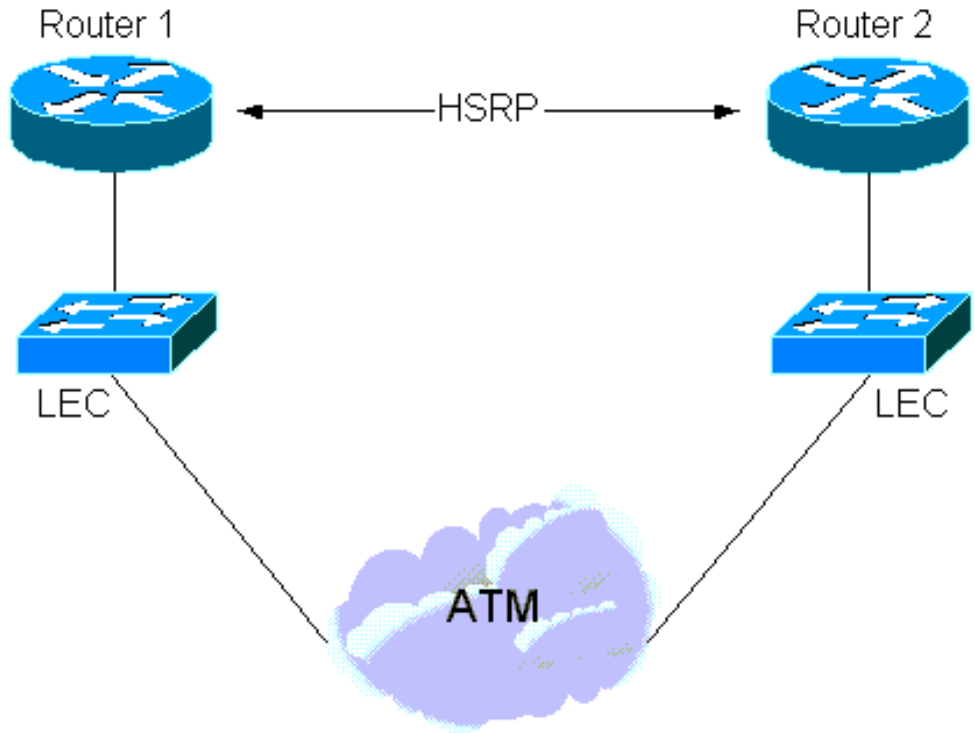
HSRP wurde für die Verwendung über LANs mit mehreren Zugriffen, Multicast oder Broadcast entwickelt (in der Regel Ethernet, Token Ring oder Fiber Distributed Data Interface [FDDI]). Daher sollte HSRP über ATM LANE gut funktionieren.

Es können mehrere Situationen auftreten, in denen HSRP und LANE interagieren:

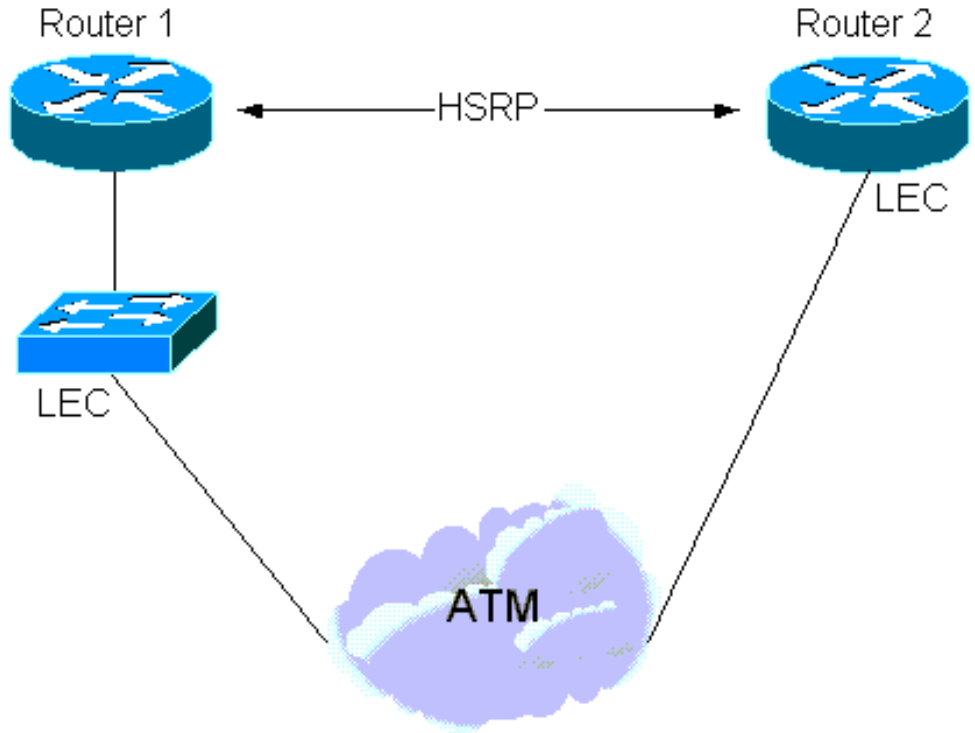
1. Seit Version 11.2 der Cisco IOS® Software kann HSRP "nativ" über LANE ausgeführt werden. In diesem Fall werden die **Standby-**Befehle direkt auf den ATM-Subschnittstellen konfiguriert, auf denen sich LAN Emulation Clients (LECs) befinden. Siehe folgende Abbildung.



2. Es gibt auch eine Instanz, in der HSRP auf LAN-Schnittstellen konfiguriert wird, ein Teil des Subnetzes jedoch eine LANE-Cloud umfasst. Dies wird durch das Intermediär eines LAN-Switches mit einer ATM-Schnittstelle (z. B. einem Cisco Catalyst 5000 mit einem LAN-Modul) erreicht. Siehe folgende
Abbildung.



3. Schließlich gibt es eine "Hybridsituation", bei der einige HSRP-Router mit LAN verbunden sind und andere sich in einem LAN hinter einem LAN-Switch befinden.



Anwenderberichte

1) Natives HSRP über LANE

Router, die an HSRP teilnehmen, senden "Hello"-Pakete über das Übertragungsmedium, um sich gegenseitig zu informieren und die aktiven Router und Standby-Router auszuwählen. Diese Pakete werden an die Multicast-Adresse 224.0.0.2 mit der Time to Live (TTL) von 1 und der Multicast-Ziel-MAC-Adresse 0100 5E00 0002 gesendet.

LANE führt hier keine neuen Probleme ein. Die in RFC 2281 beschriebenen Details gelten weiterhin beim Austausch von Hello-, Putsch- und Rückgabepaketen. Die aktiven Router und die Standby-Router werden ausgewählt.

Die Hello-Pakete werden über den Broadcast- und unbekannten Server (BUS) gesendet. Ein **Debug-ATM-Paket** (auf dem Virtual Circuit Multicast Forward [VC]) und ein **Debug-Standby** würden Folgendes ergeben:

```
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
```

Wichtig ist, zu prüfen, was der LAN Emulation Client (LEC) über den BUS empfängt (z. B. über

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
```

Dieses Hexadezimalsystem übersetzt Folgendes:

```
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
```

Bemerkenswert ist, dass die Hello-Pakete vom aktiven Router mit der Virtual MAC-Adresse (VMAC) als Quell-MAC-Adresse bezogen werden. Dies ist wünschenswert, da Learning Bridges (Switches), die diese Pakete weiterleiten, ihre CAM-Tabelle (Content-Addressable Memory) mit dem geeigneten Speicherort der VMAC aktualisieren.

Der Schlüssel zum HSRP liegt in der Zuordnung zwischen einer IP-Adresse und einer MAC-Adresse.

Im einfachsten Ausdruck ist die virtuelle IP-Adresse dauerhaft an eine virtuelle MAC-Adresse gebunden, und der einzige Aspekt, der zu beachten ist, ist, dass die Switches immer wissen, wo sich diese virtuelle MAC-Adresse befindet. Dies ist gewährleistet, da die Hellos vom VMAC beschafft werden.

```
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
```

Eine weitere Option besteht darin, dass die Router ihre verbrannten (**Standby-Nutzungs-bia**)-Adressen verwenden, die der virtuellen IP-Adresse zugeordnet sind. In diesem Fall ändert sich die Zuordnung zwischen virtuellen IP- und MAC-Adressen im Laufe der Zeit. Der neu aktive Router sendet ein Address Resolution Protocol (ARP), um die neue virtuelle IP-MAC-Adresszuordnung anzukündigen. Ein ARP ist einfach eine unerwünschte ARP-Antwort.-

Hinweis: Bestimmte (ältere) IP-Stacks verstehen möglicherweise keine 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
```

Hinweis: Um LANE einzuführen, muss neben der Virtual IP-to-MAC-Adressenzuordnung die Adressenzuordnung VMAC-to-Network-Service-Access Point (NSAP) berücksichtigt werden. Diese Zuordnung wird einfach durch den LAN Emulation-Address Resolution Protocol (LE-ARP)-Prozess aufgelöst: Ein LEC, der Datenverkehr an das aktive Gateway senden möchte, verwendet LE-ARP für die VMAC (oder physische MAC-Adresse, wenn die integrierte MAC-Adresse [BIA] verwendet wird).

Nun überlegen Sie, was passiert, wenn ein neuer Router aktiv wird: Damit die LECs über den neuen Standort des aktiven Gateways informiert werden (neue VMAC-zu-NSAP-Zuordnung), muss die LE-ARP-Tabelle geändert werden. In der Standardeinstellung werden LE-ARP-Einträge alle fünf Minuten gelöscht, in den meisten Fällen ist jedoch eine solche Zeitüberschreitung inakzeptabel - die Konvergenz muss schneller erfolgen. Die Lösung hängt davon ab, ob der LEC, der den neuen Aktiv-Status annimmt, die LANE Version 1 oder Version 2 ausführt (die LANE-Spezifikationen finden Sie unter ATM Forum.com):

- **LANE Version 1**Wenn ein Router aktiv wird, sendet er zusätzlich zu den in RFC 2281 beschriebenen Schritten einen LE-NARP, um die neue VMAC-zu-NSAP-Adressbindung bekannt zu machen. Gemäß den LANE-Spezifikationen kann ein LEC nach Erhalt eines LE-NARP den LE-ARP-Eintrag, der der MAC-Adresse entspricht, löschen oder aktualisieren. Cisco verfolgt in der Regel einen eher konservativen Ansatz und löscht den LE-ARP-Eintrag. Dies führt dazu, dass der LEC den LE-ARP sofort umstellt, ohne auf die 5-Minuten-Zeitüberschreitung warten zu müssen.**Hinweis:** Diese Lösung kann das unten beschriebene Kompatibilitätsproblem verursachen.
- **LANE Version 2**In LANE Version 2 wurden einige Mängel von LANE Version 1 behoben: Die LE-NARP wurde durch die ziellose LE-ARP und die quasi-nackte LE-NARP ersetzt. Die ziellose LE-ARP kann als ein Mittel angesehen werden, um neue Bindungen anzukündigen, während der nicht-Source-LE-NARP dazu dient, eine bestehende MAC-zu-NSAP-

Adressbindung obsolet zu machen. Implementiert wird dies so, dass ein Router, der von Standby zu Aktiv wechselt, eine ziellose LE-ARP sendet (diese wird verwendet, um eine MAC-zu-NSAP-Zuordnung anzukündigen) und wenn er von Aktiv zu Standby wechselt, eine quelloffene LE-NARP sendet (dies wird verwendet, um eine MAC-zu-NSAP-Bindung obsolet zu machen).

Problem - Interoperabilität

Es gibt ein Problem, das oft genug auftritt, um eine eingehendere Prüfung zu verdienen. Die LANE Version 1-Spezifikationen geben an, dass der LE-NARP die "alte Bindung" angeben muss, die durch die Angabe der (alten) Ziel NSAP (T-NSAP)-Adresse veraltet ist. In der Regel unterhalten Router, die an HSRP teilnehmen, keine Datenverzeichnisse untereinander.

Daher kennt der neu aktive Router diese Informationen nicht und er wird dieses Feld nicht ausfüllen, da er es nicht besser kennt. Dies stellt eine leichte Verletzung der Spezifikationen dar, und einige Anbieter ignorieren diese Pakete, wenn das T-NSAP-Adressfeld alle Nullen enthält. Leider gibt es dafür keine Problemumgehung - wenn die LE-NARP ignoriert wird, verlassen Sie sich auf das LE-ARP-Timeout (in der Regel fünf Minuten), bevor die richtige Bindung gelernt wird.

Wenn ein LE-ARP oder ein LE-NARP mit einem T-NSAP-Adressfeld aller Nullen gesendet wird, wird dies als "ziellos" bezeichnet. Wie oben bereits erwähnt, ist das mit der Einführung von LANE Version 2 (und Multiprotocol over ATM [MPOA]) Standard geworden, und das Problem existiert nicht mehr.

Dies geschieht in der Version 1 von LANE, wenn Probleme auftreten können:

- Wenn der Router die "alte Bindung" kennt, kann er auch die Spezifikationen befolgen. Diese DebuggingInnen werden nun auf dem Control Distribution VC ausgeführt:
```
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)
```
- Wenn sie die "alte Bindung" nicht kennt, tut sie ihr Bestes und kündigt zumindest die neue an:
```
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
```
  Hinweis: Diesmal ist die T-NSAP-Adresse leer.

Auch hier liegt das Verhalten vollständig im Rahmen der Vorgaben bei der Verwendung von LANE

Version 2 Clients.

Hinweis: Software, die MPOA unterstützt, unterstützt auch LANE Version 2.

Tipps zur Fehlerbehebung

Natives HSRP über LANE darf nur zu viele Probleme mit potenziellen Interoperabilitätsproblemen verursachen, da der LE-NARP keine T-NSAP enthält.

Wenn die Router Schwierigkeiten haben festzustellen, ob sie aktiv oder Standby sind, können Sie mit dem **Debug Standby-**Befehl überprüfen, ob die Hellos auf beiden Seiten sichtbar sind. Andernfalls leitet der BUS die Pakete wahrscheinlich nicht korrekt weiter.

2) HSRP über Router hinter LANE

Die Situation wird komplizierter, wenn HSRP auf LANE-Schnittstellen von Routern konfiguriert wird, die sich hinter einer LANE-Cloud befinden, wie in Abbildung 2 gezeigt.

Hinweis: Diese Abbildung zeigt logisch, dass der Router nicht über ATM verbunden ist. Es muss sich nicht unbedingt in einem Gerät befinden, das vom LAN-Switch getrennt ist (in diesem Fall fällt ein Route Switch Module [RSM] in einem Cisco Catalyst 5000 unter).

Auch hier ergibt sich die Schwierigkeit aus der MAC-Adresse-zu-NSAP-Adressenzuordnung von LANE. Wie oben erwähnt, müssen alle an die LAN-Cloud angeschlossenen Geräte informiert werden, wenn das VMAC zu einem Gerät wechselt (wenn ein neuer Router aktiv wird), das einer anderen NSAP-Adresse entspricht. Dies ist in einer nativen HSRP over LANE-Umgebung mithilfe des LE-NARP (oder des ziellosen LE-ARP) relativ einfach implementierbar.

Das Problem in diesem zweiten Fall ist, dass die LECs keine Layer-3-Informationen (IP) kennen, sondern lediglich dazu entwickelt wurden, Pakete zwischen zwei verschiedenen Medien (LAN und ATM) zu überbrücken.

Beispiel: Wenn Abbildung 2 plötzlich Router 2 aktiv wurde, sollte LAN Switch 2 alle mit der ATM (LANE)-Cloud verbundenen Geräte über die neue VMAC-zu-NSAP-Zuordnung informieren. Der LEC in LAN Switch 2 soll alle dahinter liegenden MAC-Adressen proxieren. Geräte in der gesamten LANE, die Datenverkehr an diese MAC-Adressen senden möchten, müssen dies über eine datendirekte Konfiguration zu diesem LEC tun. Intuitiv könnte man annehmen, dass dies kein großes Problem ist, da Router 2, sobald er den aktiven Zustand übernimmt, die Quelladresse der MAC-Adresse mit der VMAC-Quelladresse beginnt. Diese Informationen werden dann von allen LAN-Switches erfasst, und alles wird schnell konvergiert. Dies gilt für Umgebungen ohne LAN, aber LANE ist aus folgenden Gründen besonders:

In LANE kann ein Datenpaket normalerweise über zwei Pfade übertragen werden:

- Die Datenleitung, wenn es sich bei diesem Paket um ein Unicast-Paket handelt, für das das Ziel einer bekannten NSAP zugeordnet wurde und das Datendirect bereits eingerichtet wurde.
- Der BUS für unbekannte Unicasts und Multicasts.

Aus diesem Grund sendet dieselbe MAC-Adresse Pakete, die von einem LAN-Switch über zwei verschiedene Pfade empfangen werden. Multicasts und unbekannte Unicasts werden über den BUS eintreffen, wohingegen bekannte Unicasts über Datenverzeichnisse eintreffen. Wenn keine besonderen Anstrengungen unternommen wurden, würde ein LAN-Switch diese MAC-Adresse

abhängig vom letzten empfangenen Paket entweder über einen Datendirect oder über den BUS erlernen. Dies ist nicht wünschenswert, da der BUS nur zum Senden von Paketen für unbekannte Unicasts oder Multicasts verwendet werden sollte. In diesem Stadium wird nichts über die BUS gelernt, aber in Wirklichkeit entscheiden Sie sich, folgende Schritte zu tun:

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.

Um zum Beispiel zurückzukehren, kann davon ausgegangen werden, dass alle LECs in diesem ELAN die VMAC-NSAP-Zuordnung für Router 1 bereits kennen, bevor Router 2 aktiv wird. Alle LAN-Switches wissen auch, dass sich das VMAC hinter dem LAN-Switch 1 befindet. Wenn Router 2 aktiv wird und die Hello-Pakete sendet, werden diese über den BUS an die LANE Cloud weitergeleitet. Daher aktualisiert keiner der LAN-Switches seine CAM-Tabellen mit diesen neuen Informationen, und alle an diese VMAC gesendeten Pakete werden fehlgeleitet, bis die LAN-Switches diesen Eintrag "vergessen" (die Standardeinstellung beträgt fünf Minuten).

Hinweis: Die Gesamtverbindung kann für bis zu 10 Minuten unterbrochen werden, da der LE-ARP-Alterungs-Timer auf den LECs standardmäßig ebenfalls fünf Minuten beträgt. Eine Reduzierung des Alterungs-Timers für MAC-Adressen ist hilfreich, löst das Problem jedoch nicht.

Dafür gibt es zwei Lösungen:

1. Wenn LAN-Switches nicht von Cisco sind, kehren Sie zu einer oben beschriebenen Methode zurück: Verwenden der Adresse für das Eingebrannte Signal. Wenn die Router nur ihre MAC-Adresse verwenden, um die Hello-Pakete zu beziehen, und die Zuordnung der virtuellen IP-Adresse ändert sich bei jedem Switchover, besteht keine Verwirrung darüber, wo sich diese MAC-Adressen befinden.
2. Wenn LAN-Switches Cisco Catalyst sind, verwenden Sie weiterhin VMAC, da das Distributed Defect Tracking System (DDTS) Änderungen enthält, die in den Cisco Bug-IDs CSCdj58719 (nur registrierte Kunden) und CSCdj60431 enthalten sind (nur registrierte Kunden). .Wenn ein Router neben der ARP-Antwort (unerwünschte ARP-Antwort), die er gemäß RFC 2281 sendet, den aktiven Status übernimmt , sendet der Router im Wesentlichen einen zweiten ARP mit der MAC-Zieladresse 0100.0CCD.CDCD. Wenn ein Cisco Catalyst dieses Paket empfängt, geschieht Folgendes:Es löscht den LE-ARP-Eintrag für den VMAC.Er lernt VMAC über den BUS.

Aus diesem Grund gibt es in den verschiedenen LECs keine mehr veralteten LE-ARP-Einträge mehr, und der neue Standort des VMAC wird auf alle Switches verteilt (z. B. über die LAN-Cloud hinaus). Damit dies ordnungsgemäß funktioniert, müssen die folgenden Mindestanforderungen an die Software erfüllt sein:

- Router müssen mindestens über die Cisco IOS Software, Version 11.1(24), Version 11.2(13) oder die gesamte Version 12.0 verfügen.
- LANE-Module müssen mindestens Version 3.2(8) aufweisen. Versionen ab 11.3W4 sind zulässig.

Cisco empfiehlt die Verwendung der neuesten Software.

3) Gemischte Umgebung

Ein letztes Problem kann in gemischten Umgebungen auftreten. Unter Berücksichtigung des obigen Szenarios und des Hinzufügens eines direkt verbundenen LANE-Endgeräts (Router oder Workstation) muss das Endgerät wie in Szenario 1 über einen Standortwechsel des aktiven Gateways informiert werden. Wenn der neu aktive Router hinter einem Switch angeschlossen ist, ist die einzige Lösung für den Switch selbst, den LE-NARP im Auftrag des Routers zu senden. Genau das ist es, was zu tun ist.

Zusätzlich zu den oben beschriebenen Schritten sendet ein Cisco Catalyst ein Paket, das für 0100 0CCD CDCD bestimmt ist, ein LE-NARP (kein Source LE-NARP bei Ausführung von LANE Version 2), das ausschließlich dazu dient, die LE-ARP-Caches für VMAC zu löschen.

Schlussfolgerung

HSRP over LANE funktioniert prinzipiell gut, aber unter bestimmten Umständen können Benutzer die Verbindung für kurze Zeit verlieren, wenn sie in einen der oben beschriebenen Schlupflöcher fallen.

Wichtig!: Um den Erfolg mit HSRP über LANE sicherzustellen, sollten Sie mindestens die folgenden beiden Empfehlungen befolgen:

- Um sicher zu sein, müssen Sie auf mindestens die neueste Version der Cisco IOS Software, Version 12.0, aktualisieren.
- In Umgebungen mit Geräten verschiedener Anbieter empfiehlt es sich, die Version 2 der LANE oder die integrierte Adresse zu verwenden, um Probleme zu vermeiden.

Zugehörige Informationen

- Support-Seiten für ATM-Technologie
- Technischer Support - Cisco Systems