Implementazione di HSRP su LANE

Sommario

Introduzione

Lo scopo di questo documento è quello di descrivere i problemi che possono verificarsi quando si implementa il protocollo HSRP (Hot Standby Router Protocol) in un ambiente LANE (LAN Emulation). Descrive molte delle specifiche di HSRP su LANE e fornisce suggerimenti per la risoluzione dei problemi per vari scenari.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

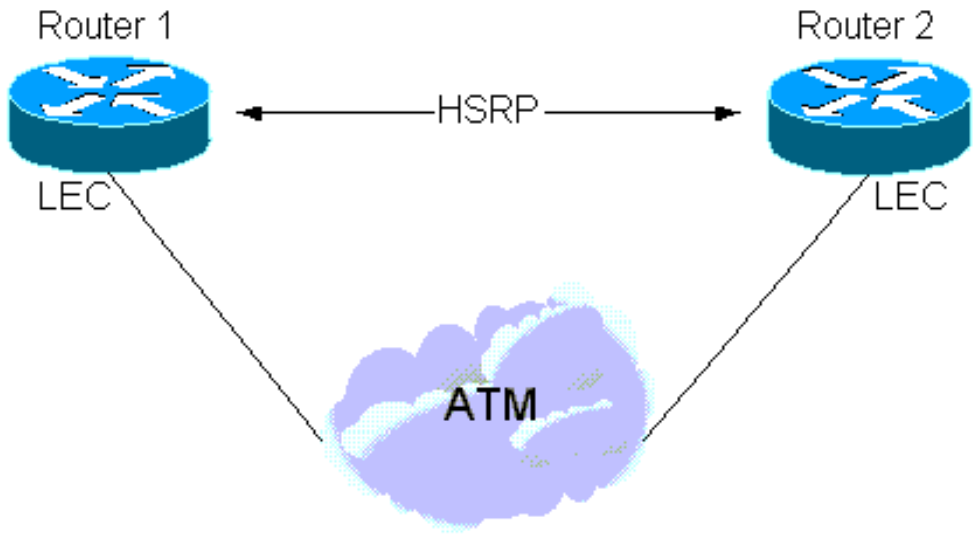
In breve, lo scopo di HSRP è quello di consentire agli host di una subnet di utilizzare un singolo

router "virtuale" come gateway predefinito. Al protocollo HSRP partecipano più router per selezionare il router attivo, che assume il ruolo di gateway predefinito e di router di backup in caso di errore di quello attivo. Di conseguenza, il gateway predefinito apparirà sempre attivo anche se cambia il router del primo hop fisico. Una descrizione completa dell'HSRP è disponibile nella RFC 2281 .

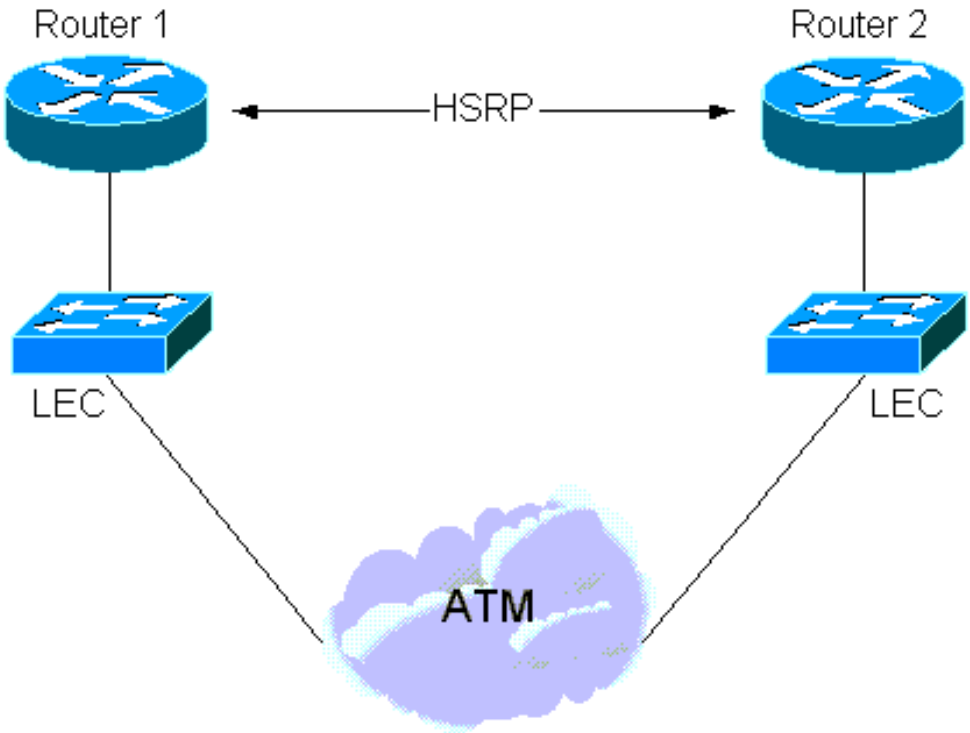
HSRP è stato progettato per l'utilizzo su LAN con capacità multi-accesso, multicast o broadcast (in genere Ethernet, Token Ring o Fiber Distributed Data Interface [FDDI]). Pertanto, l'HSRP deve funzionare correttamente su LANE ATM.

Possono verificarsi diverse situazioni che coinvolgono l'interazione tra HSRP e LANE:

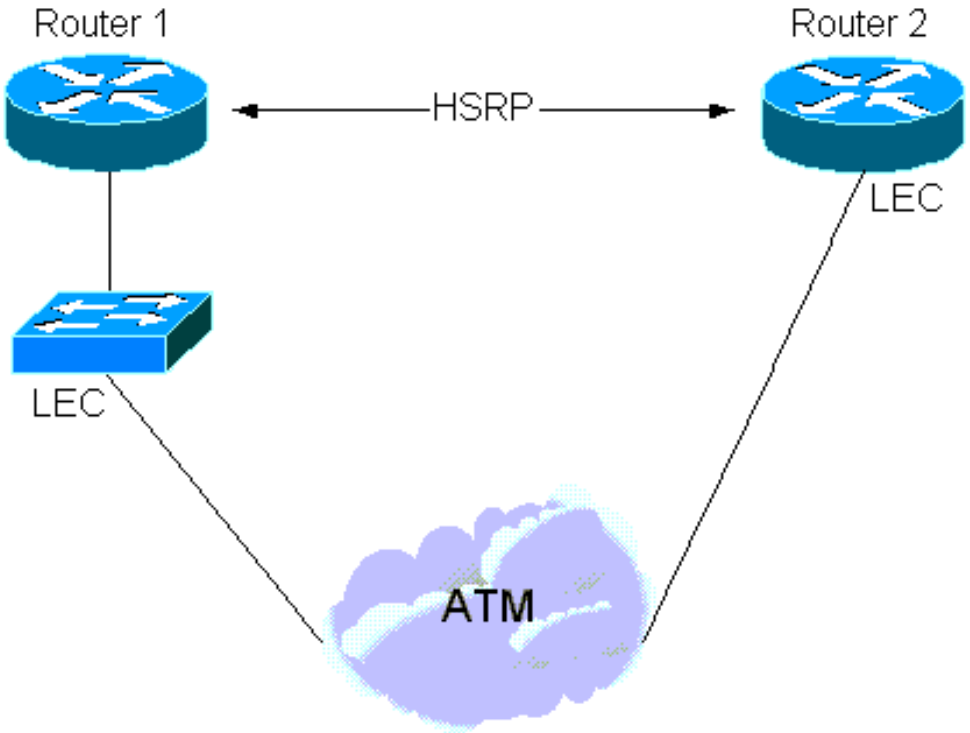
1. A partire dal software Cisco IOS® versione 11.2, HSRP può essere eseguito "in modo nativo" su LANE. In questo caso, i comandi di **standby** vengono configurati direttamente sulle sottointerfacce ATM in cui risiedono i client di emulazione LAN (LEC). Vedere l'illustrazione seguente.



2. Esiste anche un'istanza in cui HSRP è configurato sulle interfacce LAN, ma parte della subnet si estende su un cloud LANE. A tale scopo, è necessario usare uno switch LAN con interfaccia ATM (ad esempio, Cisco Catalyst 5000 con modulo LANE). Vedere l'illustrazione seguente.



3. Infine, una situazione "ibrida" prevede che alcuni router HSRP siano collegati alla LAN e altri che si trovino su una LAN dietro uno switch
   LAN.



Case study

1) HSRP nativo su LANE

I router che partecipano all'HSRP inviano pacchetti "hello" sul supporto di broadcast per scambiarsi informazioni e selezionare i router attivi e in standby. Questi pacchetti vengono inviati all'indirizzo multicast 24.0.0.2 con un valore TTL (Time to Live) pari a 1 e un indirizzo MAC di destinazione multicast pari a 0100 5E00 0002.

LANE non introduce nuovi problemi, quindi i dettagli descritti nella RFC 2281 sono ancora applicabili attraverso lo scambio di pacchetti di salve, colpo di stato e dimissioni, e vengono selezionati i router attivi e in standby.

I pacchetti hello vengono inviati sul bus (Broadcast and Unknown Server) e di seguito viene riportato ciò che un **pacchetto ATM di debug** (sul circuito virtuale Multicast Forward [VC]) e un **standby di debug** rivelerebbero:

```
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
```

Èimportante esaminare ciò che il client di emulazione LAN (LEC) riceve tramite il BUS (ad

esempio, tramite il 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
```

Questo dump esadecimale si traduce in:

```
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
```

Ciò che è degno di nota è che i pacchetti hello vengono originati dal router attivo con l'indirizzo MAC virtuale (VMAC) come indirizzo MAC di origine. Ciò è consigliabile perché i bridge di apprendimento (switch) che inoltrano questi pacchetti aggiorneranno la tabella CAM (Content-Addressable Memory) con la posizione appropriata del VMAC.

La chiave per l'HSRP si trova nel mapping tra un indirizzo IP e un indirizzo MAC.

Nella più semplice delle espressioni, l'indirizzo IP virtuale è associato in modo permanente a un indirizzo MAC virtuale e l'unico aspetto di cui preoccuparsi è che gli switch sanno sempre dove si trova questo indirizzo MAC virtuale. Ciò è garantito dal fatto che gli helper provengono dal 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
```

In alternativa, i router utilizzano gli indirizzi incorporati (**uso standby-bia**) mappati all'indirizzo IP virtuale. In questo caso, il mapping tra l'indirizzo IP virtuale e l'indirizzo MAC cambia nel tempo: il router appena attivo invia un protocollo ARP (Address Resolution Protocol) per annunciare il nuovo mapping tra gli indirizzi IP virtuali e MAC. Una ARP è semplicemente una risposta ARP non richiesta.-

Nota: alcuni stack IP (meno recenti) potrebbero non comprendere gli 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
```

Nota: per introdurre LANE, la chiave è che oltre al mapping degli indirizzi IP-MAC virtuali, è necessario tenere conto del mapping degli indirizzi NSAP (VMAC-to-Network-Service-Access-Point). Questa mappatura viene semplicemente risolta tramite il processo LE-ARP (LAN Emulation-Address Resolution Protocol): un LEC che desidera inviare il traffico al gateway attivo utilizzerà LE-ARP per il VMAC (o l'indirizzo MAC fisico se si utilizza il BIA).

Considerare ora cosa succede quando un nuovo router diventa attivo: affinché i LEC siano informati della nuova posizione del gateway attivo (nuova mappatura da VMAC a NSAP), è necessario modificare la tabella LE-ARP. Per impostazione predefinita, le voci LE-ARP scadono ogni cinque minuti ma, nella maggior parte dei casi, fare affidamento su questo timeout è inaccettabile. La convergenza deve essere più rapida. La soluzione dipende dal fatto che il LEC presuma che il nuovo stato Attivo esegua LANE versione 1 o versione 2 (per le specifiche LANE, vedere ATM Forum.com):

- **LANE versione 1**Quando un router diventa attivo, in aggiunta ai passaggi descritti nella RFC 2281 , invia un LE-NARP per comunicare il nuovo binding tra indirizzi VMAC e NSAP. In base alle specifiche LANE, una volta ricevuto un LE-NARP, un LEC può scegliere di cancellare o aggiornare la voce LE-ARP corrispondente all'indirizzo MAC. La tendenza all'interno di Cisco è quella di adottare un approccio più conservativo e scegliere di cancellare la voce LE-ARP; in questo modo, il LEC cambierà immediatamente LE-ARP senza dover attendere il timeout di cinque minuti.**Nota:** questa soluzione potrebbe causare il problema di compatibilità descritto di seguito.
- **LANE versione 2**Nella versione 2 di LANE, sono state risolte alcune carenze della versione 1 di LANE: Le-NARP è stato sostituito da LE-ARP senza obiettivo e le-NARP senza sorgente. Il target-less LE-ARP può essere visto come un veicolo per pubblicizzare nuovi binding, mentre lo scopo del non-source LE-NARP è quello di rendere obsoleto un indirizzo MAC-to-NSAP esistente. In questo modo, se un router passa da Standby ad Active, invia un LE-ARP senza destinazione (utilizzato per annunciare un mapping da MAC a NSAP) e, se passa da Active a Standby, invia un LE-NARP senza origine (utilizzato per rendere obsoleto un binding da MAC

a NSAP).

Problema - Interoperabilità

C'è un problema che spesso si presenta abbastanza da meritare un esame più approfondito. Le specifiche LANE versione 1 stabiliscono che LE-NARP deve specificare il "vecchio binding", che viene reso obsoleto specificando il (vecchio) indirizzo Target NSAP (T-NSAP). In genere, i router che partecipano a HSRP non gestiscono i reciproci indirizzi dati.

Pertanto, il router appena attivo non conosce queste informazioni e sceglierà di non completare il campo perché non ne sa di più. Si tratta di una lieve violazione delle specifiche e alcuni fornitori ignoreranno questi pacchetti se il campo dell'indirizzo T-NSAP è composto interamente da zeri. Sfortunatamente, non esistono soluzioni alternative per questo problema. Se le-NARP vengono ignorate, è necessario attenersi al timeout LE-ARP (generalmente cinque minuti) prima di apprendere il binding corretto.

Quando si invia un LE-ARP o LE-NARP con un campo di indirizzo T-NSAP composto da tutti gli zeri, il campo viene denominato "targetless" (senza destinazione). Come si è visto in precedenza, con l'avvento di LANE versione 2 (e Multiprotocol over ATM [MPOA]), questo è diventato standard e il problema cessa di esistere.

Questo è quanto viene fatto in LANE versione 1 dove possono verificarsi problemi:

- Se il router conosce il "vecchio binding", potrebbe anche rispettare le specifiche. A questo punto, vengono eseguiti i seguenti debug su 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)
```

- Se non conosce il "vecchio legame", fa del suo meglio e almeno pubblicizza quello nuovo:

```
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
```

  Nota: questa volta l'indirizzo T-NSAP è vuoto.

Anche in questo caso, il comportamento è completamente conforme alle specifiche quando si utilizzano client LANE versione 2.

Nota: il software che supporta MPOA supporta anche LANE versione 2.

Suggerimenti per la risoluzione dei problemi

L'HSRP nativo su LANE non dovrebbe generare troppi problemi oltre al potenziale problema di interoperabilità dovuto alla mancanza di LE-NARP del T-NSAP.

Se i router hanno difficoltà a stabilire se sono attivi o in standby, usare il comando **debug standby** per verificare se gli helper sono visibili su entrambi i lati. In caso contrario, è probabile che il BUS non stia inoltrando correttamente i pacchetti.

2) HSRP su router dietro LANE

La situazione diventa più complicata quando l'HSRP viene configurato sulle interfacce LANE dei router situati dietro un cloud LANE, come mostrato nella Figura 2.

Nota: la figura mostra logicamente il router non ATM collegato. non deve necessariamente trovarsi su un dispositivo separato rispetto allo switch LAN (in questo caso, è presente un Route Switch Module (RSM) di Cisco Catalyst 5000).

Anche in questo caso, la difficoltà è dovuta alla mappatura degli indirizzi da indirizzo MAC a NSAP imposta da LANE. Come accennato in precedenza, quando il VMAC passa a un dispositivo (quando un nuovo router diventa attivo) che corrisponde a un altro indirizzo NSAP, tutti i dispositivi collegati al cloud LANE devono essere informati. Ciò viene implementato abbastanza facilmente in un ambiente HSRP nativo su LANE utilizzando LE-NARP (o LE-ARP senza destinazione).

Il problema in questo secondo caso è che i LEC non sono a conoscenza di alcuna informazione di layer 3 (IP), sono progettati esclusivamente per collegare pacchetti tra due diversi supporti (LAN e ATM).

Ad esempio, nella Figura 2, se il router 2 diventa improvvisamente attivo, è consigliabile che lo switch LAN 2 informi tutti i dispositivi connessi al cloud ATM (LANE) della nuova mappatura VMAC-NSAP. Il LEC nello switch LAN 2 viene definito proxy per tutti gli indirizzi MAC sottostanti. I dispositivi nella rete LANE che desiderano inviare traffico a questi indirizzi MAC devono farlo tramite una configurazione data-direct verso questo LEC. Intuitivamente, si potrebbe pensare che questo non sarà un grande problema, poiché, non appena il router 2 si assume lo stato Active, inizierà a ricevere gli hellos con il VMAC come indirizzo MAC di origine. Queste informazioni verrebbero quindi acquisite da tutti gli switch LAN e tutto convergerebbe rapidamente. Ciò è vero in ambienti non LANE, ma LANE è speciale per il seguente motivo:

In LANE, un pacchetto dati può in genere essere trasmesso attraverso due percorsi:

- Data-Direct se il pacchetto è un unicast per il quale la destinazione è stata mappata a un NSAP noto e se il data-direct è già stato stabilito.
- BUS per unicast e multicast sconosciuti.

Pertanto, uno stesso indirizzo MAC genererà pacchetti che verranno ricevuti da uno switch LAN su due percorsi diversi. I multicast e gli unicast sconosciuti arriveranno tramite il BUS, mentre gli unicast noti arriveranno tramite data-direct. Se non è stato fatto alcuno sforzo particolare, uno switch LAN continua ad apprendere questo indirizzo MAC su un data-direct o sul BUS a seconda dell'ultimo pacchetto ricevuto. Ciò non è opportuno perché il bus deve essere utilizzato solo per inviare pacchetti per unicast o multicast sconosciuti. In questa fase, non si impara nulla con il BUS, ma in realtà, scegliere di fare quanto segue:

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.

Per tornare all'esempio, si presume che tutti i LEC nella ELAN siano già a conoscenza del mapping VMAC-NSAP per il router 1 prima che il router 2 diventi attivo. Tutti gli switch LAN sanno anche che il VMAC è dietro lo switch LAN 1. Quando il router 2 diventa attivo e l'origine dei pacchetti hello, questi vengono inoltrati al cloud LANE tramite il BUS. Pertanto, nessuno switch LAN aggiorna le proprie tabelle CAM con le nuove informazioni e tutti i pacchetti inviati a questo VMAC verranno indirizzati in modo errato finché gli switch LAN non "dimenticano" questa voce (l'impostazione predefinita è 5 minuti).

Nota: la connettività complessiva potrebbe in realtà andare persa per un massimo di 10 minuti poiché anche il timer di aging LE-ARP sui LEC è di 5 minuti per impostazione predefinita. Ridurre il timer di aging per gli indirizzi MAC è utile, ma non consente di risolvere il problema.

Le soluzioni possibili sono due:

1. Se gli switch LAN non sono Cisco, ripristinare un metodo descritto sopra: utilizzando l'indirizzo incorporato. Se i router utilizzano il proprio indirizzo MAC solo per l'origine dei pacchetti hello e l'indirizzo IP virtuale cambia mapping ogni volta che si verifica un passaggio, non c'è confusione sulla posizione di questi indirizzi MAC.
2. Se gli switch LAN sono Cisco Catalyst, continuare a usare il VMAC a causa delle modifiche fornite dal Distributed Defect Tracking System (DTS) descritto negli ID bug Cisco CSCdj58719 (solo utenti registrati) e CSCdj60431 (solo utenti registrati).In sostanza, quando un router assume lo stato Active, in aggiunta alla risposta ARP (ARP non richiesta) che invia in conformità alla RFC 2281 , invia un secondo ARP con un indirizzo MAC di destinazione di 100.0CCD.CCD. Quando un Cisco Catalyst riceve questo pacchetto, svolge due attività:Cancella la voce LE-ARP per VMAC.Impara il VMAC sul BUS.

Per questo motivo, non ci sono più voci LE-ARP obsolete nei vari LEC e la nuova posizione del VMAC viene propagata a tutti gli switch (ad esempio, oltre il cloud LANE). Per il corretto funzionamento di questa funzionalità, è necessario che siano soddisfatti i seguenti requisiti software minimi:

- I router devono avere almeno il software Cisco IOS versione 11.1(24), versione 11.2(13) o tutta la versione 12.0.
- I moduli LANE devono avere almeno la versione 3.2(8). 11.3W4 e versioni successive sono accettabili.

Cisco consiglia di utilizzare il software più recente.

3) Ambiente misto

C'è un ultimo problema che può sorgere in ambienti misti. Sulla base dello scenario precedente e aggiungendo un dispositivo terminale LANE a connessione diretta (router o workstation), il dispositivo terminale deve essere informato di un cambiamento di posizione del gateway attivo nello stesso modo in cui si trova nello scenario 1. Se il router appena attivo è connesso dietro uno switch, l'unica soluzione è che lo switch stesso invii il comando LE-NARP per conto del router e questa è esattamente la cosa da fare.

Oltre ai passaggi descritti in precedenza, se un Cisco Catalyst riceve un pacchetto destinato a 1000.000 CCD, invia un LE-NARP (le-NARP non sorgente con LANE versione 2), il cui unico scopo è cancellare le cache LE-ARP per il VMAC.

Conclusioni

Come dimostrato, l'HSRP su LANE funziona bene in linea di principio ma, in determinate circostanze, gli utenti possono perdere la connettività per brevi periodi se rientrano in una delle scappatoie descritte sopra.

Importante!: Per garantire il successo dell'HSRP su LANE, attenersi almeno alle seguenti due raccomandazioni:

- Per sicurezza, eseguire l'aggiornamento almeno all'ultima versione del software Cisco IOS versione 12.0.
- Negli ambienti multivendor, è preferibile utilizzare LANE versione 2 o l'indirizzo incorporato per evitare problemi.

Informazioni correlate

- Pagine di supporto per la tecnologia ATM
- Supporto tecnico – Cisco Systems