Implementación de HSRP Sobre LANE

Contenido

Introducción

El propósito de este documento es delinear los problemas que pueden ser encontrados al implementar el Hot Standby Router Protocol (HSRP) en un entorno del LAN Emulation (LANE). Describe muchos de los específicos del HSRP over LANE y proporciona los consejos de Troubleshooting para los diversos escenarios.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

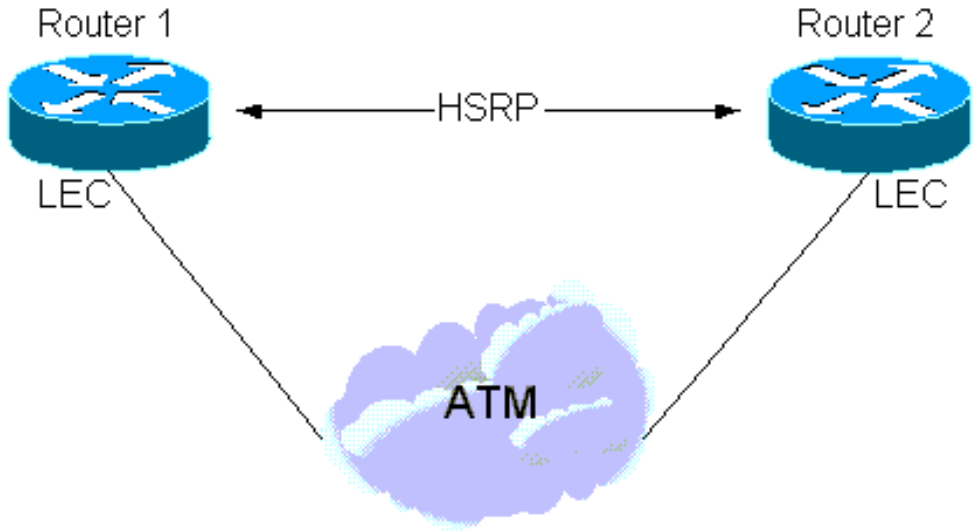
Antecedentes

En resumen, el propósito del HSRP es permitir que los host en una subred utilicen a un solo router “virtual” como el default gateway – los routeres múltiples participan en el protocolo HSRP para elegir al router activo, que asume el papel del default gateway y de un router de backup en caso de que el activo falle. El resultado es que el default gateway aparecerá siempre estar para arriba incluso si el primer router de saltos físico cambia. Una descripción completa del HSRP se puede encontrar en el RFC 2281 .

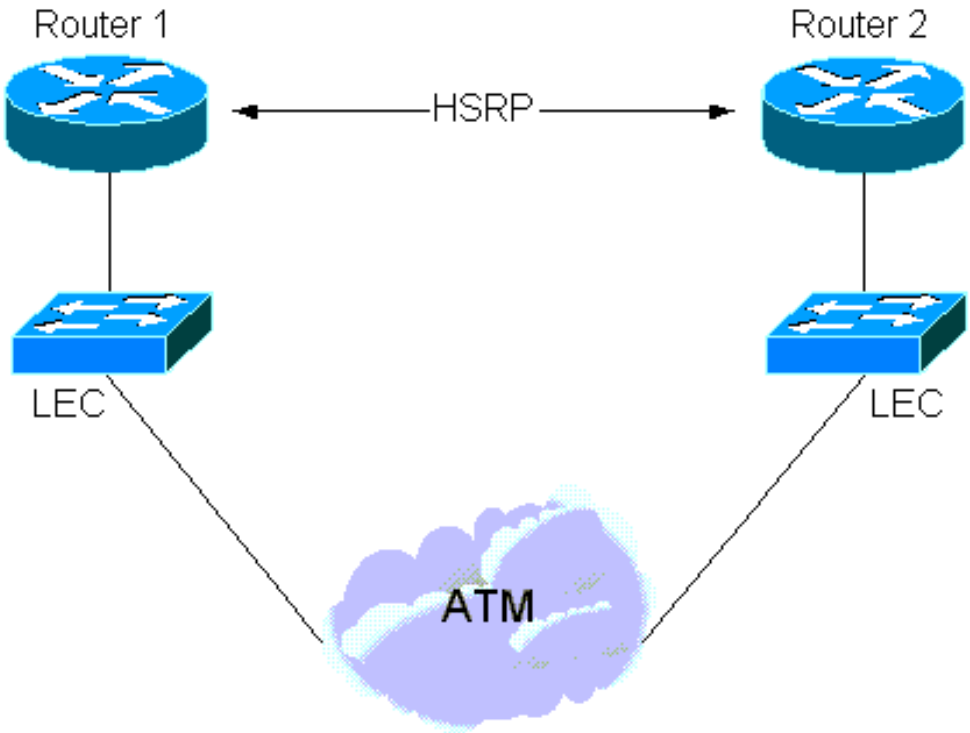
El HSRP fue diseñado para el uso sobre multiacceso, el Multicast, o el broadcast LAN capaces (típicamente [FDDI] de los Ethernetes, del Token Ring, o del Fiber Distributed Data Interface). Por lo tanto, el HSRP debe trabajar bastante por encima del LANE ATM.

Varias situaciones que implican el HSRP y la interacción LANE pueden presentarse:

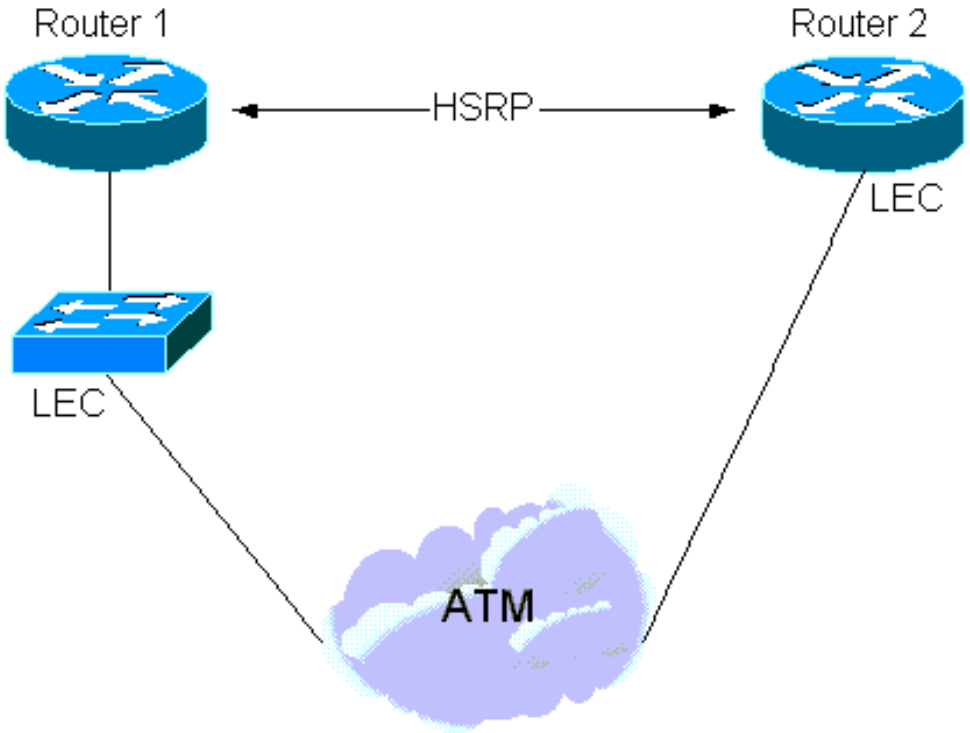
1. Desde el Software Release 11.2 de Cisco IOS®, el HSRP puede ejecutarse “nativo” sobre el LANE. En este caso, configuran a los **comandos standby** directamente en las subinterfaces ATM donde reside el (LECs) de los LAN Emulation Clients. Vea el ejemplo siguiente.



2. También hay un caso donde el HSRP se configura en las interfaces LAN, pero la parte de la subred atraviesa una nube de LANe. Esto es lograda por el intermedio de un switch LAN con una interfaz ATM (tal como un Cisco Catalyst 5000 con un módulo LANE). Vea el ejemplo siguiente.



3. Finalmente, hay una situación “híbrida” donde LANE-asocian a algunos routers del HSRP y otros están en un LAN detrás de un switch
   LAN.



Estudios de casos

1) HSRP over LANE nativo

El Routers que participa en el HSRP envía “hola” los paquetes sobre el medio de broadcast para aprender sobre uno a y elegir el active y a los routeres en espera. Estos paquetes se envían a la dirección Multicast 224.0.0.2 con un Time to Live (TTL) de 1 y una dirección MAC del destino multidifusión de 0100 5E00 0002.

El LANE no introduce ningún nuevo problema aquí así que los detalles descritos en el RFC 2281 todavía se aplican – con el intercambio de hola, el golpe, y dimiten los paquetes, el active y eligen a los routeres en espera.

Los paquetes de saludo se envían sobre el broadcast y servidor desconocidos (BUS) y lo que sigue es lo que un **paquete del debug ATM** (en el [VC] delantero del circuito virtual del Multicast) y un **recurso seguro del debug** revelaría:

```
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
```

De la importancia está mirando qué el (LEC) del LAN Emulation Client recibe sobre el BUS (por ejemplo, por el Multicast adelante):

```
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
```

Este vaciado Hex traduce al siguiente:

```
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
```

Cuál es significativo es que los paquetes de saludo son originados por el router activo con el MAC address virtual (VMAC) como MAC Address de origen – esto es deseable porque los Learning Bridge (Switches) que remiten estos paquetes pondrán al día su tabla de la memoria de contenido direccionable (CAM) con la ubicación apropiada del VMAC.

La clave al HSRP miente dentro de la asignación entre una dirección IP y una dirección MAC.

En la expresión más simple, la dirección IP virtual está limitada permanentemente a una dirección MAC virtual y el único aspecto a preocuparse alrededor es que el Switches sabe siempre dónde

se localiza esta dirección MAC virtual. Se asegura esto porque el hellos es originado por el 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
```

Otra opción es que el Routers utiliza su quemar-en los direccionamientos (uso-**BIA espera**) asociados a la dirección IP virtual. En este caso, la asignación en medio IP virtual y cambios de la dirección MAC en un cierto plazo – el router activo envía nuevamente un Address Resolution Protocol (ARP) para anunciar la nueva correspondencia de direcciones virtual IP-a-MAC. Un ARP es simplemente una respuesta ARP no solicitada. -

Nota: Ciertas pilas IP (más viejas) pueden no entender los 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: Para introducir el LANE, la clave es ésa encima de la correspondencia de direcciones virtual IP-a-MAC, allí debe explicar la correspondencia de direcciones de la VMAC-a-Red-Servicio-Acceso-punta (NSAP). Esta asignación se resuelve simplemente con el proceso del protocolo lan emulation address resolution (LE-ARP): un LEC que desea enviar el tráfico al gateway activo utilizará el LE-ARP para el VMAC (o la MAC física si usa el [BIA] del Burned-In MAC Address).

Ahora considere qué sucede cuando un nuevo router hace activo: para que los LEC sean informados la nueva ubicación del gateway activo (nueva mapeo de VMAC a NSAP), la tabla LE-ARP debe ser modificada. Por abandono, las entradas del LE-ARP miden el tiempo hacia fuera de cada cinco minutos pero, en la mayoría de los casos, la confianza en este descanso es inaceptable – la convergencia debe ser más rápida. La solución depende encendido si el LEC si se asume que el nuevo estado activo es la versión LANE corriente 1 o versión 2 (véase la atmósfera Forum.com para las especificaciones de LANe):

- **Versión LANE 1**Cuando un router hace activo, además de los pasos descritos en el RFC 2281 , envía un LE-NARP para hacer la nueva vinculación de dirección VMAC-a-NSAP sabida. Según las especificaciones de LANe, tras la recepción de un LE-NARP, un LEC puede elegir borrar o poner al día la entrada del LE-ARP correspondiente a la dirección MAC. La tendencia dentro de Cisco es adoptar el más enfoque conservador y elegir borrar la entrada del LE-ARP – ésta causará el LEC inmediatamente al re-LE-ARP sin tener que esperar el descanso del minuto cinco.**Nota:** Esta solución puede causar los problemas de compatibilidad descritos más abajo.
- **Versión LANE 2**En la versión LANE 2, ciertos defectos de la versión LANE 1 fueron paliados: el LE-NARP ha sido reemplazado por el LE-ARP targetless y la ninguno-fuente LE-NARP. El LE-ARP targetless se puede considerar como vehículo para hacer publicidad de los nuevos atascamientos mientras que el propósito de la ninguno-fuente el LE-NARP es rendir Obsoleto una vinculación de dirección existente MAC-a-NSAP. La manera que se implementa esto es que si un router cambia de espera al Active, envía un LE-ARP targetless (ésta se utiliza para hacer publicidad de una asignación de MAC a NSAP) y si cambia de activo al recurso seguro, él envía una ninguno-fuente LE-NARP (ésta se utiliza para dejar una vinculación de MAC a NSAP Obsoleta).

Problema - Interoperabilidad

Hay un problema que se presenta a menudo bastante para merecer un examen más profundizado. Las especificaciones de la versión LANE 1 estado que el LE-NARP debe especificar el “atascamiento viejo,” que está siendo hecho Obsoleto especificando (el viejo) direccionamiento de la blanco NSAP (el T-NSAP). Típicamente, el Routers que participa en el HSRP no mantiene las vías directas de datos entre uno a.

Por lo tanto, el router activo no sabe nuevamente que esta información y ella elegirá no completar este campo puesto que no sabe mejor. Ésta es una violación menor de las especificaciones y algunos vendedores ignorarán estos paquetes si el campo de dirección T-NSAP es todos los ceros. Desafortunadamente, no hay solución alternativa para esto – si se ignora el LE-NARP, confíe en el descanso del LE-ARP (típicamente cinco minutos) antes de que el atascamiento correcto sea docto.

Cuando un LE-ARP o un LE-NARP se envía con un campo de dirección T-NSAP de todos los ceros, se llama “targetless.” Según lo visto arriba, con la llegada del [MPOA] de la versión LANE 2 (y del multiprotocolo sobre ATM), esto tiene estándar convertido y el problema deja de existir.

Esto es qué se hace en la versión LANE 1 donde los problemas pueden presentarse:

- Si el router conoce el “atascamiento viejo,” puede ser que también obedezca las especificaciones. Estos debugs ahora se adquieren el control distribuyen el 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)
```
- Si no conoce el “atascamiento viejo,” hace su mejor y por lo menos hace publicidad del nuevo:`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: Esta vez la dirección de T-NSAP es en blanco.

Una vez más el comportamiento está totalmente dentro de lo especificado al usar a los clientes de la versión LANE 2.

Nota: El software que soporta el MPOA también soporta la versión LANE 2.

Consejos de Troubleshooting

El HSRP over LANE nativo no debe engendrar demasiados problemas con excepción del problema de interoperabilidad potencial debido al LE-NARP falto del T-NSAP.

Si el Routers tiene dificultad en el establecimiento de si él es activo o espera, utilice el **comando debug standby** de ver si el hellos se ve en los ambos lados. Si no, entonces el BUS no está remitiendo probablemente correctamente los paquetes.

2) HSRP sobre el Routers detrás del LANE

La situación llega a ser más complicada cuando el HSRP se configura en las interfaces LANE del Routers situado detrás de una nube de LANe, como se ilustra en el cuadro 2.

Nota: Esta figura representa lógicamente el hecho de que el router es no ATM asociado. No tiene que necesariamente estar en un dispositivo separado al switch LAN (un [RSM] del Route Switch Module en un Cisco Catalyst 5000 baja bajo este caso).

Una vez más la dificultad se presenta debido a la asignación del MAC-direccionamiento-a-NSAP-direccionamiento impuesta por el LANE. Según lo observado arriba, cuando el Switches VMAC a un dispositivo (cuando un nuevo router hace activo) que corresponde a otro NSAP Address, todos los dispositivos asociados a la nube de LANe debe ser informado. Esto se implementa bastante fácilmente en un entorno nativo del HSRP over LANE usando el LE-NARP (o el LE-ARP targetless).

El problema en este segundo caso es que los LEC no son conscientes de ninguna información de la capa 3 (IP), ellos se diseña solamente a los Bridge Packet entre dos diversos media (el LAN y la atmósfera).

Por ejemplo, en el cuadro 2, si el router2 llegó a ser repentinamente activo, después sería deseable que el switch LAN 2 informe a todos los dispositivos conectados con la nube atmósfera (LANE) sobre el nuevo mapeo de VMAC a NSAP. El LEC en el switch LAN 2 reputa el envío a través de proxy para todas las direcciones MAC que están detrás de él. Los dispositivos a través del LANE que desea enviar el tráfico a estas direcciones MAC deben hacer tan por una configuración vía directa de datos hacia este LEC. Intuitivo, uno podría pensar que esto no será un problema grande puesto que, tan pronto como el router2 asuma el estado activo, comenzará el hellos de la compra de componentes con el VMAC como el MAC Address de origen. Esta información entonces sería aprendida por todos los switches LAN y todo convergería rápidamente. Esto es verdad en los entornos NON-LANE, pero el LANE es especial por la razón siguiente:

En el LANE, un paquete de datos se puede transmitir generalmente a través de dos trayectorias:

- El vía directa de datos si este paquete es un unicast para las cuales el destino se ha asociado a un NSAP sabido y si el vía directa de datos se ha establecido ya.
- El BUS para las unidifusiones desconocidas y los Multicast.

Por lo tanto, una misma dirección MAC los paquetes de origen que serán recibidos por un switch LAN sobre dos diversas trayectorias. Los Multicast y las unidifusiones desconocidas llegarán por el BUS mientras que el unicasts sabido llega por las vías directas de datos. Si no se hubiera hecho ningún esfuerzo en particular, un switch LAN guardaría el aprender de esta dirección MAC sobre un vía directa de datos o sobre el BUS dependiendo del paquete más reciente recibido. Esto es indeseable porque el BUS se debe utilizar solamente para enviar los paquetes para las unidifusiones desconocidas o los Multicast. En esta etapa, nada es docto sobre el BUS, pero en la realidad, elige hacer el siguiente:

```
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.

Para volver al ejemplo, es seguro asumir que todos los LEC en este ELAN son ya conscientes del mapeo de VMAC-NSAP para el router1 antes de cuando el router2 llega a ser activo. Todos los switches LAN también saben que el VMAC está detrás del switch LAN 1. Cuando el router2 se convierte en Active y fuentes los paquetes de saludo, éstos se remiten a la nube de LANe sobre el BUS. Por lo tanto, ningunos de los switches LAN pondrán al día sus tablas CAM con esta nueva información y todos los paquetes enviados a este VMAC serán dirigidos mal hasta que los switches LAN “olviden” esta entrada (el envejecimiento predeterminado que es cinco minutos).

Nota: La conectividad general se pudo perder realmente por hasta 10 minutos puesto que el LE-ARP Temporizador de desactualización en los LEC también es cinco minutos por abandono. La reducción Temporizador de desactualización para las direcciones MAC ayudará, pero no resuelve realmente al problema.

Hay dos soluciones para esto:

1. Si los switches LAN son no Cisco, invierta a un método descrito arriba: usando la dirección impresa a fuego. Si el Routers utiliza solamente su dirección MAC a la fuente los paquetes de saludo y eso la dirección IP virtual cambia la asignación siempre que ocurra a Switch-sobre, no hay confusión posible en cuanto a donde se localizan estas direcciones MAC.
2. Si los switches LAN son Catalyst de Cisco, después mantenga el usar del VMAC debido a las modificaciones proporcionadas por el Distributed Defect Tracking System (DDTS) cubierto el bug Cisco ID CSCdj58719 (clientes registrados solamente) y CSCdj60431 (clientes registrados solamente).Esencialmente, cuando un router asume el estado activo, además del ARP (respuesta ARP no solicitada) ese envía de acuerdo con el RFC 2281 , el router envía un segundo ARP con una dirección MAC del destino de 0100.0CCD.CDCD. Cuando un Cisco Catalyst recibe este paquete hace dos cosas:Borra la entrada del LE-ARP que tiene para el VMAC.Aprende el VMAC sobre el BUS.

Debido a esto, no hay entradas añejas del LE-ARP en los diversos LEC y la nueva ubicación del VMAC se propaga a todo el Switches (por ejemplo, más allá de la nube de LANe). Para que esto trabaje correctamente, los requisitos mínimos de software siguientes deben ser cumplidos:

- El Routers debe tener por lo menos el Cisco IOS Software Release 11.1(24), la versión 11.2(13), o toda la versión 12.0.
- Los módulos LANE deben tener por lo menos versión 3.2(8). las versiones 11.3W4 y posterior son aceptables.

Cisco recomienda el usar del último software.

3) Entorno mezclado

Hay un problema final que puede presentarse en los entornos mezclados. Tomando el escenario arriba y agregando un dispositivo final directamente conectado LANE (router o puesto de trabajo), el dispositivo final necesita ser informado sobre un cambio de ubicación del gateway activo la misma manera que en el escenario 1. Si el router activo está conectado nuevamente detrás de un Switch, la única solución está para el Switch sí mismo para enviar el LE-NARP en nombre del router y es exactamente cuál esto a hacer.

Además de los pasos descritos arriba, si un Cisco Catalyst coge un paquete destinado a 0100 0CCD CDCD, envía un LE-NARP (ninguno-fuente LE-NARP si funciona con la versión LANE 2), que su único propósito es borrar los cachés del LE-ARP para el VMAC.

Conclusión

Según lo demostrado, el HSRP over LANE trabaja bien en principio pero, en determinadas circunstancias, los usuarios pueden perder la Conectividad por los períodos cortos si caen en una de las escapatorias descritas arriba.

Importante: Para asegurar el éxito con el HSRP over LANE, siga por lo menos estas dos recomendaciones:

- Para ser seguro, actualice por lo menos a la última versión de Cisco IOS Software Release 12.0.
- En los entornos del mult-vendedor, es el mejor utilizar la versión LANE 2 o a la dirección impresa a fuego para evitar los problemas.

Información Relacionada

- Páginas de soporte de la tecnología ATM
- Soporte Técnico - Cisco Systems