Implementación de HSRP Sobre LANE

Contenido

Introducción

El propósito de este documento es describir los problemas que pueden surgir al implementar el protocolo de router con espera activa (HSRP) en un entorno de LAN Emulation (LANE). Describe muchos de los aspectos específicos de HSRP sobre LANE y proporciona consejos para la resolución de problemas en varios escenarios.

Prerequisites

Requirements

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.

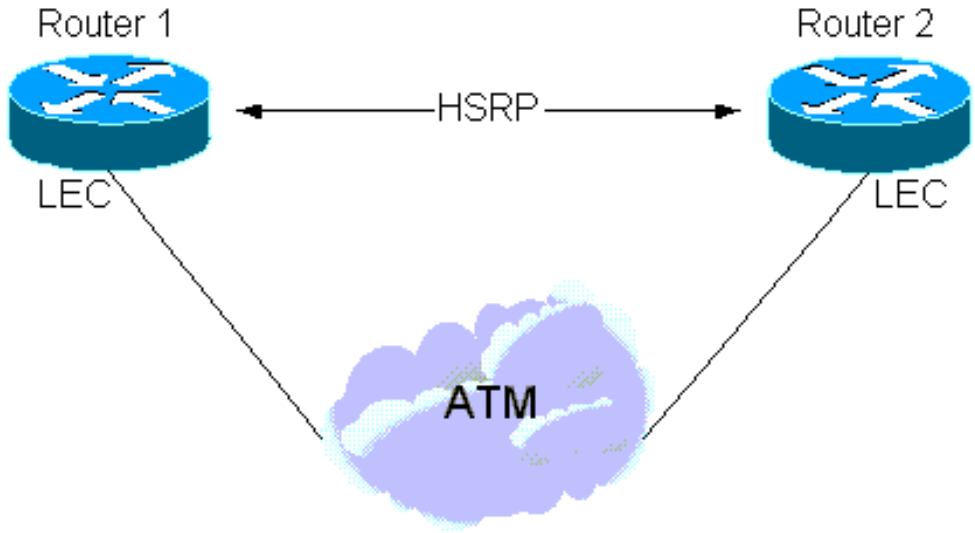
Antecedentes

En resumen, el propósito de HSRP es permitir que los hosts en una subred utilicen un único router "virtual" como los routers de gateway múltiple predeterminados participan en el protocolo HSRP para elegir el router activo, que asume el rol de gateway predeterminado y un router de respaldo en caso de que el activo falle. El resultado es que el gateway predeterminado siempre aparecerá activo aunque cambie el router físico de primer salto. Se puede encontrar una descripción completa de HSRP en RFC 2281 .

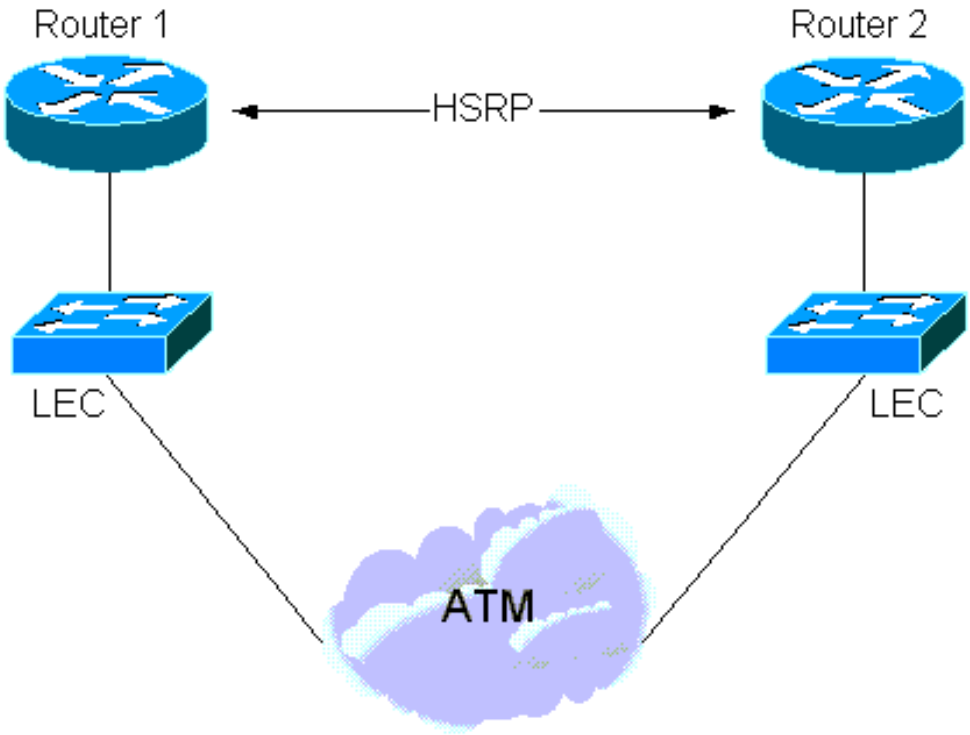
HSRP se diseñó para su uso en redes LAN con capacidad de broadcast, multidifusión o acceso múltiple (normalmente Ethernet, Token Ring o Fiber Distributed Data Interface [FDDI]). Por lo tanto, HSRP debería funcionar bien sobre ATM LANE.

Pueden surgir varias situaciones relacionadas con la interacción HSRP y LANE:

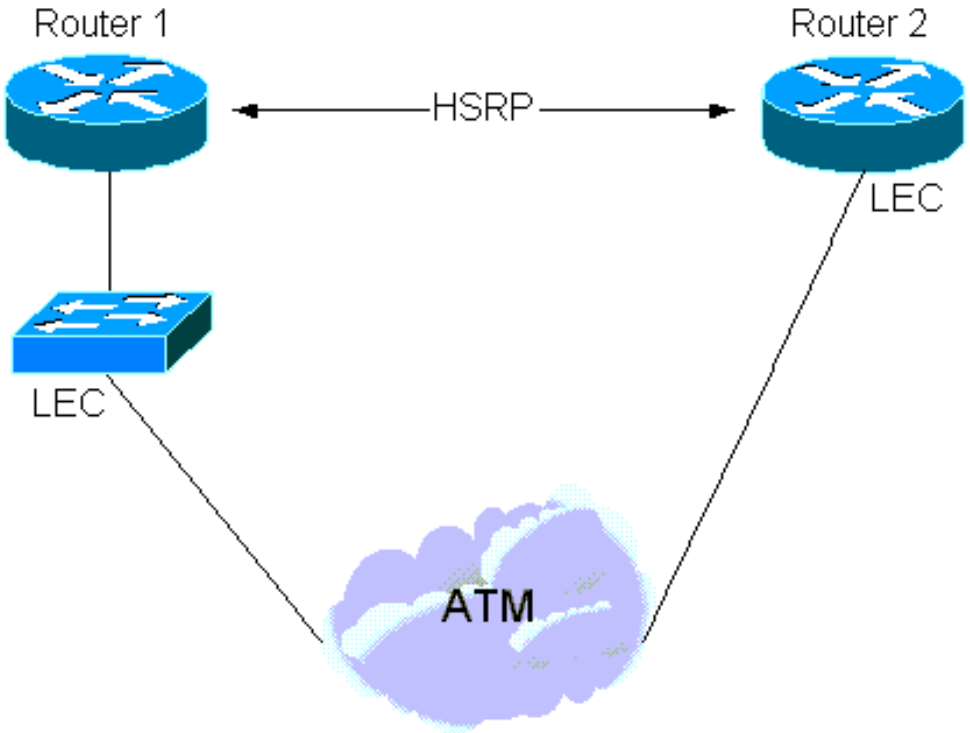
1. Desde la versión 11.2 del software del IOS® de Cisco, HSRP puede ejecutarse "nativamente" sobre LANE . En este caso, los comandos **standby** se configuran directamente en las subinterfaces ATM donde residen los clientes de emulación de LAN (LEC). Consulte la ilustración
   siguiente.



2. También hay una instancia en la que HSRP se configura en las interfaces LAN, pero parte de la subred abarca una nube LANE. Esto se logra mediante el intermedio de un switch LAN con una interfaz ATM (como un Cisco Catalyst 5000 con un módulo LANE). Consulte la ilustración
   siguiente.



3. Finalmente, hay una situación "híbrida" en la que algunos routers HSRP están conectados a LANE y otros están en una LAN detrás de un switch
   LAN.



Estudios de casos

1) HSRP nativo sobre LANE

Los routers que participan en HSRP envían paquetes de "saludo" a través del medio de difusión para aprender unos sobre otros y elegir los routers activos y en espera. Estos paquetes se envían a la dirección de multidifusión 224.0.0.2 con un tiempo de vida (TTL) de 1 y una dirección MAC de destino de multidifusión de 0100 5E00 002.

LANE no introduce nuevos problemas aquí, por lo que los detalles descritos en RFC 2281 todavía se aplican a través del intercambio de paquetes de saludo, golpe y renuncia, los routers activos y en espera son elegidos.

Los paquetes hello se envían a través del servidor de difusión y desconocido (BUS) y lo siguiente es lo que un **debug atm packet** (en el circuito virtual de reenvío multidifusión [VC]) y un **debug standby** revelarían:

```
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
```

Es importante observar lo que el cliente de emulación de LAN (LEC) recibe a través del BUS (por

ejemplo, a través del reenvío multidifusión):

```
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 hex-dump se traduce a lo 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
```

Lo que es digno de mención es que los paquetes hello son originados por el router activo con la dirección MAC virtual (VMAC) como dirección MAC de origen. Esto es deseable porque los puentes de aprendizaje (switches) que reenvían estos paquetes actualizarán su tabla de memoria direccionable por contenido (CAM) con la ubicación adecuada del VMAC.

La clave para HSRP se encuentra dentro del mapping entre una dirección IP y una dirección MAC.

En la expresión más simple, la dirección IP virtual se enlaza permanentemente a una dirección MAC virtual y el único aspecto que preocupa es que los switches siempre saben dónde se encuentra esta dirección MAC virtual. Esto se asegura porque los hellos son originados 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 los routers utilicen sus direcciones quemadas (**standby use-bia**) asignadas a la dirección IP virtual. En este caso, la asignación entre dirección MAC e IP virtual cambia con el tiempo. El router recientemente activo envía un protocolo de resolución de direcciones (ARP) para anunciar la nueva asignación de dirección IP a MAC virtual. Un ARP es simplemente una respuesta ARP no solicitada.-

Nota: Es posible que ciertas pilas IP (antiguas) no entiendan 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 LANE, la clave es que, además de la asignación de dirección IP a MAC virtual, debe haber contabilidad para la asignación de direcciones de punto de acceso de servicios de red (NSAP) a VMAC. Esta asignación se resuelve simplemente mediante el proceso de protocolo de resolución de direcciones de emulación de LAN (LE-ARP): un LEC que desee enviar tráfico al gateway activo utilizará LE-ARP para el VMAC (o MAC físico si utiliza la dirección MAC activada [BIA]).

Ahora considere qué sucede cuando un nuevo router se activa: para que se informe a los LEC de la nueva ubicación del gateway activo (nueva asignación VMAC a NSAP), se debe modificar la tabla LE-ARP. De forma predeterminada, las entradas LE-ARP se agotan cada cinco minutos pero, en la mayoría de los casos, confiar en este tiempo de espera es inaceptable-la convergencia debe ser más rápida. La solución depende de si el LEC que asume el nuevo estado activo está ejecutando LANE versión 1 o versión 2 (consulte ATM Forum.com para ver las especificaciones LANE):

- **LANE versión 1**Cuando un router se vuelve activo, además de los pasos descritos en RFC 2281 , envía un LE-NARP para dar a conocer el nuevo enlace de dirección VMAC a NSAP. Según las especificaciones LANE, cuando se recibe un LE-NARP, un LEC puede elegir borrar o actualizar la entrada LE-ARP correspondiente a la dirección MAC. La tendencia dentro de Cisco es adoptar el enfoque más conservador y elegir borrar la entrada LE-ARP; esto hará que el LEC vuelva a LE-ARP inmediatamente sin tener que esperar el tiempo de espera de cinco minutos.**Nota:** Esta solución puede causar el problema de compatibilidad descrito a continuación.
- **LANE versión 2**En LANE versión 2 se paliaron algunas deficiencias de LANE versión 1: el LE-NARP ha sido reemplazado por el LE-ARP sin objetivo y el LE-NARP sin origen. El LE-ARP sin objetivo puede verse como un vehículo para anunciar nuevos enlaces, mientras que el objetivo de LE-NARP sin fuente es hacer obsoleta una vinculación de dirección MAC a NSAP

existente. La forma en que esto se implementa es que si un router cambia de Standby a Active, envía un LE-ARP sin objetivos (esto se utiliza para anunciar una asignación de MAC a NSAP) y si cambia de Activo a En espera, envía un LE-NARP sin origen (esto se utiliza para hacer obsoleto un enlace de MAC a NSAP).

Problema - Interoperabilidad

Hay un problema que surge con frecuencia suficiente como para merecer un examen más a fondo. Las especificaciones LANE versión 1 establecen que LE-NARP debe especificar el "enlace antiguo", que se vuelve obsoleto al especificar la (antigua) dirección NSAP de destino (T-NSAP). Normalmente, los routers que participan en HSRP no mantienen direcciones de datos entre sí.

Por lo tanto, el router recientemente activo no conoce esta información y elegirá no completar este campo porque no sabe más. Esta es una leve violación de las especificaciones y algunos proveedores ignorarán estos paquetes si el campo de dirección T-NSAP es todo ceros. Desafortunadamente, no hay una solución alternativa para esto-si el LE-NARP se ignora, confíe en el tiempo de espera LE-ARP (generalmente cinco minutos) antes de que se detecte el enlace correcto.

Cuando se envía un LE-ARP o LE-NARP con un campo de dirección T-NSAP de todos ceros, se denomina "destino sin objetivo". Como se ha visto anteriormente, con la llegada de LANE versión 2 (y Multiprotocol over ATM [MPOA]), esto se ha convertido en estándar y el problema deja de existir.

Esto es lo que se hace en LANE versión 1 donde pueden surgir problemas:

- Si el router conoce el "enlace antiguo", también podría obedecer las especificaciones. Estas depuraciones se realizan ahora en el VC de distribución de control:

```
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 "enlace antiguo", hace lo mejor que puede y al menos anuncia el 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 T-NSAP está en blanco.

Una vez más, el comportamiento se ajusta completamente a las especificaciones cuando se

utilizan clientes LANE versión 2.

Nota: El software que admite MPOA también admite LANE versión 2.

Consejos de Troubleshooting

El HSRP nativo sobre LANE no debería generar demasiados problemas que no sean el problema potencial de interoperabilidad debido al LE-NARP desprovisto del T-NSAP.

Si los routers tienen dificultades para establecer si están activos o en espera, utilice el comando **debug standby** para ver si los saludos se ven en ambos lados. Si no es así, es probable que el BUS no reenvíe correctamente los paquetes.

2) HSRP sobre routers detrás de LANE

La situación se complica más cuando HSRP se configura en interfaces LANE de routers ubicados detrás de una nube LANE, como se ilustra en la Figura 2.

Nota: Esta figura representa lógicamente el hecho de que el router no está conectado a ATM. No tiene que estar necesariamente en un dispositivo separado del switch LAN (un Módulo de switch de ruta [RSM] en un Cisco Catalyst 5000 se incluye en este caso).

Una vez más, la dificultad surge debido al mapeo de direcciones MAC a direcciones NSAP impuesto por LANE. Como se indicó anteriormente, cuando el VMAC cambia a un dispositivo (cuando un nuevo router se activa) que corresponde a otra dirección NSAP, todos los dispositivos conectados a la nube LANE deben ser informados. Esto se implementa con bastante facilidad en un entorno HSRP sobre LANE nativo mediante el uso de LE-NARP (o LE-ARP sin destino).

El problema en este segundo caso es que los LEC no son conscientes de ninguna información de capa 3 (IP), están diseñados exclusivamente para conectar paquetes entre dos medios diferentes (la LAN y ATM).

Por ejemplo, en la Figura 2, si el Router 2 repentinamente se volvió Activo, sería deseable que el Switch LAN 2 informara a todos los dispositivos conectados a la nube ATM (LANE) sobre la nueva asignación VMAC a NSAP. Se dice que el LEC en el switch 2 de LAN está proxy para todas las direcciones MAC que están detrás de él. Los dispositivos en LANE que deseen enviar tráfico a estas direcciones MAC deben hacerlo mediante una configuración de datos directos hacia este LEC. Intuitivamente, se podría pensar que esto no será un gran problema ya que, tan pronto como el Router 2 asuma el estado Activo, comenzará a proveer saludos con el VMAC como la dirección MAC de origen. Esta información sería adquirida entonces por todos los switches LAN y todo convergiría rápidamente. Esto es cierto en entornos no LANE, pero LANE es especial por la siguiente razón:

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

- La dirección de datos si este paquete es una unidifusión para la cual el destino se ha mapeado a un NSAP conocido y si el data-direct ya se ha establecido.
- El BUS para unicasts y multicasts desconocidos.

Por lo tanto, una misma dirección MAC originará paquetes que serán recibidos por un switch LAN en dos trayectorias diferentes. A través del BUS llegarán multidifusión y unidifusión desconocida, mientras que las unicasts conocidas llegan por medio de direcciones de datos. Si no se hubiera

hecho un esfuerzo particular, un switch LAN seguiría aprendiendo esta dirección MAC a través de un data-direct o a través del BUS, dependiendo del último paquete recibido. Esto no es deseable porque el BUS sólo debe usarse para enviar paquetes para unicasts o multicasts desconocidos. En esta etapa, nada se aprende sobre el BUS, pero en realidad, eligen hacer lo 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 esta ELAN ya conocen la asignación VMAC-NSAP para el Router 1 antes de cuando el Router 2 se vuelva Activo. Todos los switches LAN también saben que VMAC está detrás del switch LAN 1. Cuando el Router 2 se vuelve Activo y origina los paquetes hello, éstos se reenvían a la nube LANE a través del BUS. Por lo tanto, ninguno de los switches LAN actualizará sus tablas CAM con esta nueva información y todos los paquetes enviados a este VMAC serán mal dirigidos hasta que los switches LAN "olviden" esta entrada (la antigüedad predeterminada es de cinco minutos).

Nota: La conectividad total puede perderse hasta 10 minutos, ya que el temporizador de envejecimiento LE-ARP en los LEC también es de cinco minutos de forma predeterminada. Reducir el temporizador de envejecimiento para las direcciones MAC ayudará, pero en realidad no resuelve el problema.

Hay dos soluciones para esto:

1. Si los switches LAN no son de Cisco, vuelva a un método descrito anteriormente: usando la dirección impresa a fuego. Si los routers sólo utilizan su dirección MAC para originar los paquetes hello y que la dirección IP virtual cambia la asignación cada vez que se produce un switch-over, no hay confusión sobre dónde se encuentran estas direcciones MAC.
2. Si los switches LAN son Catalyst de Cisco, siga usando el VMAC debido a las modificaciones proporcionadas por el Sistema de Seguimiento de Defectos Distribuidos (DDTS) cubierto en los ID de bug de Cisco CSCdj58719 (sólo clientes registrados) y CSCdj60431 (sólo clientes registrados).En esencia, cuando un router asume el estado Activo, además de la respuesta ARP (no solicitada) que envía de acuerdo con RFC 2281 , el router envía un segundo ARP con una dirección MAC de destino de 0100.0CCD.CDCD. Cuando un Cisco Catalyst recibe este paquete, hace dos cosas:Borra la entrada LE-ARP que tiene para el VMAC.Aprende el VMAC a través del BUS.

Debido a esto, no hay más entradas LE-ARP obsoletas en los diversos LEC y la nueva ubicación del VMAC se propaga a todos los switches (por ejemplo, más allá de la nube LANE). Para que esto funcione correctamente, deben cumplirse los siguientes requisitos mínimos de software:

- Los routers deben tener al menos la versión 11.1(24), la versión 11.2(13) o toda la versión 12.0 del software del IOS de Cisco.
- Los módulos LANE deben tener al menos la versión 3.2(8). Las versiones 11.3W4 y posteriores son aceptables.

Cisco recomienda utilizar el software más reciente.

3) Entorno mixto

Hay un problema final que puede surgir en entornos mixtos. Tomando el escenario anterior y añadiendo un dispositivo final LANE directamente conectado (router o estación de trabajo), el dispositivo final debe ser informado sobre un cambio de ubicación del gateway activo de la misma manera que en el escenario 1. Si el router recientemente activo está conectado detrás de un switch, la única solución es que el propio switch envíe el LE-NARP en nombre del router y esto es exactamente lo que se debe hacer.

Además de los pasos descritos anteriormente, si un Catalyst de Cisco recoge un paquete destinado al CDCD 0100 0CCD, envía un LE-NARP (no-source LE-NARP si ejecuta LANE versión 2), cuyo único propósito es despejar las memorias caché LE-ARP para el VMAC.

Conclusión

Como se ha demostrado, HSRP sobre LANE funciona bien en principio, pero, en determinadas circunstancias, los usuarios pueden perder la conectividad durante períodos cortos si caen en una de las lagunas descritas anteriormente.

Importante: Para asegurar el éxito con HSRP sobre LANE, siga al menos estas dos recomendaciones:

- Para estar a salvo, actualice a al menos la última versión de Cisco IOS Software Release 12.0.
- En entornos de varios proveedores, es mejor utilizar LANE versión 2 o la dirección impresa a fuego para evitar problemas.

Información Relacionada

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