Implementando HSRP sobre LANE

Contents

Introduction

A finalidade deste documento é destacar os problemas que podem ser encontrados ao implementar o HSRP (Hot Standby Router Protocol) em um ambiente LANE (LAN Emulation). Ele descreve muitas das especificações do HSRP sobre LANE e fornece dicas de solução de problemas para vários cenários.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

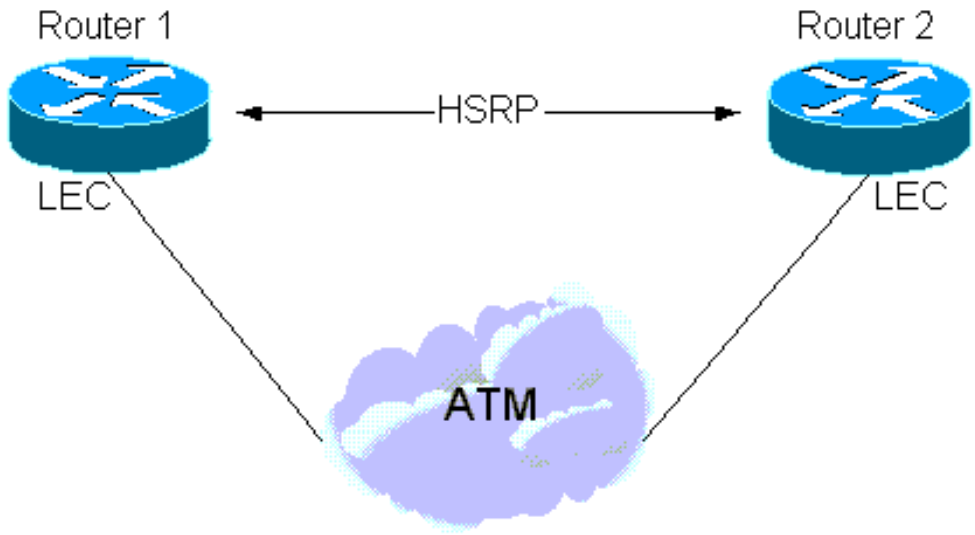
Em resumo, o objetivo do HSRP é permitir que os hosts em uma sub-rede usem um único

roteador "virtual", já que os roteadores de gateway padrão-vários participam do protocolo HSRP para eleger o roteador ativo, que assume a função de gateway padrão e um roteador de backup, caso o roteador ativo falhe. O resultado é que o gateway padrão sempre parecerá ativo mesmo se o roteador do primeiro salto físico for alterado. Uma descrição completa do HSRP pode ser encontrada no RFC 2281 .

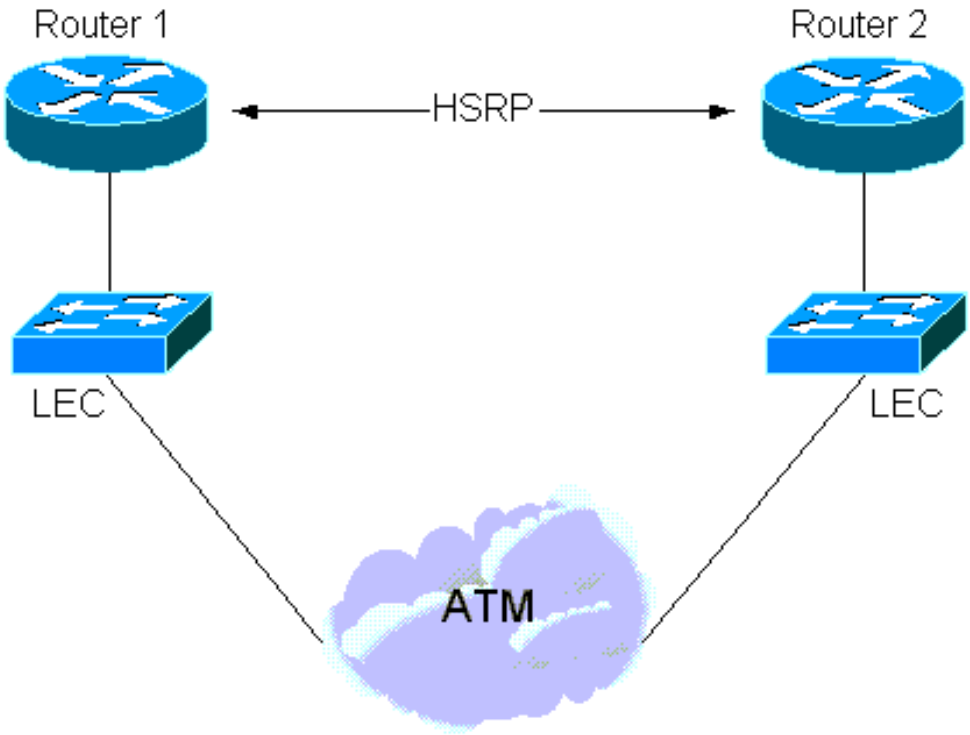
O HSRP foi projetado para uso em LANs com capacidade para multiacesso, multicast ou transmissão (tipicamente Ethernet, Token Ring ou Fiber Distributed Data Interface [FDDI]). Portanto, o HSRP deve funcionar bem sobre ATM LANE.

Várias situações envolvendo HSRP e interação LANE podem surgir:

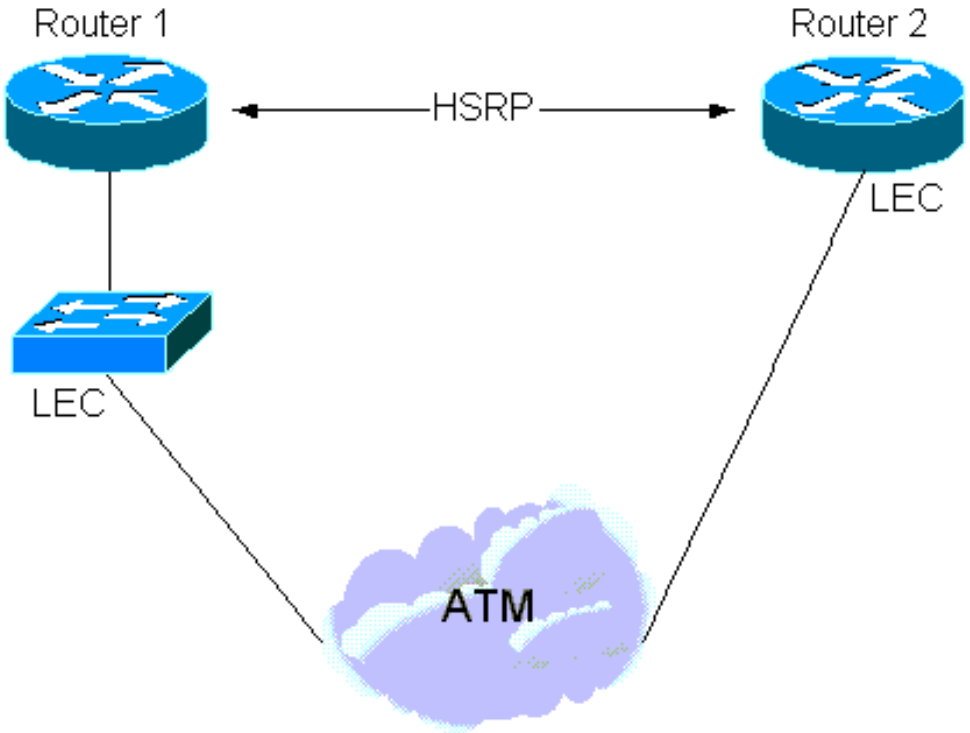
1. Desde o Cisco IOS® Software Release 11.2, o HSRP pode executar "nativamente" sobre LANE . Nesse caso, os comandos **standby** são configurados diretamente nas subinterfaces ATM nas quais os LAN Emulation Clients (LECs) residem. Veja a seguinte ilustração.



2. Há também uma instância em que o HSRP é configurado em interfaces de LAN, mas parte da sub-rede abrange uma nuvem LANE. Isso é feito pelo intermediário de um switch LAN com uma interface ATM (como um Cisco Catalyst 5000 com um módulo LANE). Veja a seguinte
ilustração.



3. Finalmente, há uma situação "híbrida" em que alguns roteadores HSRP estão conectados à LAN e outros estão em uma LAN por trás de um switch
   LAN.



Estudos de caso

1) HSRP nativo sobre LANE

Os roteadores que participam do HSRP enviam pacotes de "saudação" pelo meio de transmissão para aprenderem uns sobre os outros e elegerem os roteadores ativo e standby. Esses pacotes são enviados para o endereço multicast 224.0.0.2 com um Time to Live (TTL) de 1 e um endereço MAC de destino multicast de 0100 5E00 0002.

O LANE não apresenta novos problemas aqui, portanto os detalhes descritos no RFC 2281 ainda aplicam-se através da troca de pacotes hello, coup e resign, os roteadores ativos e em standby são eleitos.

Os pacotes hello são enviados pelo servidor de broadcast e desconhecido (BUS) e o seguinte é o que um **pacote atm de depuração** (no circuito virtual de encaminhamento multicast [VC]) e um **standby de depuração** revelariam:

```
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
```

Éimportante observar o que o LAN Emulation Client (LEC) recebe sobre o BUS (por exemplo, por

meio do 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
```

Esse hex-dump é traduzido do seguinte modo:

```
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
```

O que é notável é que os pacotes hello são originados pelo roteador ativo com o endereço MAC virtual (VMAC) como endereço MAC de origem - isso é desejável porque as bridges de aprendizagem (switches) que encaminham esses pacotes atualizarão sua tabela de memória endereçável de conteúdo (CAM) com o local apropriado do VMAC.

A chave para o HSRP está no mapeamento entre um endereço IP e um endereço MAC.

Na expressão mais simples, o endereço IP virtual é permanentemente vinculado a um endereço MAC virtual e o único aspecto com o qual se preocupar é que os switches sempre sabem onde esse endereço MAC virtual está localizado. Isso é garantido porque as saudações são fornecidas pelo 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
```

Outra opção é que os roteadores usem seus endereços gravados (**standby use-bia**) mapeados para o endereço IP virtual. Nesse caso, o mapeamento entre o IP virtual e o endereço MAC muda com o tempo - o roteador recém-ativo envia um Address Resolution Protocol (ARP) para anunciar o novo mapeamento de endereço IP para MAC virtual. Um ARP é simplesmente uma resposta ARP não solicitada.-

Observação: algumas pilhas de IP (mais antigas) podem não entender 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
```

Observação: para apresentar a LANE, a chave é que, além do mapeamento de endereço IP para MAC virtual, deve haver contabilidade para o mapeamento de endereço de NSAP (Network-Service-Access-Point, ponto de acesso de serviço de rede). Esse mapeamento é simplesmente resolvido através do processo do Protocolo de Resolução de Endereço de Emulação de LAN (LE-ARP - LAN Emulation-Address Resolution Protocol): um LEC que deseje enviar tráfego para o gateway ativo usará o LE-ARP para o VMAC (ou MAC físico se estiver usando o endereço MAC gravado [BIA]).

Agora, considere o que acontece quando um novo roteador se torna ativo: para que os LECs sejam informados sobre a nova localização do gateway ativo (novo mapeamento de VMAC para NSAP), a tabela LE-ARP deve ser modificada. Por padrão, as entradas de LE-ARP atingem o tempo limite a cada cinco minutos, mas, na maioria dos casos, depender desse tempo limite é inaceitável. A convergência deve ser mais rápida. A solução depende se o LEC supondo que o novo status Ativo esteja executando a versão 1 do LANE ou a versão 2 (consulte ATM Forum.com para obter as especificações LANE):

- **LANE versão 1**Quando um roteador se torna ativo, além das etapas descritas no RFC 2281 , ele envia um LE-NARP para tornar conhecida a nova associação de endereço VMAC para NSAP. De acordo com as especificações LANE, ao receber um LE-NARP, um LEC pode optar por limpar ou atualizar a entrada LE-ARP correspondente ao endereço MAC. A tendência na Cisco é adotar a abordagem mais conservadora e optar por limpar a entrada LE-ARP. Isso fará com que o LEC retorne imediatamente o LE-ARP sem ter que esperar pelo intervalo de cinco minutos.**Observação:** essa solução pode causar o problema de compatibilidade descrito abaixo.
- **LANE versão 2**Na versão 2 do LANE, algumas deficiências da versão 1 do LANE foram atenuadas: o LE-NARP foi substituído pelo LE-ARP sem destino e pelo LE-NARP sem origem. O LE-ARP sem destino pode ser visto como um veículo para anunciar novas associações, enquanto o objetivo do LE-NARP sem origem é tornar obsoleto um vínculo de endereço MAC para NSAP existente. A forma como isso é implementado é que se um

roteador muda de Standby para Ativo, ele envia um LE-ARP sem destino (usado para anunciar um mapeamento MAC para NSAP) e se muda de Ativo para Standby, ele envia um LE-NARP sem origem (usado para tornar obsoleto um enlace MAC para NSAP).

Problema - Interoperabilidade

Há um problema que muitas vezes surge para merecer uma análise mais aprofundada. As especificações LANE versão 1 afirmam que o LE-NARP deve especificar a "associação antiga", que está sendo tornada obsoleta especificando o (antigo) endereço de destino NSAP (T-NSAP). Normalmente, os roteadores que participam do HSRP não mantêm os diretórios de dados entre si.

Portanto, o roteador recém-ativo não conhece essas informações e optará por não preencher esse campo, pois não sabe melhor. Essa é uma leve violação das especificações e alguns fornecedores ignorarão esses pacotes se o campo de endereço T-NSAP for totalmente zero. Infelizmente, não há solução alternativa para isso se o LE-NARP for ignorado, confie no tempo limite LE-ARP (geralmente cinco minutos) antes que a associação correta seja aprendida.

Quando um LE-ARP ou LE-NARP é enviado com um campo de endereço T-NSAP de todos os zeros, ele é chamado de "sem destino". Como visto acima, com o advento da versão 2 da LANE (e do Multiprotocol over ATM [MPOA]), isso se tornou padrão e o problema deixa de existir.

Isso é feito na versão 1 do LANE, onde podem surgir problemas:

- Se o roteador conhece a "associação antiga", ele também pode obedecer às especificações. Essas depurações agora são feitas no VC de distribuição de controle:

```
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 não souber o "antigo enlace", fará o melhor e, pelo menos, anunciará o novo:

```
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
```

  Observação: desta vez, o endereço T-NSAP está em branco.

Novamente, o comportamento está completamente dentro das especificações ao usar clientes LANE versão 2.

Observação: o software que suporta MPOA também suporta LANE versão 2.

Dicas para Troubleshooting

O HSRP nativo sobre LANE não deve gerar muitos problemas além do possível problema de interoperabilidade devido ao LE-NARP desprovido do T-NSAP.

Se os roteadores tiverem dificuldade para determinar se estão ativos ou em espera, use o comando **debug standby** para ver se as saudações são vistas em ambos os lados. Caso contrário, o BUS provavelmente não está encaminhando corretamente os pacotes.

2) HSRP sobre roteadores atrás da LANE

A situação se torna mais complicada quando o HSRP é configurado em interfaces LANE de roteadores localizados atrás de uma nuvem LANE, como ilustrado na Figura 2.

Observação: esta figura mostra logicamente o fato de que o roteador não é ATM conectado. Ele não precisa necessariamente estar em um dispositivo separado do switch LAN (um Route Switch Module [RSM] em um Cisco Catalyst 5000 está sob esse caso).

Novamente, a dificuldade surge devido ao mapeamento de endereço MAC para endereço NSAP imposto pela LANE. Como observado acima, quando o VMAC muda para um dispositivo (quando um novo roteador se torna ativo) que corresponde a outro endereço NSAP, todos os dispositivos conectados à nuvem LANE devem ser informados. Isso é implementado com bastante facilidade em um ambiente nativo HSRP sobre LANE usando o LE-NARP (ou LE-ARP sem destino).

O problema nesse segundo caso é que os LECs não estão cientes de nenhuma informação de camada 3 (IP), eles são projetados apenas para fazer a ponte de pacotes entre dois meios diferentes (a LAN e o ATM).

Por exemplo, na Figura 2, se o Roteador 2 subitamente se tornou Ativo, então seria desejável que o switch 2 da LAN informasse todos os dispositivos conectados à nuvem ATM (LANE) sobre o novo mapeamento de VMAC para NSAP. Diz-se que o LEC no switch 2 da LAN está fazendo proxy para todos os endereços MAC que estão por trás dele. Os dispositivos através da LANE que desejam enviar tráfego para esses endereços MAC devem fazer isso por meio de uma configuração direta de dados para esse LEC. Intuitivamente, pode-se pensar que isso não será um grande problema, pois, assim que o Roteador 2 assumir o estado Ativo, ele começará a terceirizar saudações com o VMAC como o endereço MAC de origem. Essas informações seriam aprendidas por todos os switches LAN e tudo convergiria rapidamente. Isso é verdade em ambientes não LANE, mas a LANE é especial pelo seguinte motivo:

Na LANE, um pacote de dados pode geralmente ser transmitido através de dois caminhos:

- O data-direct se esse pacote for um unicast para o qual o destino foi mapeado para um NSAP conhecido e se o data-direct já foi estabelecido.
- O barramento para unicasts e multicasts desconhecidos.

Portanto, um mesmo endereço MAC originará pacotes que serão recebidos por um switch LAN em dois caminhos diferentes. Multicasts e unicasts desconhecidos chegarão por meio do BUS, enquanto unicasts conhecidos chegam por meio de diretórios de dados. Se nenhum esforço específico tivesse sido feito, um switch LAN continuaria aprendendo esse endereço MAC por meio de um direto de dados ou pelo BUS, dependendo do último pacote recebido. Isso é

indesejável porque o BUS só deve ser usado para enviar pacotes para unicasts ou multicasts desconhecidos. Neste estágio, nada é aprendido sobre o BUS, mas na realidade, opta por fazer o seguinte:

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 voltar ao exemplo, é seguro supor que todos os LECs neste ELAN já estão cientes do mapeamento VMAC-NSAP para o Roteador 1 antes de quando o Roteador 2 se tornar Ativo. Todos os switches LAN também sabem que o VMAC está por trás do switch LAN 1. Quando o Roteador 2 se torna Ativo e origina os pacotes de saudação, eles são encaminhados para a nuvem LANE sobre o BUS. Portanto, nenhum dos switches LAN atualizará suas tabelas CAM com essas novas informações e todos os pacotes enviados para esse VMAC serão direcionados incorretamente até que os switches LAN "se esqueçam" dessa entrada (o envelhecimento padrão é de cinco minutos).

Observação: a conectividade geral pode realmente ser perdida por até 10 minutos, já que o temporizador de envelhecimento LE-ARP nos LECs também é de cinco minutos por padrão. A redução do temporizador de envelhecimento para endereços MAC ajudará, mas na verdade não resolve o problema.

Há duas soluções para isso:

1. Se os switches LAN não forem Cisco, reverta para um método descrito acima: usando o endereço gravado. Se os roteadores usarem apenas seu endereço MAC para originar os pacotes de saudação e se o endereço IP virtual alterar o mapeamento sempre que um comutador ocorre, não há confusão possível quanto à localização desses endereços MAC.
2. Se os switches de LAN forem Cisco Catalyst, continue usando o VMAC devido às modificações fornecidas pelo Sistema de Rastreamento de Defeito Distribuído (DDTS - Distributed Defect Tracking System) coberto pelos IDs de bug da Cisco CSCdj58719 (somente clientes registrados) e CSCdj60431 (apenas clientes registrados).Em essência, quando um roteador assume o estado Ativo, além do ARP (resposta ARP não solicitada) que ele envia de acordo com o RFC 2281 , o roteador envia um segundo ARP com um endereço MAC de destino 0100.0CCD.CDCD. Quando um Cisco Catalyst recebe esse pacote, ele faz duas coisas:Limpa a entrada LE-ARP que tem para o VMAC.Ele aprende o VMAC sobre o BUS.

Por causa disso, não há mais entradas LE-ARP obsoletas nos vários LECs e a nova localização do VMAC é propagada para todos os switches (por exemplo, além da nuvem LANE). Para que isso funcione corretamente, os seguintes requisitos mínimos de software devem ser atendidos:

- Os roteadores devem ter pelo menos o software Cisco IOS versão 11.1(24), versão 11.2(13) ou toda a versão 12.0.
- Os módulos LANE devem ter pelo menos a versão 3.2(8). As versões 11.3W4 e posteriores são aceitáveis.

A Cisco recomenda o uso do software mais recente.

3) Ambiente misto

Há um último problema que pode surgir em ambientes mistos. Tomando o cenário acima e adicionando um dispositivo final LANE diretamente conectado (roteador ou estação de trabalho), o dispositivo final precisa ser informado sobre uma mudança de local do gateway ativo da mesma forma que no cenário 1. Se o roteador recém-ativo estiver conectado atrás de um switch, a única solução é que o próprio switch envie o LE-NARP em nome do roteador e isso é exatamente o que fazer.

Além das etapas descritas acima, se um Cisco Catalyst capta um pacote destinado ao CDCD 0100 0CCD, ele envia um LE-NARP (sem fonte LE-NARP se estiver executando a versão 2 do LANE), cujo único objetivo é limpar os caches LE-ARP para o VMAC.

Conclusão

Como demonstrado, o HSRP sobre LANE funciona bem em princípio, mas, em certas circunstâncias, os usuários podem perder a conectividade por curtos períodos de tempo se estiverem em uma das lacunas descritas acima.

Importante! Para garantir o sucesso com o HSRP na LANE, siga pelo menos estas duas recomendações:

- Para ser seguro, atualize para pelo menos a versão mais recente do Cisco IOS Software Release 12.0.
- Em ambientes de vários fornecedores, é melhor usar o LANE versão 2 ou o endereço gravado para evitar problemas.

Informações Relacionadas

- Páginas de Suporte da Tecnologia ATM
- Suporte Técnico - Cisco Systems