# Implementando HSRP sobre LANE

## Índice



## Introdução

A finalidade deste documento é esboçar as edições que podem ser encontradas ao executar o Hot Standby Router Protocol (HSRP) em um ambiente do LAN Emulation (LANE). Descreve muitos dos específicos do HSRP over LANE e fornece dicas de Troubleshooting para várias encenações.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

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

### Convenções

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

## Informações de Apoio

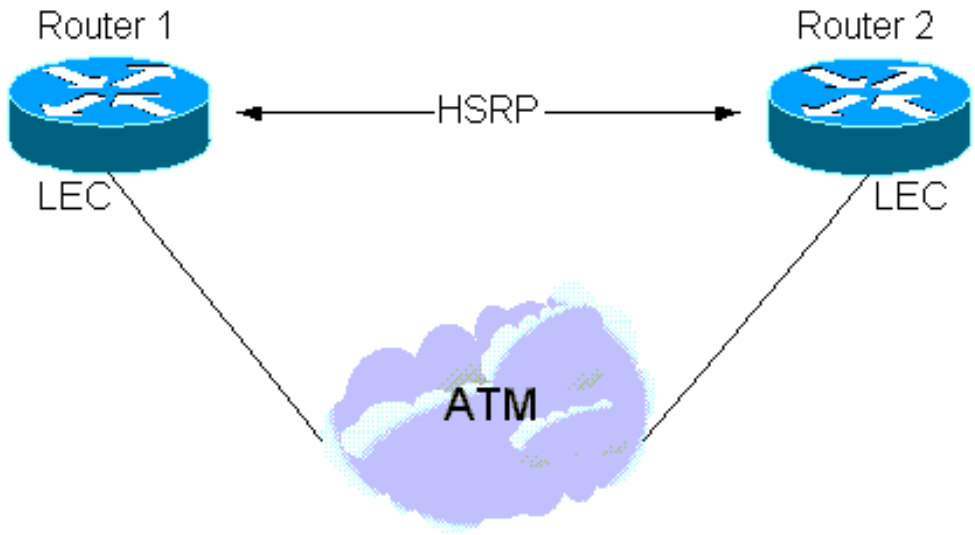
Em resumo, a finalidade do HSRP é permitir que os anfitriões em uma sub-rede usem um único

roteador “virtual” como o gateway padrão – os roteadores múltiplos participam no protocolo de HSRP a fim eleger o roteador ativo, que supõe o papel do gateway padrão e de um roteador de backup caso que ativo falha. O resultado é que o gateway padrão parecerá sempre estar acima mesmo se o primeiro roteador de salto físico muda. Uma descrição completa do HSRP pode ser encontrada no RFC 2281 .

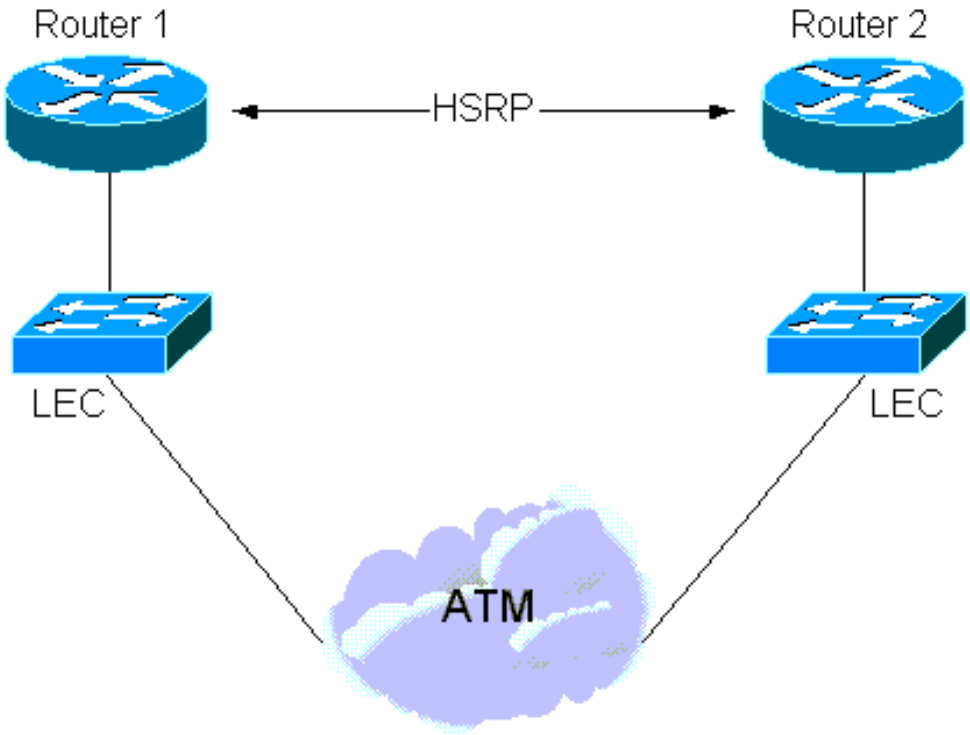
O HSRP foi projetado para o uso sobre o multi-acesso, Multicast, ou transmita LAN capazes (tipicamente [FDDI] dos Ethernet, do Token Ring, ou do Fiber Distributed Data Interface). Consequentemente, o HSRP deve trabalhar bem sobre o LANE ATM.

Diversas situações que envolvem o HSRP e a interação de pista podem elevarar:

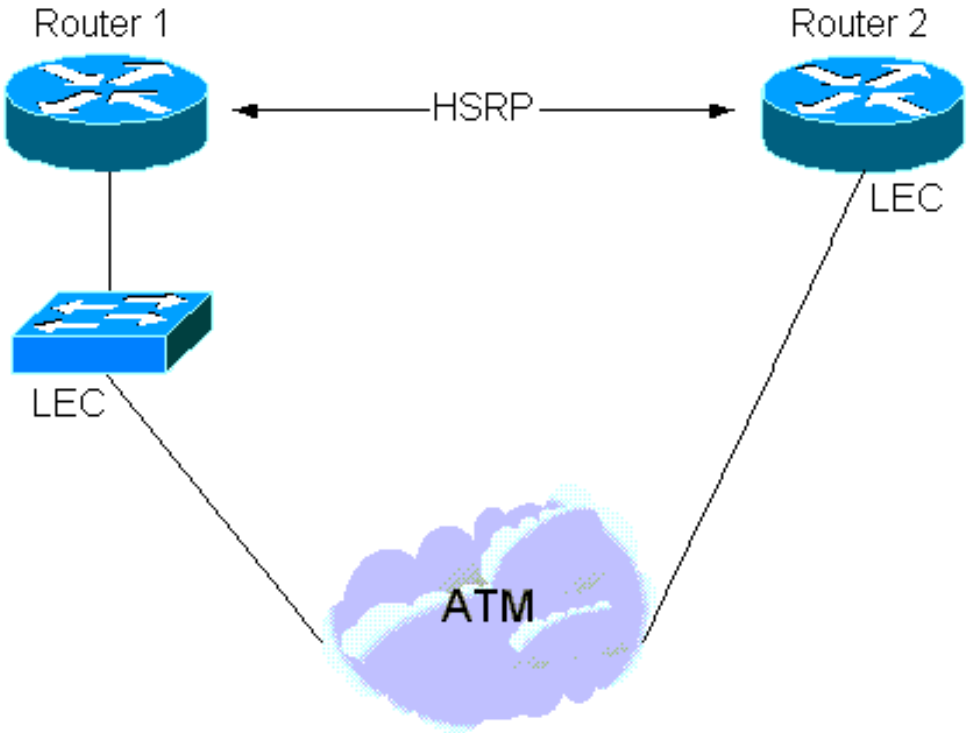
1. Desde o Software Release 11.2 de Cisco IOS®, o HSRP pode ser executado “nativamente” sobre o LANE. Neste caso, os **comandos standby** são configurados diretamente nas subinterfaces ATM onde os clientes de LAN Emulation (LEC) residem. Veja a seguinte ilustração.




2. Igualmente há um exemplo onde o HSRP seja configurado em interfaces de LAN, mas parte da sub-rede mede um nuvem de pista. Isto é realizado pelo intermediário de um switch LAN com uma interface ATM (tal como um Cisco catalyst 5000 com um módulo LANE). Veja a seguinte
ilustração.




3. Finalmente, há uma situação “híbrida” onde alguns roteadores de HSRP LANE-sejam anexados e outro estejam em um LAN atrás de um switch LAN.




## Estudos de caso

### 1) HSRP over LANE nativo

O Roteadores que participa no HSRP envia “olá!” pacotes sobre o meio de transmissão a fim aprender sobre se e eleger os roteadores ativo e em standby. Estes pacotes são enviados ao endereço de multicast 224.0.0.2 com um Time to Live (TTL) de 1 e um MAC address do destino multicast de 0100 5E00 0002.

O LANE não introduz nenhuma edição nova aqui assim que os detalhes descritos no RFC 2281 ainda aplicam-se – com a troca de olá!, o golpe, e renunciam-se pacotes, os roteadores ativo e em standby são elegidos.

Os pacotes Hello são enviados sobre a transmissão e servidor desconhecido (BARRAMENTO) e o seguinte é que um **pacote atm debugar** (no [VC] dianteiro dos circuitos virtuais do Multicast) e um **apoio debugar** revelaria:

```
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
```

Da importância está olhando o que o cliente de LAN Emulation (LEC) recebe sobre o BARRAMENTO (por exemplo, pelo Multicast para a frente):

```
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
```

Esta cópia parcial da memória de HEX traduz ao seguinte:

```
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 originado pelo roteador ativo com o endereço MAC virtual (VMAC) como o endereço MAC de origem – este é desejável porque os bridges de aprendizagem (Switches) que enviam estes pacotes atualizarão sua tabela de memória de conteúdo endereçável (CAM) com o lugar apropriado do VMAC.

A chave ao HSRP encontra-se dentro do mapeamento entre um endereço IP de Um ou Mais Servidores Cisco ICM NT e um MAC address.

Na expressão a mais simples, o endereço IP de Um ou Mais Servidores Cisco ICM NT virtual é

limitado permanentemente a um endereço MAC virtual e o único aspecto a preocupar-se aproximadamente é que o Switches sabe sempre onde este endereço MAC virtual é encontrado. Isto é assegurado porque os hellos são originado 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
```

Uma outra opção é que o Roteadores usa o seu queimar-(uso-**BIA à espera**) nos endereços traçados ao endereço IP de Um ou Mais Servidores Cisco ICM NT virtual. Neste caso, o mapeamento entre o IP virtual e as mudanças do MAC address ao longo do tempo – recentemente o roteador ativo manda um Address Resolution Protocol (ARP) a fim anunciar o mapeamento de endereço IP-à-MAC virtual novo. Um ARP é simplesmente uma reação ARP espontânea. -

**Nota:** Determinadas pilhas de IP (mais velhas) não podem compreender 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 introduzir o LANE, a chave é aquela sobre o mapeamento de endereço IP-à-MAC virtual, lá deve esclarecer o mapeamento de endereço do VMAC-à-Rede-Serviço-Acesso-ponto (NSAP). Este mapeamento é simplesmente resolved com o processo do protocolo lan emulation address resolution (LE-ARP): um LEC que deseja enviar o tráfego ao gateway ativo usará o LE-ARP para o VMAC (ou o MAC físico se usando o [BIA] do endereço MAC de operação antecipada).

Considere agora o que acontece quando um roteador novo se torna ativo: para que os LEC sejam informados do lugar novo do gateway ativo (mapeamento VMAC para NSAP novo), a tabela LE-ARP deve ser alterada. À revelia, as entradas do LE-ARP cronometram para fora cada cinco minutos mas, na maioria dos casos, confiar neste intervalo é inaceitável – a convergência deve ser mais rápida. A solução depende sobre se o LEC que supõe o status ativo novo é a versão LANE running 1 ou a versão 2 (veja ATM Forum.com para as especificações de pista):

- **Versão LANE 1**Quando um roteador se torna ativo, além do que as etapas descritas no RFC 2281 , manda um LE-NARP a fim fazer a binding do endereço VMAC-à-NSAP nova conhecida. De acordo com as especificações de pista, após recepção de um LE-NARP, um LEC pode escolher cancelar ou atualizar a entrada do LE-ARP que corresponde ao MAC address. A tendência dentro de Cisco é adotar mais abordagem conservadora e escolhê-la cancelar a entrada do LE-ARP – esta causará o LEC imediatamente ao re-LE-ARP sem ter que esperar o intervalo do cinco minutos.**Nota:** Esta solução pode causar o problema de compatibilidade descrito abaixo.
- **Versão LANE 2**Na versão LANE 2, determinados defeitos da versão LANE 1 foram aliviados: o LE-NARP foi substituído pelo LE-ARP targetless e pela nenhum-fonte LE-NARP. O LE-ARP targetless pode ser considerado como um veículo para anunciar emperramentos novos visto que a finalidade da nenhum-fonte o LE-NARP é render Obsoleto uma binding do endereço MAC-à-NSAP existente. A maneira que esta é executada é que se um roteador muda de à espera ao Active, manda um LE-ARP targetless (esta está usada para anunciar um mapeamento MAC a nsap) e se muda de ativo ao apoio, ele manda uma nenhum-fonte LE-NARP (esta está usada para tornar umas ligações MAC a nsap Obsoletos).

## Problema - Interoperabilidade

Há um problema que elevare frequentemente bastante para merecer um exame mais detalhado. As especificações da versão LANE 1 indicam que o LE-NARP deve especificar “o emperramento velho,” que está sendo feito Obsoleto especificando o endereço (velho) do alvo NSAP (o T-NSAP). Tipicamente, o Roteadores que participa no HSRP não mantém dados dirige entre se.

Consequentemente, recentemente o roteador ativo não sabe que estas informação e escolherá não terminar este campo desde que não sabe melhor. Esta é uma violação leve das especificações e alguns vendedores ignorarão estes pacotes se o campo de endereço T-NSAP é todos os zero. Infelizmente, não há nenhuma ação alternativa para esta – se o LE-NARP é ignorado, confie no intervalo do LE-ARP (tipicamente cinco minutos) antes que o emperramento correto esteja instruído.

Quando um LE-ARP ou um LE-NARP são enviados com um campo de endereço T-NSAP de todos os zero, está chamado “targetless.” Como visto acima, com o advento do [MPOA] da versão LANE 2 (e do multiprotocolo sobre ATM), isto tem o padrão tornado e o problema cessa de existir.

Este é o que é feito na versão LANE 1 onde os problemas podem elevarar:

- Se o roteador conhece “o emperramento velho,” pôde também obedecer as especificações. Estes debugam são tomados agora no controle distribuem o 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 não conhecem “o emperramento velho,” fazem seu melhor e anunciam pelo menos 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
```
**Nota:** Esta vez o endereço T-NSAP está vazio.

Além disso, o comportamento está completamente dentro das especificações ao usar clientes da versão LANE 2.

**Nota:** O software que apoia o MPOA igualmente apoia a versão LANE 2.

## Dicas para Troubleshooting

O HSRP over LANE nativo não deve gerar problemas demais diferentes da questão de

interoperabilidade potencial devido ao LE-NARP desprovido do T-NSAP.

Se o Roteadores tem a dificuldade em estabelecer se é ativo ou à espera, use o **comando debug standby** ver se os hellos são vistos em ambos os lados. Se não, então o BARRAMENTO provavelmente não está enviando corretamente os pacotes.

## 2) HSRP sobre o Roteadores atrás do LANE

A situação torna-se mais complicada quando o HSRP é configurado nas interfaces LANE de roteadores situadas atrás de um nuvem de pista, como ilustrado em figura 2.

**Nota:** Esta figura descreve logicamente o fato de que o roteador é não-ATM anexado. Não tem que necessariamente estar em um dispositivo separado ao switch LAN (um [RSM] do módulo de switch de rota em um Cisco catalyst 5000 cai sob este caso).

Além disso, a dificuldade elevara devido ao mapeamento do MAC-endereço-à-NSAP-endereço imposto pelo LANE. Como notável acima, quando o VMAC comuta a um dispositivo (quando um roteador novo se torna ativo) que corresponda a um outro endereço nsap, todos os dispositivos anexados ao nuvem de pista devem ser informados. Isto é executado razoavelmente facilmente em um ambiente nativo do HSRP over LANE usando o LE-NARP (ou o LE-ARP targetless).

O problema neste segundo caso é que os LEC não estão cientes de nenhuma informação da camada 3 (IP), eles é projetado unicamente aos pacotes de Bridge entre dois media diferentes (o LAN e o ATM).

Por exemplo, em figura 2, se o roteador2 se tornou de repente ativo, a seguir seria desejável para o switch LAN 2 informar todos os dispositivos conectados à nuvem ATM (LANE) sobre o mapeamento VMAC para NSAP novo. O LEC no switch LAN 2 seriam proxying para todos os endereços MAC que são atrás dele. Os dispositivos através do LANE que deseja enviar o tráfego a estes endereços MAC devem fazer assim por um direcionamento de dados setup para este LEC. Intuitivamente, se poderia pensar que este não será um problema grande desde que, assim que o roteador2 supusesse o estado ativo, começará hellos da fonte com o VMAC como o endereço MAC de origem. Esta informação seria aprendida então por todos os switch LAN e tudo convirgiria rapidamente. Isto é verdadeiro nos ambientes NON-LANE, mas o LANE é especial para a seguinte razão:

No LANE, um pacote de dados pode geralmente ser transmitido através de dois trajetos:

- O direcionamento de dados se este pacote é um unicast para que o destino esteve traçado a um NSAP conhecido e se o direcionamento de dados tem sido estabelecido já.
- O BARRAMENTO para unicasts desconhecidos e Multicast.

Consequentemente, um mesmo MAC address os pacotes de origem que serão recebidos por um switch LAN sobre dois trajetos diferentes. Os Multicast e os unicasts desconhecidos chegarão pelo BARRAMENTO visto que os unicasts conhecidos chegam por direcionamentos de dados. Se nenhum esforço específico tinha sido feito, um switch LAN manter-se-ia aprender este MAC address sobre um direcionamento de dados ou sobre o BARRAMENTO segundo o último pacote recebido. Isto é indesejável porque o BARRAMENTO deve somente ser usado para enviar pacotes para unicasts desconhecidos ou Multicast. Nesta fase, nada é instruído sobre o BARRAMENTO, mas na realidade, escolha 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 retornar ao exemplo, é seguro supor que todos os LEC neste ELAN estão já cientes do mapeamento VMAC-NSAP para o roteador1 antes de quando o roteador2 se torna ativo. Todos os switch LAN igualmente sabem que o VMAC é atrás do switch LAN 1. Quando o roteador2 se transforma Active e fontes os pacotes Hello, estes estão enviados ao nuvem de pista sobre o BARRAMENTO. Consequentemente, nenhuns dos switch LAN atualizarão suas tabelas CAM com esta informação nova e todos os pacotes enviados a este VMAC serão orientados mal até que os switch LAN “esqueçam” sobre esta entrada (o envelhecimento do padrão que é cinco minutos).

**Nota:** A conectividade total pôde realmente ser perdida por até os minutos 10 desde que o aging timer do LE-ARP nos LEC igualmente é cinco minutos à revelia. Reduzir o aging timer para endereços MAC ajudará, mas não resolve realmente o problema.

Há duas soluções para esta:

1. Se os switch LAN são não-Cisco, reverta a um método descrito acima: usando o endereço operação antecipada. Se o Roteadores usa somente seu MAC address à fonte os pacotes Hello e aquele as alterações de endereço do IP virtual que traçam sempre que a interruptor-sobre ocorre, não há nenhuma confusão possível a respeito de onde estes endereços MAC são encontrados.
2. Se os switch LAN são Cisco catalyst, a seguir mantenha usar o VMAC devido às alterações fornecidas pelo Distributed Defect Tracking System (DDTS) coberto no Bug da Cisco ID CSCdj58719 (clientes registrados somente) e CSCdj60431 (clientes registrados somente).Essencialmente, quando um roteador supõe o estado ativo, além do que o ARP (reação ARP espontânea) esse envia de acordo com o RFC 2281 , o roteador envia um segundo ARP com um endereço MAC de destino de 0100.0CCD.CDCD. Quando um Cisco catalyst recebe este pacote faz duas coisas:Cancela a entrada que do LE-ARP tem para o VMAC.Aprende o VMAC sobre o BARRAMENTO.

Devido a isto, não há não mais entrada velha do LE-ARP nos vários LEC e o lugar novo do VMAC é propagado a todo o Switches (por exemplo, além do nuvem de pista). Para que isto trabalhe corretamente, os seguintes requisitos de software mínimo devem ser cumpridos:

- O Roteadores deve ter pelo menos o Cisco IOS Software Release 11.1(24), a versão 11.2(13), ou a toda a versão 12.0.
- Os módulos LANE devem ter pelo menos a versão 3.2(8). as versões 11.3W4 e são mais tarde aceitáveis.

**Cisco recomenda usar o software mais recente.**

## 3) Ambiente misto

Há uma edição final que pode elevarar nos ambientes mistos. Tomando a encenação acima e adicionando um dispositivo final diretamente conectado LANE (roteador ou estação de trabalho), o dispositivo final precisa de ser informado sobre uma alteração de local do gateway ativo a mesma maneira que na encenação 1. Se o roteador ativo é conectado recentemente atrás de um interruptor, a única solução é para o interruptor próprio para mandar o LE-NARP em nome do

roteador e este é exatamente o que a fazer.

Além do que as etapas descritas acima, se um Cisco catalyst pegara um pacote destinado a 0100 0CCD CDCD, manda um LE-NARP (nenhum-fonte LE-NARP se executando a versão LANE 2), que seu propósito único seja cancelar os esconderijos do LE-ARP para o VMAC.

## Conclusão

Como demonstrado, o HSRP over LANE trabalha bem em princípio mas, em certas circunstâncias, os usuários podem perder períodos de tempo da Conectividade para breve se caindo em uma das fendas descritas acima.

Importante! A fim assegurar o sucesso com HSRP over LANE, siga pelo menos estas duas recomendações:

- Para ser seguro, elevação pelo menos à versão a mais atrasada do Cisco IOS Software Release 12.0.
- Em ambientes do mult-vendedor, é o melhor usar a versão LANE 2 ou o endereço operação antecipada a fim evitar problemas.

## Informações Relacionadas

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