LANE 経由の HSRP の実装

内容

概要

このドキュメントは、LAN エミュレーション (LANE) 環境でホットスタンバイ ルータ プロトコル (HSRP) を実装している場合に発生する可能性のある問題の概要説明を目的としています。LANE 上での HSRP の詳細について説明し、さまざまなシナリオでのトラブルシューティングのヒントを示します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

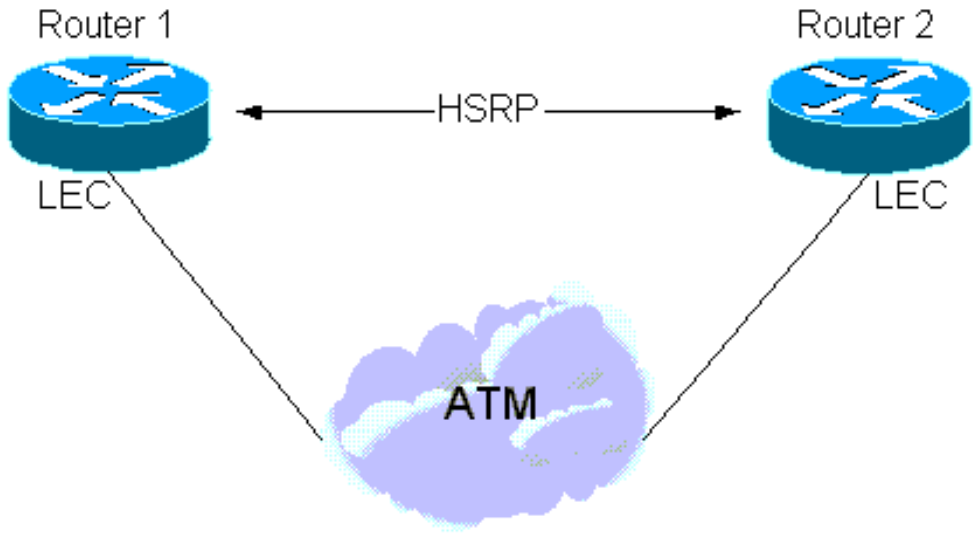
要約すると、HSRPの目的は、サブネット内のホストがデフォルトゲートウェイの複数のルータ

がHSRPプロトコルに参加し、アクティブルータが故障した場合にデフォルトゲートウェイとバックアップルータの役割を引き継ぐようにすることです。その結果、物理ファーストホップルータが変更されても、デフォルトゲートウェイは常にアップしているように見えます。HSRPの詳細については、RFC 2281を参照してください 。

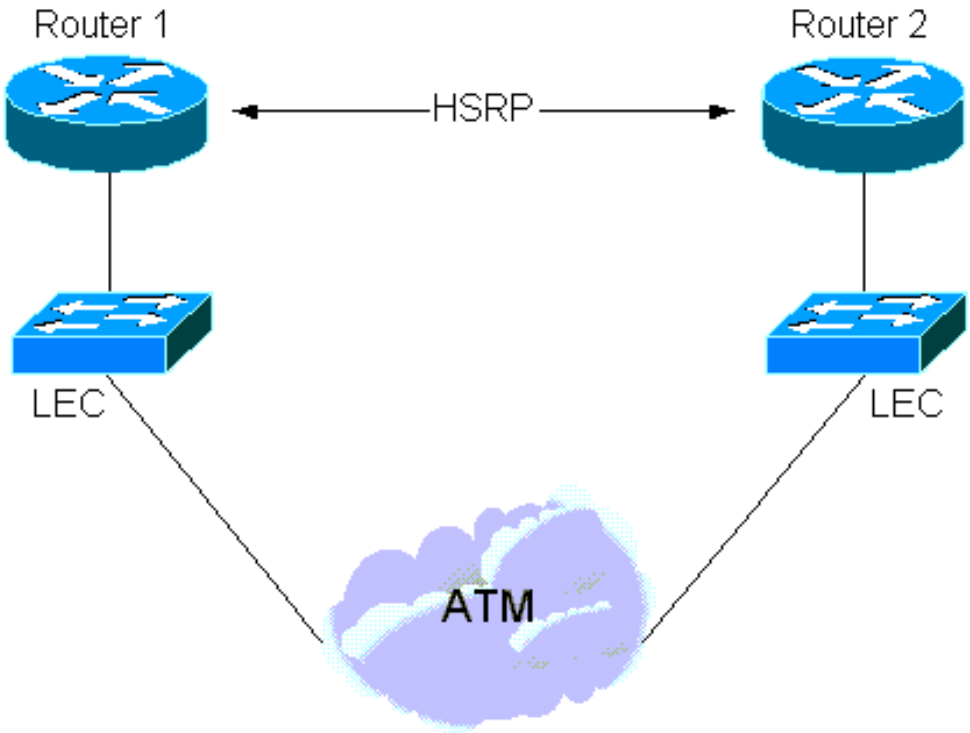
HSRPは、マルチアクセス、マルチキャスト、またはブロードキャスト対応LAN(通常はイーサネット、トークンリング、またはファイバ分散データインターフェイス(FDDI))で使用するように設計されています。 したがって、HSRPはATM LANE上で適切に動作します。

HSRPとLANEのインタラクションに関連するいくつかの状況が発生する可能性があります。

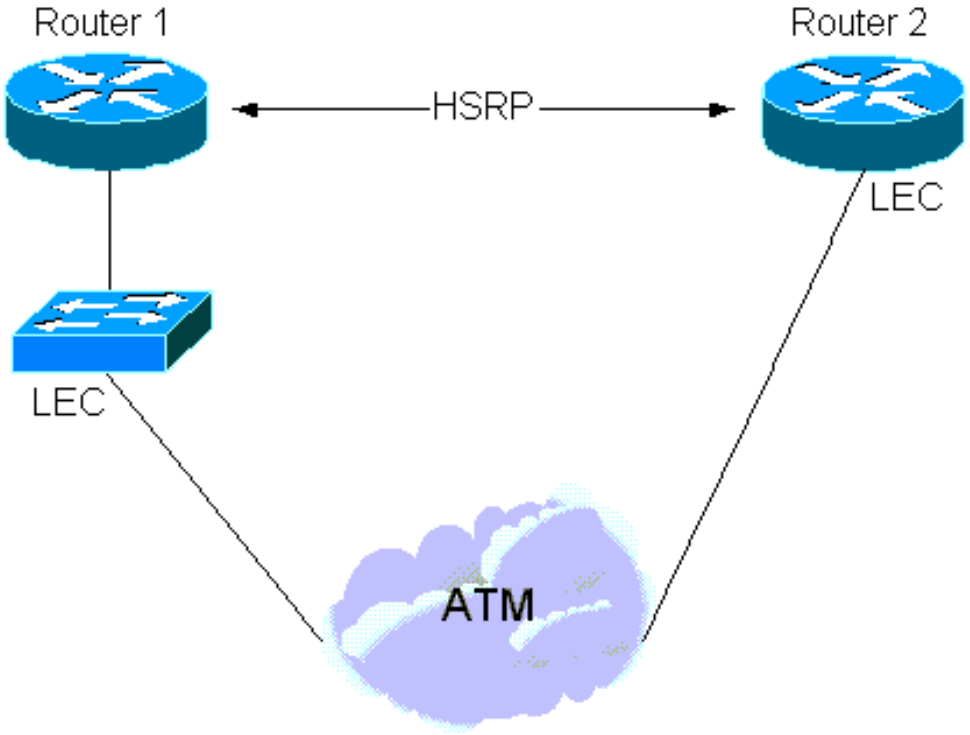
1. Cisco IOS®ソフトウェアリリース11.2以降では、HSRPはLANE上で「ネイティブ」に動作できます（HSRPはネイティブに動作します）。この場合、**standbyコマンド**は、LANエミュレーションクライアント(LEC)が存在するATMサブインターフェイスで直接設定されます。次の図を参照してください。



2. また、LANインターフェイスでHSRPが設定されているが、サブネットの一部がLANEクラウドにまたがるインスタンスもあります。これは、ATMインターフェイス（LANEモジュールを搭載したCisco Catalyst 5000など）を備えたLANスイッチの中間インターフェイスによって実現されます。 次の図を参照してください。



3. 最後に、一部のHSRPルータがLANE接続され、他のルータがLANスイッチの背後のLAN上にある「ハイブリッド」状態があります。



ケース スタディ

1)ネイティブHSRP Over LANE

HSRPに参加しているルータは、ブロードキャストメディアを介して「hello」パケットを送信し、相互の情報を取得し、アクティブルータとスタンバイルータを選出します。これらのパケットはマルチキャストアドレス224.0.0.2に送信され、Time to Live（TTL；存続可能時間）は1で、マルチキャスト宛先MACアドレスは0100 5E00 0002です。

LANEでは新しい問題が発生しないため、RFC 2281で説明されている詳細は 、hello、coup、

resignパケットの交換を通じて適用され、アクティブルータとスタンバイルータが選出されます。

helloパケットはブロードキャストおよび不明なサーバ(BUS)を介して送信されます。次に、**debug atm packet**(VC)と**debug standbyを示します。**

```
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
```

重要なのは、LANエミュレーションクライアント(LEC)がBUSを介して受信する内容（たとえば、マルチキャスト転送を介して）を調べることです。

```
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
```

この16進数ダンプは次のように変換されます。

```
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
```

注目すべき点は、helloパケットの送信元が仮想MACアドレス(VMAC)で、送信元MACアドレスはアクティブルータです。これは、これらのパケットを転送するラーニングブリッジ（スイッチ）が、VMACの適切な場所でContent-Addressable Memory(CAM)テーブルを更新します。

HSRPの鍵は、IPアドレスとMACアドレスのマッピング内にあります。

最も簡単な表現では、仮想IPアドレスは仮想MACアドレスに永続的にバインドされており、心配する唯一の側面は、スイッチが常にこの仮想MACアドレスの場所を認識していることです。これは、helloがVMACによって送信されるため、確実です。

```
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
```

もう1つのオプションは、ルータが仮想IPアドレスにマッピングされた焼き込み(**standby use-bia**)アドレスを使用することです。この場合、仮想IPとMACアドレスのマッピングは時間の経過とともに変化します。新しいアクティブルータは、新しい仮想IPとMACアドレスのマッピングをアナウンスするためにアドレス解決プロトコル(ARP)を送信します。ARPは単に非要請ARP応答です。

注：特定の(古い)IPスタックはARPを理解できない場合があります。

```
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
```

注：LANEを導入するには、仮想IP-to-MACアドレスマッピングの上に、VMAC-to-Network-Service-Access-Point(NSAP)アドレスマッピングのアカウンティングが必要であることが重要です。このマッピングは、LAN Emulation-Address Resolution Protocol(LE-ARP)プロセスを通じて解決されます。アクティブゲートウェイにトラフィックを送信するLECは、VMACに対してLE-ARPを使用します(または、バーンドインMACアドレス(BIA)を使用している場合は物理MACを使用します)。

次に、新しいルータがアクティブになったときに何が起こるかを考えます。LECにアクティブゲートウェイの新しい場所（新しいVMACとNSAPのマッピング）を通知するには、LE-ARPテーブルを変更する必要があります。デフォルトでは、LE-ARPエントリは5分ごとにタイムアウトしますが、ほとんどの場合、このタイムアウトに依存することは許容できないコンバージェンスが高速である必要があります。解決策は、新しいアクティブステータスがLANEバージョン1またはバージョン2を実行していると仮定してLECが判断するかどうかによって異なります(LANE仕様についてはATM Forum.comを参照)。

- **LANEバージョン1**ルータがアクティブになると、RFC 2281 で説明されている手順に加えて、新しいVMACとNSAPのアドレスバインディングを認識させるためにLE-NARPを送信します。LANEの仕様によると、LE-NARPを受信すると、LECはMACアドレスに対応するLE-ARPエントリをクリアまたは更新することを選択できます。シスコでは、より控えめなアプローチを採用し、LE-ARPエントリをクリアする傾向があります。これにより、LECは5分間のタイムアウトを待たずに、すぐにLE-ARPを再び使用できます。**注：このソリュー**ションは、次に示す互換性の問題を引き起こす可能性があります。
- **LANEバージョン2**LANEバージョン2では、LANEバージョン1の一部の欠点が解消されました。LE-NARPは、ターゲットレスLE-ARPと非ソースLE-NARPに置き換えられました。ターゲットのないLE-ARPは、新しいバインディングをアドバタイズする手段と見なされることがあります。一方、ソースのないLE-NARPの目的は、古いMACからNSAPへの既存のアドレスバインディングをレンダリングすることです。これを実装する方法は、ルータがスタンバイからアクティブに変更されると、ターゲットのないLE-ARP（MACからNSAPへのマッピングをアドバタイズするために使用）を送信し、アクティブからスタンバイに変更されると、ソースのないLE-NARPを送信します。

問題：相互運用性

より詳細な検査を受けるだけの問題が頻繁に発生します。LANEバージョン1仕様では、LE-NARPは「古いバインディング」を指定する必要があります。これは、（古い）ターゲットNSAP(T-NSAP)アドレスを指定することによって廃止されます。通常、HSRPに参加しているルータは、相互のデータ転送を維持しません。

したがって、新しいアクティブルータはこの情報を認識せず、このフィールドを入力しないことを選択します。これは、このフィールドが適切に認識されないためです。これは仕様に対する軽度の違反であり、一部のベンダーは、T-NSAPアドレスフィールドがすべてゼロの場合、これらのパケットを無視します。残念ながら、LE-NARPが無視される場合は、正しいバインディングが学習される前にLE-ARPタイムアウト（通常5分）に依存してください。

LE-ARPまたはLE-NARPが、すべて0のT-NSAPアドレスフィールドを使用して送信される場合、「ターゲットレス」と呼ばれます。 上記のように、LANEバージョン2(およびMultiprotocol over ATM(MPOA))の登場により、これは標準となり、問題は存在しなくなります。

問題が発生する可能性があるLANEバージョン1では、次のことが行われます。

- ルータが「古いバインディング」を認識している場合は、仕様に従う可能性があります。次のデバッグは、Control Distribute VCで行われています。

```
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)
```

- 「古いバインディング」を知らない場合は、最善を尽くし、少なくとも新しいバインディングをアドバタイズします。

```
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
```

注：今回は、T-NSAPアドレスが空白です。

ここでも、LANEバージョン2クライアントを使用する場合の動作は完全に仕様範囲内です。

注：MPOAをサポートするソフトウェアは、LANEバージョン2もサポートしています。

トラブルシューティングのヒント

LANE上のネイティブHSRPでは、T-NSAPが存在しないLE-NARPによる潜在的な相互運用性の問題を除き、多くの問題が発生することはありません。

ルータがアクティブかスタンバイかを確立できない場合は、**debug standbyコマンドを使用**して、

両側にhelloが表示されているかどうかを確認します。そうでない場合は、BUSがパケットを正しく転送していない可能性があります。

2) LANEの背後にあるルータでのHSRP

図2に示すように、LANEクラウドの背後にあるルータのLANEインターフェイスでHSRPを設定すると、状況はさらに複雑になります。

注：この図は、ルータが非ATM接続であることを論理的に示しています。必ずしもLANスイッチとは別のデバイスに存在する必要はありません(Cisco Catalyst 5000のRoute Switch Module（RSM；ルートスイッチモジュール）はこの場合に該当します)。

繰り返しますが、LANEによって課されたMACアドレスとNSAPアドレスのマッピングが問題になります。上記のように、VMACが別のNSAPアドレスに対応するデバイス（新しいルータがアクティブになった場合）に切り替わる場合、LANEクラウドに接続されているすべてのデバイスに通知する必要があります。これは、LE-NARP（またはターゲットレスLE-ARP）を使用して、ネイティブHSRP over LANE環境で簡単に実装できます。

この2番目のケースの問題は、LECがレイヤ3(L3)情報(IP)を認識しておらず、2つの異なるメディア（LANとATM）間でパケットをブリッジするように設計されているだけです。

たとえば、図2で、ルータ2が突然アクティブになった場合、LANスイッチ2はATM(LANE)クラウドに接続されているすべてのデバイスに新しいVMACとNSAPのマッピングを通知することが望ましいでしょう。LANスイッチ2のLECは、背後にあるすべてのMACアドレスをプロキシしていると言われます。これらのMACアドレスにトラフィックを送信するLANE上のデバイスは、このLECに対するデータ直接設定を介して送信する必要があります。直感的に言えば、これは大きな問題ではないと思うかもしれません。ルータ2がアクティブ状態を想定するとすぐに、送信元MACアドレスとしてVMACを持つhelloパケットの送信を開始します。この情報はすべてのLANスイッチによって学習され、すべてが急速に収束します。これは非LANE環境では当てはまりますが、LANEは次の理由で特別です。

LANEでは、データパケットは通常、次の2つのパスを通じて送信できます。

- このパケットが既知のNSAPに宛先がマッピングされているユニキャストであり、データダイレクトがすでに確立されている場合、データダイレクト。
- 不明なユニキャストおよびマルチキャストのBUS。

したがって、同じMACアドレスが、2つの異なるパスを介してLANスイッチによって受信されるパケットを送信します。マルチキャストと未知のユニキャストはBUS経由で到着しますが、既知のユニキャストはデータリダイレクト経由で到着します。特に努力が行われていなければ、LANスイッチは、最後に受信したパケットに応じて、データダイレクトまたはバス経由でこのMACアドレスを学習し続けます。これは、BUSは不明なユニキャストまたはマルチキャストのパケットを送信するためだけに使用する必要があるため、望ましくありません。この段階では、BUSを介して何も学習されませんが、実際には次のことを選択します。

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.

この例に戻るには、ルータ2がアクティブになる前に、このELAN内のすべてのLECがルータ1のVMAC-NSAPマッピングをすでに認識していると仮定するのが安全です。すべてのLANスイッチは、VMACがLANスイッチ1の背後にあることを認識しています。ルータ2がアクティブになり、helloパケットを送信すると、これらはバスを介してLANEクラウドに転送されます。したがって、どのLANスイッチも、この新しい情報でCAMテーブルを更新せず、このVMACに送信されたすべてのパケットは、LANスイッチがこのエントリを「忘れる」まで（デフォルトのエージングは5分）誤って送信されます。

注：LECのLE-ARPエージングタイマーもデフォルトで5分であるため、実際には全体の接続が最大10分間失われる可能性があります。MACアドレスのエージングタイマーを減らすことは役に立ちますが、実際には問題は解決しません。

これには、次の2つのソリューションがあります。

1. LANスイッチがシスコ以外の場合は、上記の方法に戻します。焼き込みアドレスを使用します。ルータがMACアドレスのみを使用してhelloパケットを送信し、スイッチオーバーが発生するたびに仮想IPアドレスがマッピングを変更する場合、これらのMACアドレスの場所に関する混乱はありません。
2. LANスイッチがCisco Catalystの場合は、Cisco Bug ID CSCdj58719（登録ユーザ専用）およびCSCdj60431で説明されている分散型不具合トラッキングシステム(DDTS)の変更により、VMACの使用ををを使用ををし続続続してください(登録ユーザ専用)。基本的には、ルータがアクティブ状態であると仮定すると、RFC 2281に従って送信するARP(Unsolicited ARP Response)に加え、ルータは宛先MACアドレス0100.0CCD.CDCDの2番目ARP.Cisco Catalystはこのパケットを受信すると、次の2つの処理を行います。VMACに対するLE-ARPエントリをクリアします。VMACをBUS経由で学習します。

このため、さまざまなLECに古いLE-ARPエントリがなくなり、VMACの新しい場所がすべてのスイッチに伝搬されます（たとえば、LANEクラウドを越えて）。 これを正しく動作させるには、次の最低限のソフトウェア要件を満たす必要があります。

- ルータには、少なくともCisco IOSソフトウェアリリース11.1(24)、バージョン11.2(13)、またはすべてのバージョン12.0が必要です。
- LANEモジュールには、バージョン3.2(8)以上が必要です。11.3W4以降のバージョンは許容されます。

最新のソフトウェアの使用を推奨します。

3)混在環境

混合環境で発生する可能性のある最終的な問題が1つあります。上記のシナリオに従い、直接接続されたLANEエンドデバイス（ルータまたはワークステーション）を追加すると、エンドデバイスはシナリオ1と同じようにアクティブゲートウェイの場所の変更を通知する必要があります。スイッチの背後に新しいアクティブルータが接続されている場合は、

上記の手順に加えて、Cisco Catalystが0100 0CCD CDCD宛てのパケットをピックアップすると、LE-NARP（LANEバージョン2を実行している場合はソースなしLE-NARP）を送信します。これは、VMACののLE ARPキャッシュをクリア唯一目的です。

結論

示されているように、LANE上のHSRPは基本的に正常に動作しますが、特定の状況では、上記の

ループホールのいずれかに該当すると、ユーザが短時間の接続を失う可能性があります。

重要：LANE上でHSRPを正常に動作させるには、少なくとも次の2つの推奨事項に従ってください。

- 安全のために、少なくとも最新バージョンのCisco IOSソフトウェアリリース12.0にアップグレードしてください。
- マルチベンダー環境では、問題を回避するためにLANEバージョン2または焼き付けアドレスを使用するのが最適です。

関連情報

- ATM テクノロジーに関するサポート ページ
- テクニカルサポート - Cisco Systems