# ASA站點間透明群集的常見問題

## 目錄



本文檔介紹跨網路EtherChannel透明模式站點間群集的一些常見問題。

- 調適型安全裝置(ASA)防火牆
- ASA集群

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

從ASA 9.2版開始，支援站點間集群，其中ASA單元可以位於不同的資料中心，並且集群控制鏈路(CCL)通過資料中心互聯(DCI)連線。 可能的部署方案包括：

- 單個介面站點間集群
- 跨網路EtherChannel透明模式站點間集群
- 跨網路EtherChannel路由模式站點間集群（從9.5起支援）

# MAC移動通知

當內容可定址儲存器(CAM)表中的MAC地址更改埠時，生成MAC MOVE通知。但是，在CAM表中新增或刪除MAC地址時，不會生成MAC MOVE通知。假設通過VLAN10中的介面GigabitEthernet0/1獲知MAC地址X，一段時間後，通過VLAN 10中的GigabitEthernet0/2看到相同的MAC，則生成MAC MOVE通知。

Switch：的系統日誌

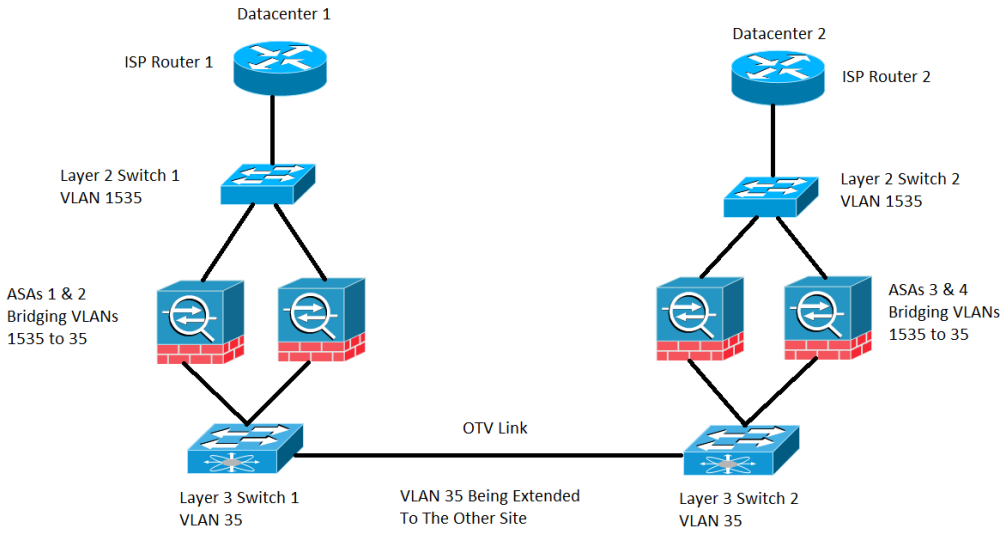
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

來自ASA的系統日誌：

```
ASA-4-412001: MAC 003a.7b58.24c5 moved from DMZ to INSIDE
```

# 網路圖表

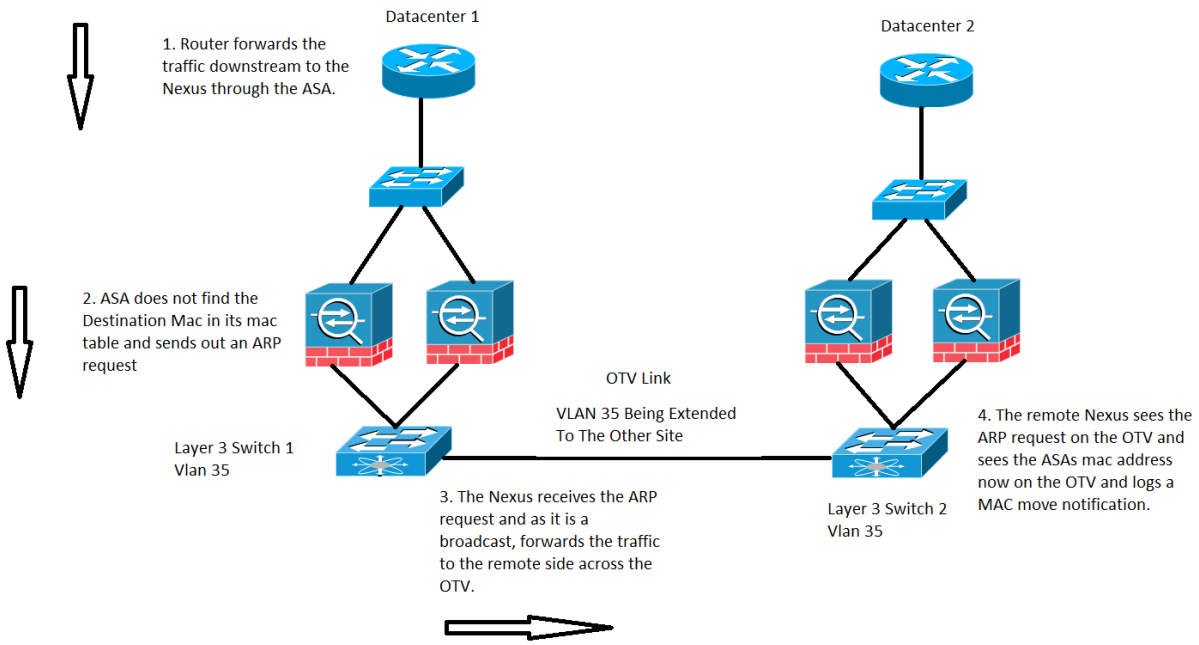
站點間集群部署，其中ASA配置為透明模式橋接VLAN 1535和VLAN 35。內部VLAN 35在重疊傳輸虛擬化(OTV)上擴展，而外部VLAN 1535未在OTV上擴展，如下圖所示




# 交換機上的MAC移動通知

## 案例 1

目的地為某MAC地址的流量，該MAC地址的條目不在ASA的MAC表中，如下圖所示：




在透明ASA中，如果到達ASA的資料包的目標MAC地址不在mac地址表中，則發出該目標的地址解析協定(ARP)請求（如果與BVI位於同一子網）或網際網路控制消息協定(ICMP)請求，Time To Live 1(TTL 1)將源MAC作為Bridge Virtual Interface(BVI)MAC地址，將目標MAC地址作為目標媒體訪問控制器(DMAC)丟失。

在上述情況下，您有以下流量：

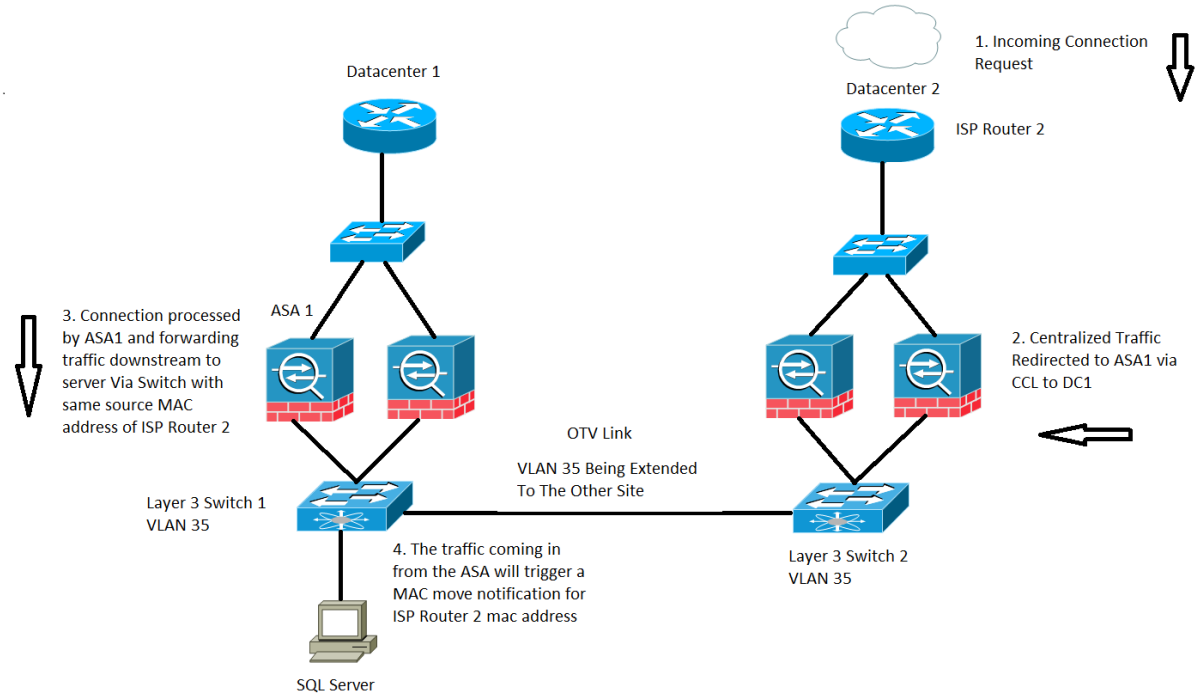
1. 資料中心1上的ISP路由器將流量轉發到ASA後方的特定目標。
2. 其中一個ASA可以接收流量，在這種情況下，ASA不知道流量的目標MAC地址。
3. 現在，流量的目標IP與BVI位於同一個子網中，如前所述，ASA現在會生成目標IP的ARP請求。
4. 交換機1接收流量，由於請求是廣播，因此它會將流量轉發到資料中心2以及通過OTV鏈路。
5. 當交換機2在OTV鏈路上看到來自ASA的ARP請求時，它將記錄MAC MOVE通知，因為以前的ASA的MAC地址是通過直連介面獲知的，現在通過OTV鏈路獲知。

### 建議

這是一個角落方案。MAC表在群集中同步，因此成員沒有特定主機的條目的可能性較低。對於群集擁有的BVI MAC，偶爾MAC移動被認為是可接受的。

## 案例 2

ASA的集中式流處理，如下圖所示：




ASA集群中基於檢測的流量分為三種型別：

- 集中式
- 已發佈
- 半分散式

在集中式檢查的情況下，需要檢查的任何流量都會重定向到ASA集群的主裝置。如果ASA集群的從屬裝置收到流量，則通過CCL將其轉發到主機。

在前面的影象中，使用的是集中式檢查協定(CIP)的SQL流量，此處描述的行為適用於任何CIP。

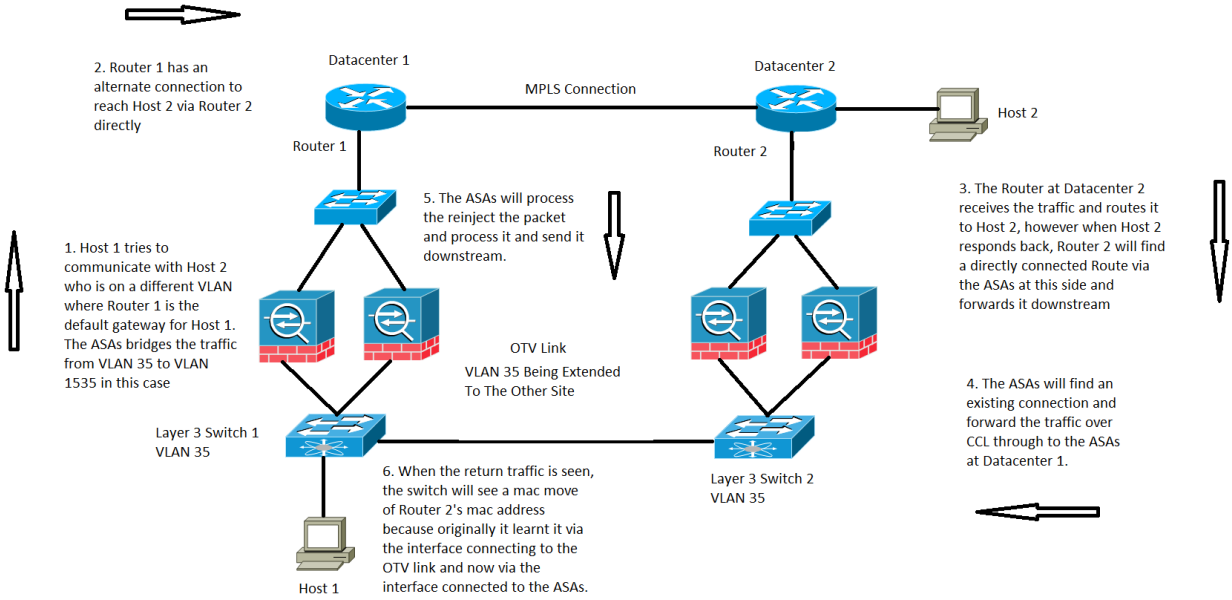
您會在資料中心2上接收流量，其中只有ASA集群的從屬裝置，主裝置位於資料中心1，即ASA 1。

1. 資料中心2上的ISP路由器2接收流量，並將其向下轉發到其站點的ASA。
2. 其中一個ASA可以接收此流量，一旦它確定需要檢查此流量，當協定集中時，它會通過CCL將流量轉發到主裝置。
3. ASA 1通過CCL接收流量，處理流量並將其下發到SQL Server。
4. 現在，當ASA 1將流量轉發到下游時，它將保留位於資料中心2的ISP路由器2的原始源mac地址並將其傳送到下游。
5. 當交換機1收到此特定流量時，它會登入MAC MOVE通知，因為它最初通過連線到資料中心2的OTV鏈路看到ISP Router 2的MAC地址，現在它看到來自連線到ASA 1的介面的流量。

**建議**

建議根據優先順序將集中連線路由到託管主機的任何站點，如下圖所示：

## 案例 3

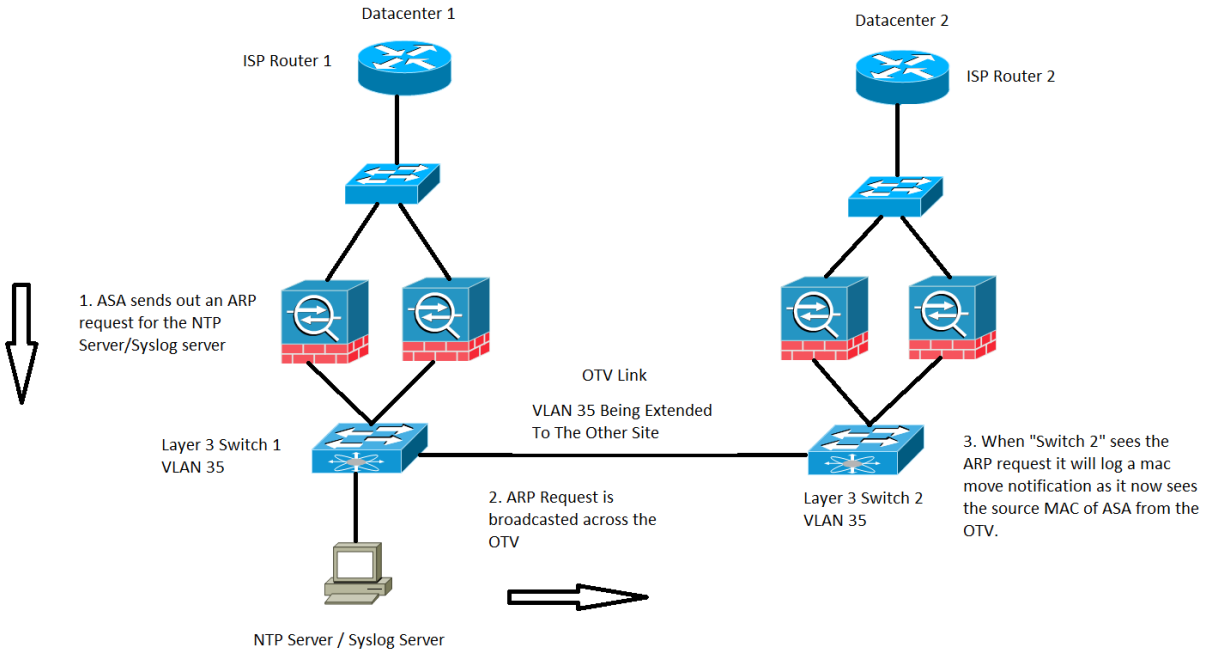



對於透明模式下的域間控制器(DC)通信，此特定流量流不涵蓋或記錄，但從ASA流量處理的角度來看，此特定流量流確實有效。但是這會在交換器上產生MAC移動通知。

1. VLAN 35上的主機1嘗試與另一個資料中心上的主機2通訊。
2. 主機1有一個預設網關，即路由器1，而路由器1具有到達主機2的路徑，它可以通過備用鏈路直接與路由器2通訊。在這種情況下，我們假設使用多協定標籤交換(MPLS)，而不是通過ASA集群。
3. Router 2收到傳入流量並將其路由到主機2。
4. 現在，當主機2作出響應時，路由器2收到返回流量，它通過ASA找到直接連線的路由，而不是通過MPLS傳送的流量。
5. 在這個階段，離開Router 2的流量具有Router 2送出介面的來源MAC。
6. 資料中心2的ASA接收返回流量，並查詢存在且由資料中心1的ASA建立的連線。
7. 資料中心2的ASA通過CCL將返回流量傳送回資料中心1的ASA。
8. 在這個階段，資料中心1的ASA處理返回流量並將其向下傳送到交換機1。資料包的源MAC仍然與路由器2送出介面的源MAC相同。
9. 現在，交換機1收到資料包後，會記錄MAC移動通知，因為最初它通過連線到OTV鏈路的介面獲取了Router 2的MAC地址，但在此階段，它開始從連線到ASA的介面獲取MAC地址。

## 案例 4

ASA生成的流量，如下圖所示：

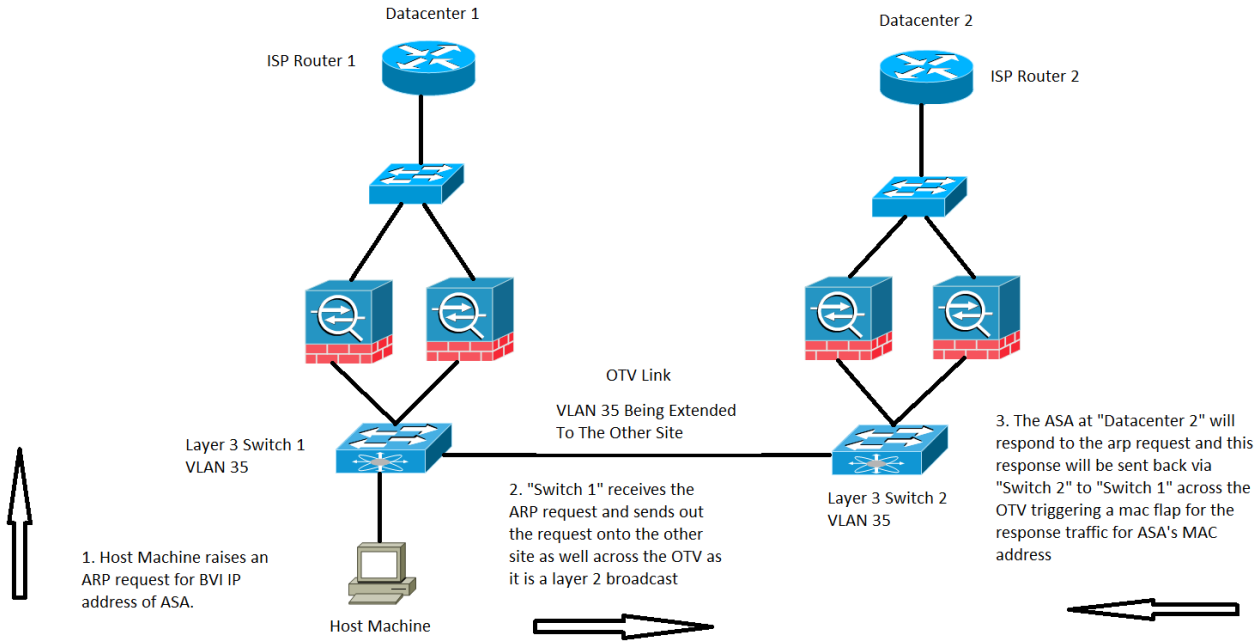



對於ASA自身生成的任何流量，將觀察此特定情況。這裡考慮了兩種可能的情況，其中ASA嘗試訪問網路時間協定(Network Time Protocol, NTP)或系統日誌伺服器，它們與其BVI介面位於同一子網中。但是，它不僅限於這兩種情況，只要流量由ASA為直接連線到BVI IP地址的任何IP地址生成，就可能會出現這種情況。

1. 如果ASA沒有NTP伺服器/系統日誌伺服器的ARP資訊，則ASA將為該伺服器生成ARP請求。
2. 由於ARP請求是一個廣播資料包，因此交換機1將從ASA的已連線介面接收此資料包，並通過特定VLAN中的所有介面（包括通過OTV的遠端站點）將其泛洪。
3. 遠端站點交換機2將從OTV鏈路收到此ARP請求，由於ASA的源MAC，它會生成一個MAC擺動通知，因為相同的MAC地址通過OTV通過其與ASA直連的本地介面獲知。

## 案例 5

從直連主機發往ASA的BVI IP地址的流量，如下圖所示：



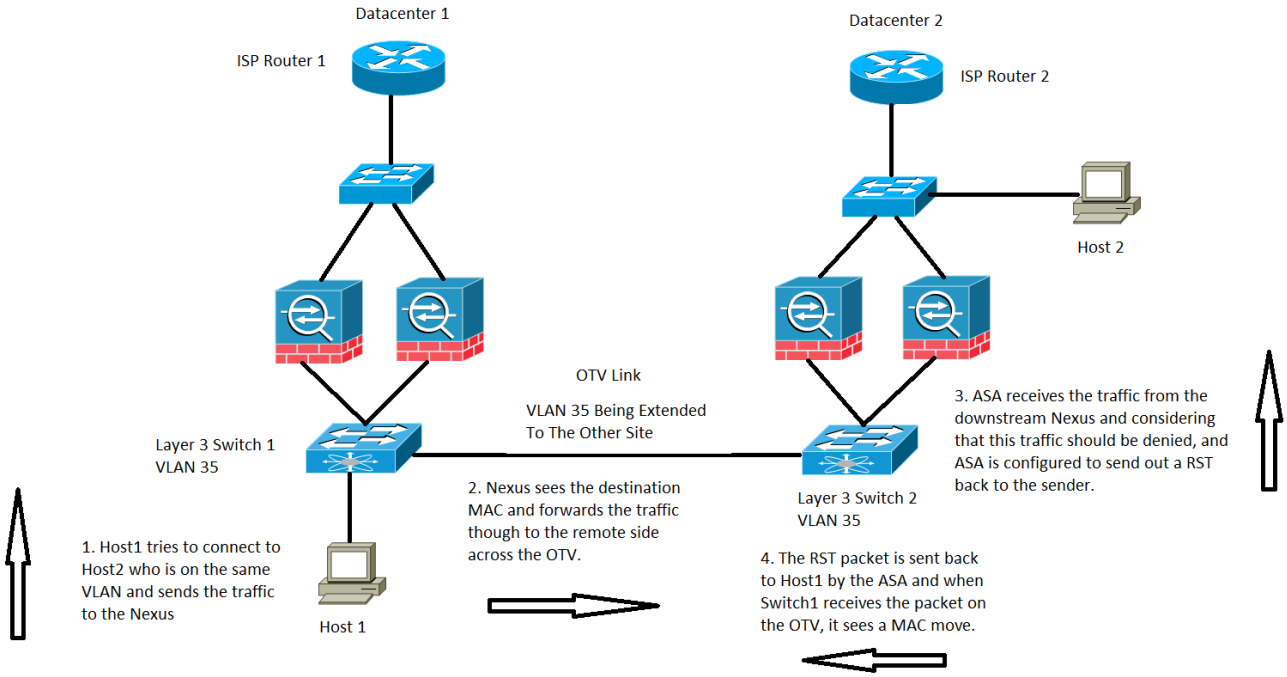

在流量目的地為ASA的BVI IP地址時，也可以觀察MAC移動。

在此場景中，ASA直連網路上的主機電腦正在嘗試連線到ASA。

1. 主機沒有ASA的ARP並觸發ARP請求。
2. Nexus接收流量，由於是廣播流量，因此它還會通過OTV將流量傳送到另一個站點。
3. 遠端資料中心2上的ASA可以響應ARP請求，並通過與遠端端交換機2、本地端交換機1和終端主機相同的路徑傳送流量。
4. 在本地交換機1上看到ARP響應時，它會觸發一個MAC移動通知，因為它看到來自OTV鏈路的ASA的MAC地址。

## 案例 6

ASA設定為拒絕其將RST傳送到主機的流量，如下圖所示：




在本例中，主機1位於VLAN 35上，它嘗試與同一第3層VLAN中的主機2通訊，但是，主機2實際上位於資料中心2 VLAN 1535上。

1. 通過連線到ASA的介面，在交換機2上可以看到主機2MAC地址。
2. 交換機1通過OTV鏈路檢視主機2的MAC地址。
3. 主機1將流量傳送到主機2，該流量沿交換機1、OTV、交換機2、資料中心的ASA的路徑傳輸。
4. ASA會拒絕此特定資料包，由於ASA配置為將RST發回主機1，因此RST資料包將返回ASA的源MAC地址。
5. 當此資料包通過OTV返回到交換機1時，交換機1會記錄有關ASA MAC地址的MAC MOVE通知，因為它現在通過OTV看到該MAC地址，而在此之前，它會從其直連介面看到該地址。

# 驗證

目前沒有適用於此組態的驗證程序。

# 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

- Cisco ASA系列CLI配置指南
- 技術支援與文件 - Cisco Systems