ASA站点间透明集群的常见问题

目录

本文档介绍跨网络EtherChannel透明模式站点间集群的一些常见问题。

Cisco

- 自适应安全设备(ASA)防火墙
- ASA集群

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

从ASA版本9.2开始，支持站点间集群，其中ASA设备可位于不同的数据中心，并且集群控制链路(CCL)通过数据中心互联(DCI)连接。 可能的部署方案包括：

- 单个接口站点间集群
- 跨网络EtherChannel透明模式站点间集群
- 跨网络EtherChannel路由模式站点间集群（从9.5开始受支持）

MAC移动通知

当内容可寻址存储器(CAM)表中的MAC地址更改端口时，生成MAC MOVE通知。但是，当MAC地址从CAM表中添加或删除时，不会生成MAC MOVE通知。假设如果MAC地址X通过VLAN10中的接口GigabitEthernet0/1获知，并且在一段时间后通过VLAN 10中的GigabitEthernet0/2发现相同的MAC，则会生成MAC MOVE通知。

交换机的系统日志：

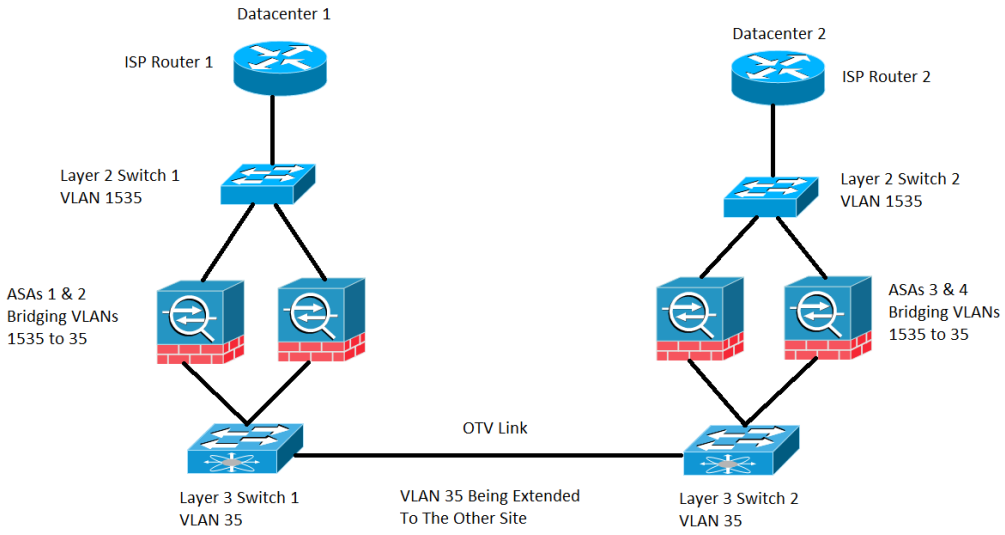
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

从ASA发出的系统日志：

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

网络图

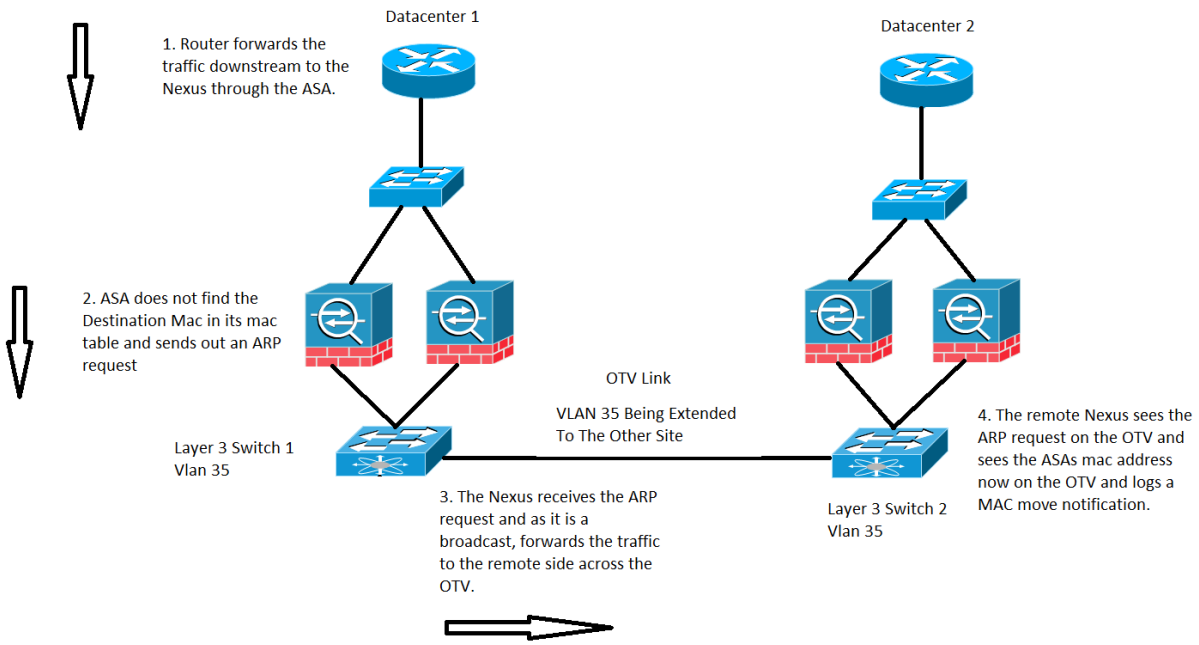
站点间集群部署，其中ASA配置为透明模式桥接VLAN 1535和VLAN 35。内部VLAN 35通过重叠传输虚拟化(OTV)扩展，而外部VLAN 1535不通过OTV扩展，如图所示



交换机上的MAC移动通知

场景 1

发往MAC地址的流量，其条目不在ASA的MAC表中，如图所示：



在透明ASA中，如果到达ASA的数据包的目的MAC地址不在mac地址表中，它会向该目的地（如果与BVI位于同一子网中）发送地址解析协议(ARP)请求，或发送Internet控制消息协议(ICMP)请求，其生存时间为11)缺少源MAC作为网桥虚拟接口(BVI)MAC地址和目的MAC地址作为目的媒体访问控制器(DMAC)。

在上述情况下，您有以下流量：

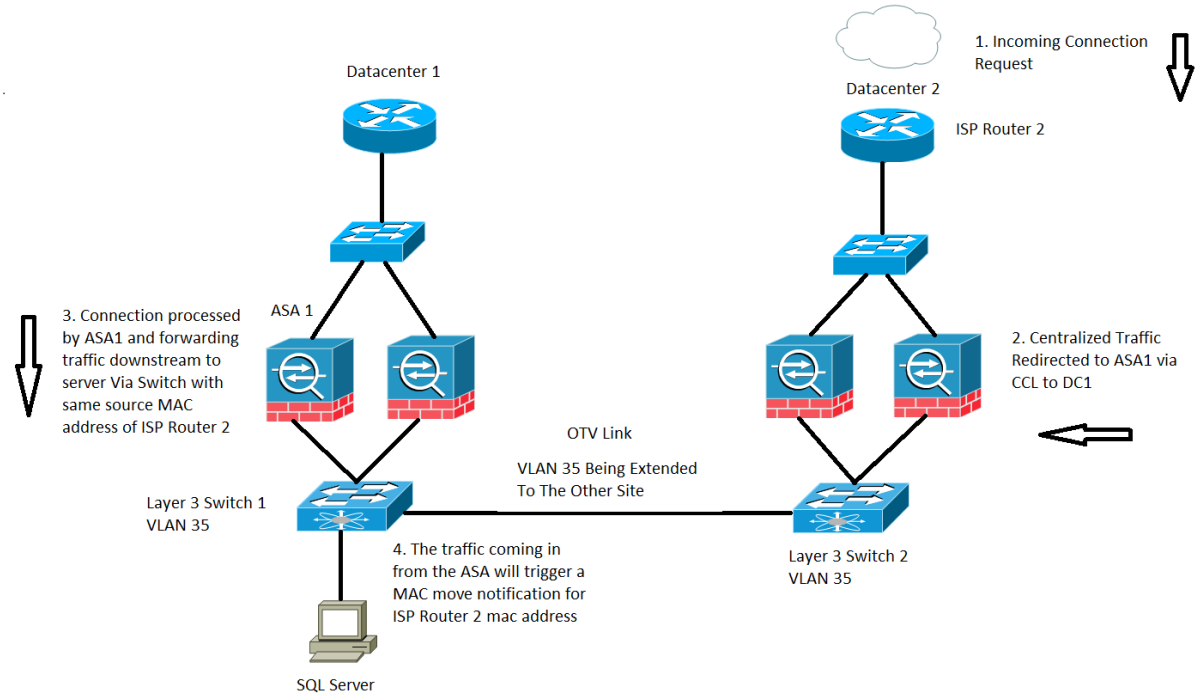
1. 数据中心1上的ISP路由器将流量转发到ASA后面的特定目的地。
2. 任一ASA都可以接收流量，在这种情况下，ASA不知道流量的目标MAC地址。
3. 现在，流量的目标IP与BVI的目标IP位于同一子网中，如前所述，ASA现在生成目标IP的ARP请求。
4. 交换机1接收流量，由于请求是广播，因此它会通过OTV链路将流量转发到数据中心2。
5. 当交换机2在OTV链路上看到来自ASA的ARP请求时，它会记录MAC MOVE通知，因为以前ASA的MAC地址是通过直连接口获取的，现在它通过OTV链路获取。

建议

这是一种拐角方案。MAC表在集群中同步，因此成员没有特定主机条目的可能性较低。集群拥有的BVI MAC偶尔的MAC移动被视为可接受。

场景 2

ASA的集中流处理，如图所示：



跨ASA集群的基于检测的流量分为三种类型：

- 集中
- 分布式
- 半分布式

在集中检查的情况下，需要检查的所有流量都会重定向到ASA集群的主设备。如果ASA集群的从设备收到流量，则通过CCL将其转发到主设备。

在前面的映像中，您使用SQL流量，该流量是集中检查协议(CIP)，此处描述的行为适用于任何CIP。

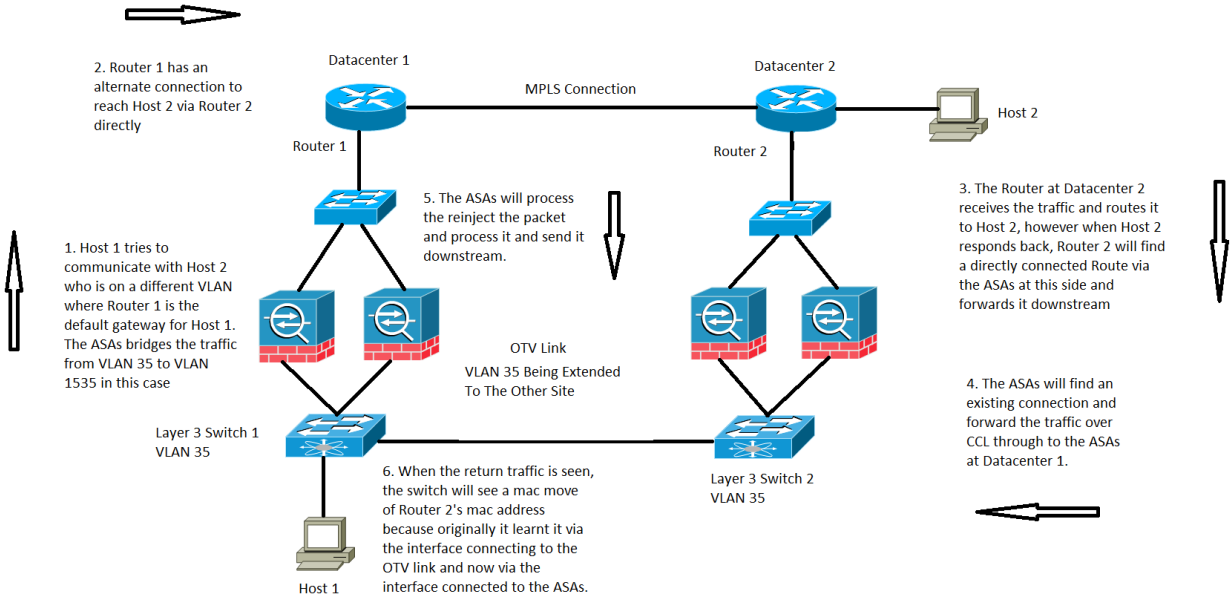
您在数据中心2上收到流量，其中您只有ASA集群的从属设备，主设备位于数据中心1，即ASA 1。

1. 数据中心2上的ISP路由器2接收流量，并将其下行转发到其站点的ASA。
2. 任一ASA都可以接收此流量，一旦确定需要检查此流量，并且当协议集中时，它会通过CCL将流量转发到主设备。
3. ASA 1通过CCL接收流量，处理流量并将其下行发送到SQL Server。
4. 现在，当ASA 1向下游转发流量时，它会保留位于数据中心2的ISP路由器2的原始源mac地址，并将其发送到下游。
5. 当交换机1收到此特定流量时，它会登录MAC MOVE通知，因为它最初通过连接到数据中心2的OTV链路看到ISP路由器2的MAC地址，现在它看到从连接到ASA 1的接口传入的流量。

建议

建议将集中连接路由到主站点（基于优先级）的任意一个站点，如图所示：

场景 3

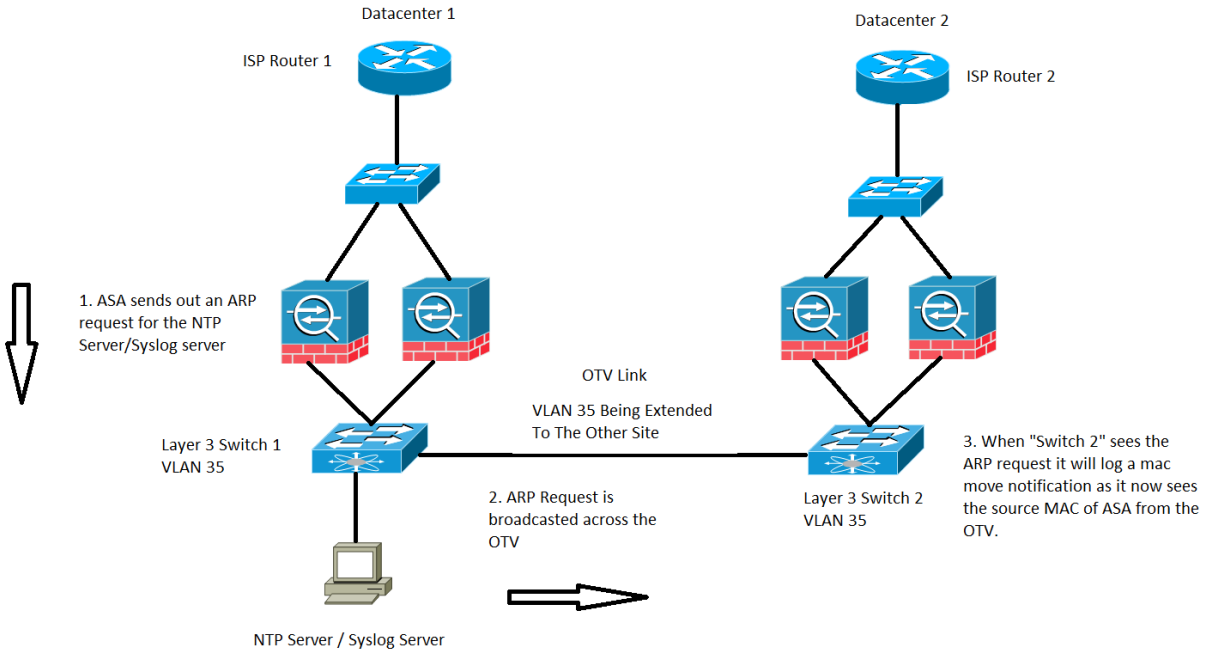


对于透明模式下的域间控制器(DC)通信，此特定流量不会被覆盖或记录，但此特定流量确实从ASA流处理的角度起作用。但是，它可能导致交换机上的MAC移动通知。

1. VLAN 35中的主机1尝试与位于另一数据中心的主机2通信。
2. 主机1具有默认网关，即路由器1，路由器1具有到达主机2的路径，方法是能够通过备用链路直接与路由器2通信。在本例中，我们假定是多协议标签交换(MPLS)，而不是通过ASA集群。
3. 路由器2接收传入流量并将其路由到主机2。
4. 现在，当主机2回复时，路由器2收到返回流量，它通过ASA找到直连路由，而不是通过MPLS发送的流量。
5. 在此阶段，离开路由器2的流量具有路由器2送出接口的源MAC地址。
6. 位于数据中心2的ASA接收返回流量，并查找存在且由位于数据中心1的ASA建立的连接。
7. 数据中心2的ASA通过CCL将返回流量发回数据中心1的ASA。
8. 在此阶段，数据中心1的ASA处理返回的流量，并将其向下发送到交换机1。数据包的源MAC仍与路由器2的送出接口相同。
9. 现在，当交换机1收到数据包时，它会记录MAC移动通知，因为最初它通过连接到OTV链路的接口获知了路由器2的MAC地址，但在此阶段，它开始从连接到ASA的接口获知MAC地址。

场景 4

ASA生成的流量，如图所示：

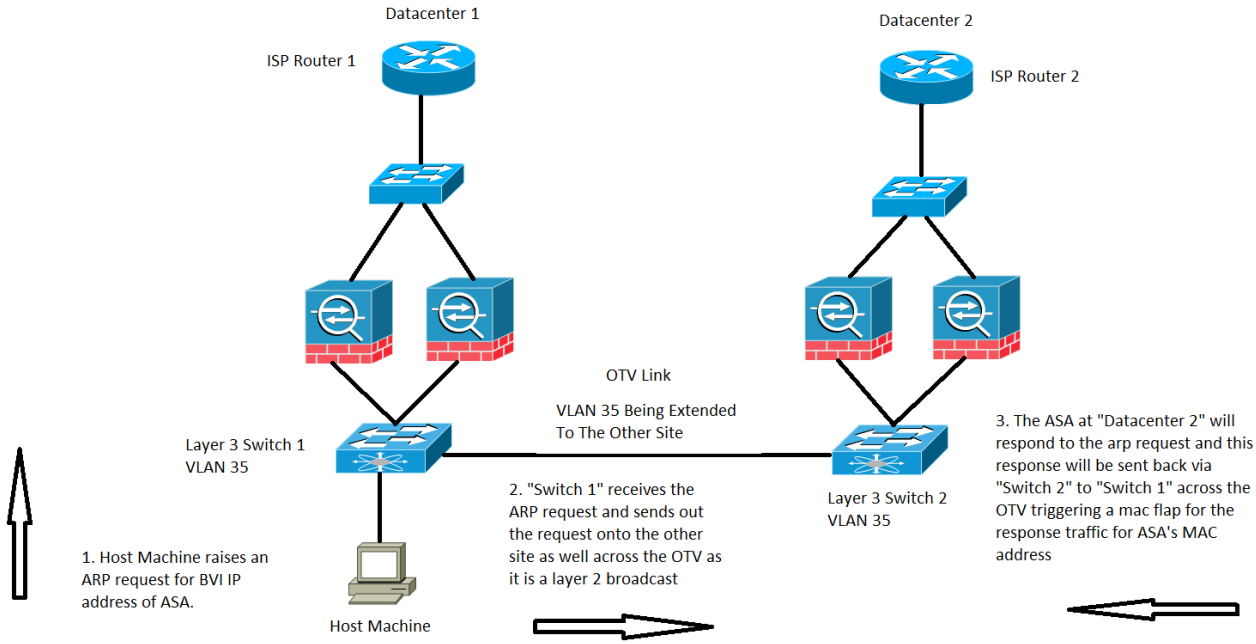


对于ASA自身生成的任何流量，将观察此特定情况。这里考虑了两种可能的情况，其中ASA尝试访问与其BVI接口位于同一子网的网络时间协议(NTP)或系统日志服务器。但是，它不仅限于这两种情况，每当ASA为直接连接到BVI地址的任何IP地址生成流量时，都会发生这种情况。

1. 如果ASA没有NTP服务器/系统日志服务器的ARP信息，则ASA将为该服务器生成ARP请求。
2. 由于ARP请求是广播数据包，因此交换机1将从其ASA的连接接口接收此数据包，并将其泛洪到特定VLAN中的所有接口，包括OTV上的远程站点。
3. 远程站点交换机2将从OTV链路接收此ARP请求，由于ASA的源MAC，它会生成MAC抖动通知，因为通过OTV的本地直连接口，ASA获知了相同的MAC地址。

方案 5

从直连主机发往ASA的BVI IP地址的流量，如图所示：



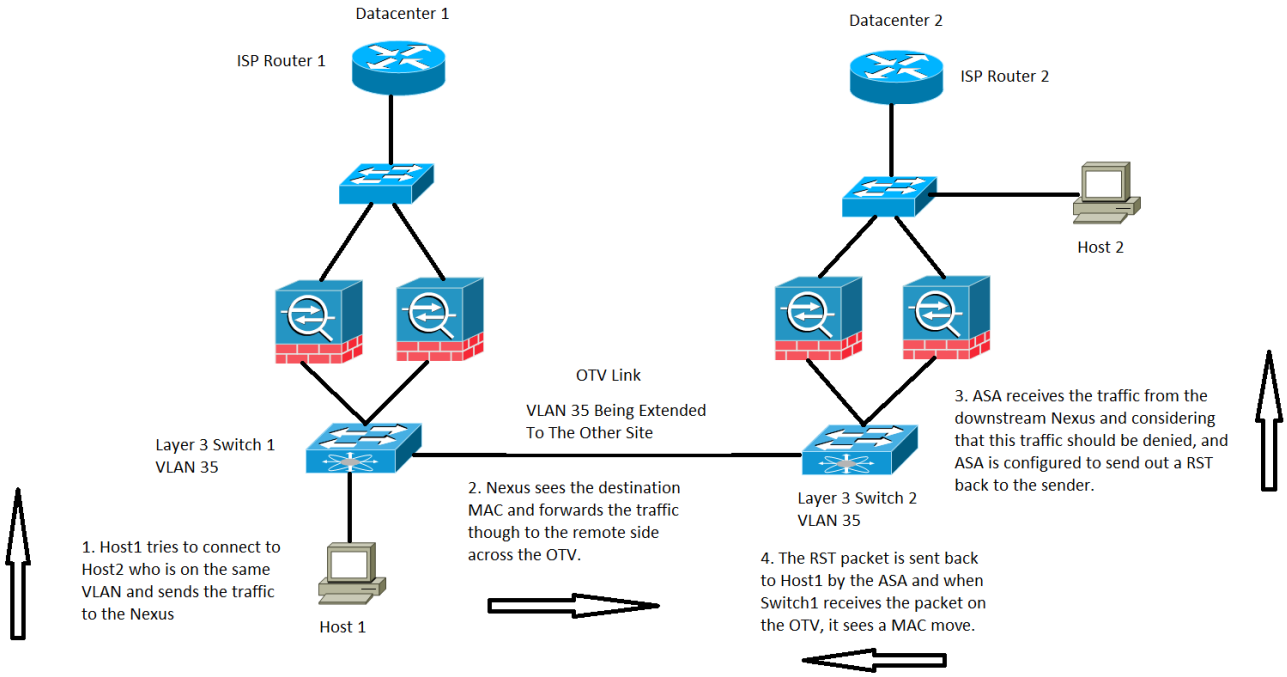
当流量发往ASA的BVI IP地址时，也可以观察MAC MOVE。

在场景中，我们在ASA的直连网络上拥有一台主机，并且正尝试连接到ASA。

1. 主机没有ASA的ARP并触发ARP请求。
2. Nexus会接收流量，并再次作为广播流量通过OTV将流量发送到另一站点。
3. 远程数据中心2上的ASA可以响应ARP请求，并通过远程端的交换机2、本地端的OTV、交换机1以及终端主机的相同路径发回流量。
4. 当在本地端交换机1上看到ARP响应时，它会触发MAC移动通知，因为它会看到从OTV链路进入的ASA的MAC地址。

方案 6

ASA设置为拒绝与其一起向主机发送RST的流量，如图所示：



在本例中，VLAN 35中有一台主机Host 1，它尝试与同一第3层VLAN中的主机2通信，但是，主机2实际上位于数据中心2 VLAN 1535中。

1. 通过连接到ASA的接口，可在交换机2上看到主机2的MAC地址。
2. 交换机1将通过OTV链路看到主机2的MAC地址。
3. 主机1将流量发送到主机2，这遵循位于数据中心2的交换机1、OTV、交换机2和ASA的路径。
4. ASA拒绝此特定数据包，并且当ASA配置为向主机1发回RST时，RST数据包返回ASA的源MAC地址。
5. 当此数据包通过OTV返回到交换机1时，交换机1会记录ASA MAC地址的MAC MOVE通知，因为它现在可以在OTV上看到MAC地址，在它从其直连接口看到该地址之前。

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

- Cisco ASA系列CLI配置指南
- 技术支持和文档 - Cisco Systems