ASA站点间透明集群的常见问题

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

MAC移动通知

网络图

交换机上的MAC移动通知

- 场景 1
  - 建议
- 场景 2
  - 建议
- 场景 3
- 场景 4
- 方案 5
- 方案 6

验证

故障排除

相关信息

简介

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。

先决条件

要求

Cisco 建议您了解以下主题：

- 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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

从ASA 9.2版开始，支持站点间集群，其中ASA单元可以位于不同的数据中心，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，会生成MAC MOVE通知。但是，在CAM表中添加或删除MAC地址时，不会生成MAC MOVE通知。假设通过VLAN10中的接口GigabitEthernet0/1获知MAC地址X，一段时间后，通过VLAN 10中的GigabitEthernet0/2看到相同的MAC，则生成MAC MOVE通知。

来自交换机的系统日志：

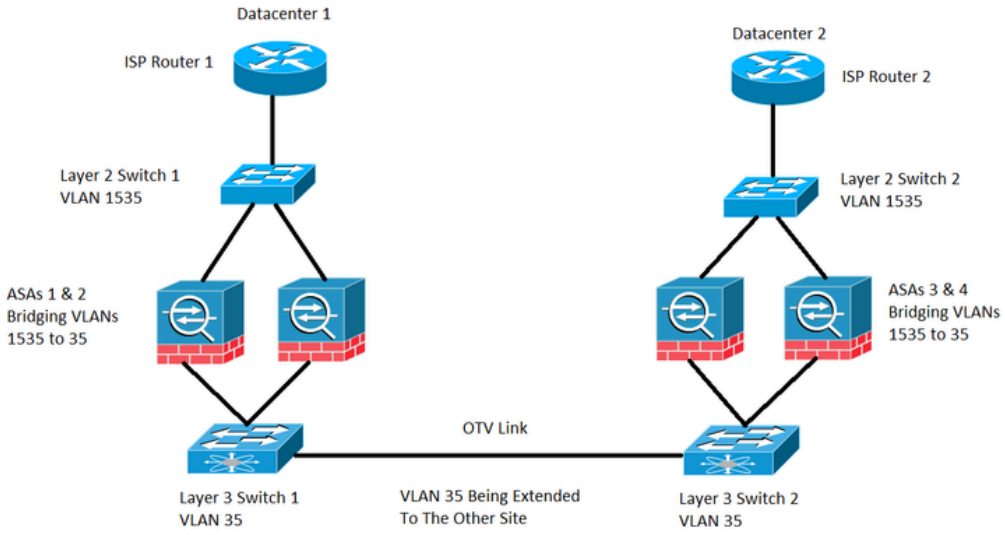
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1 to Gigab
```

来自ASA的系统日志：

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

网络图

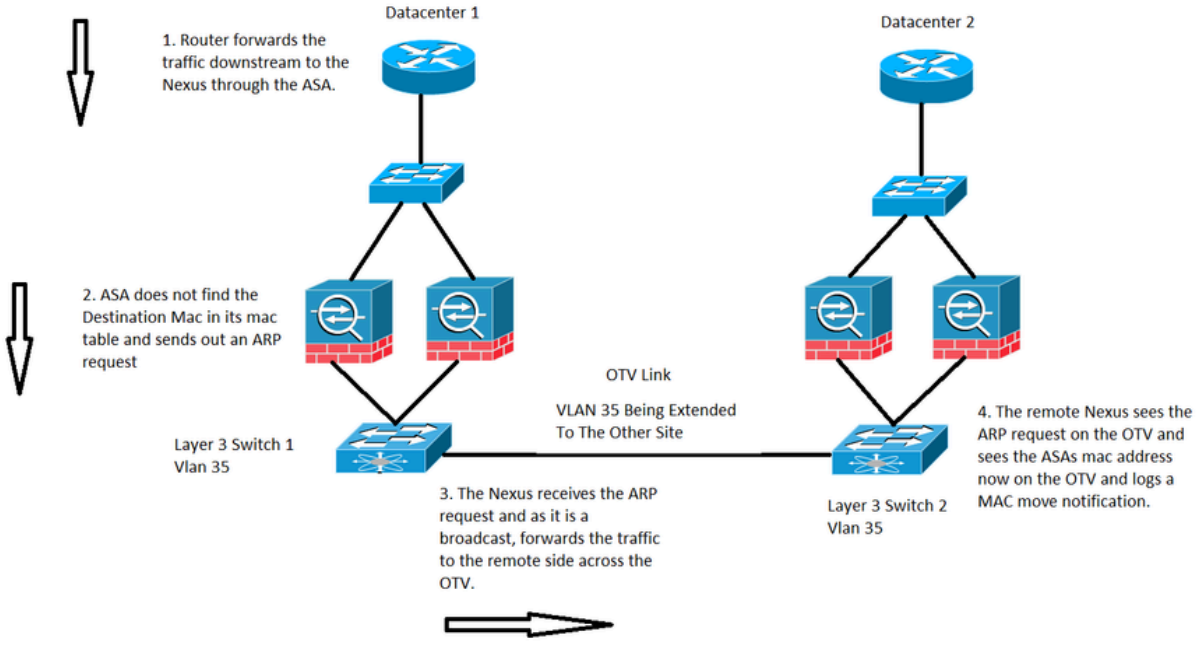
站点间集群部署，其中ASA配置为透明模式桥接VLAN 1535和VLAN 35。内部VLAN 35在重叠传输虚拟化(OTV)上扩展，而外部VLAN 1535未在OTV上扩展，如图所示



交换机上的MAC移动通知

场景 1

流向其MAC地址条目在ASA的MAC表中不存在的MAC地址的流量，如图所示：



在透明ASA中，如果到达ASA的数据包的目标MAC地址不在MAC地址表中，它会发出该目标的地址解析协议(ARP)请求（如果与BVI位于同一子网）或互联网控制消息协议(ICMP)请求，生存时间1(TTL 1)将源MAC作为网桥虚拟接口(BVI)MAC地址，将目标MAC地址作为目标媒体访问控制器(DMAC)丢失。

在前面的案例中，您有以下流量：

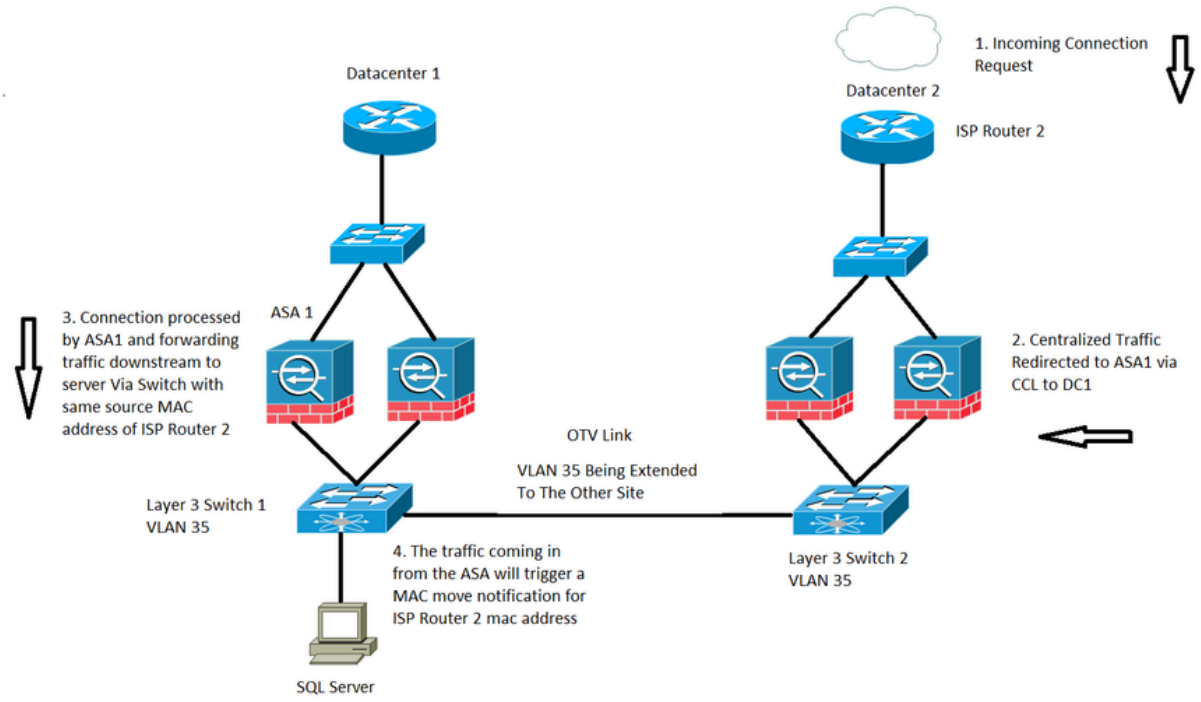
1. 数据中心1上的ISP路由器将流量转发到ASA后的特定目标。
2. 两台ASA都可以接收流量，在这种情况下，ASA不知道流量的目标MAC地址。
3. 现在，流量的目标IP与BVI位于同一子网中，如前所述，ASA现在会为目标IP生成ARP请求。
4. 交换机1接收流量，由于请求是广播，因此它会将流量转发到数据中心2以及通过OTV链路。
5. 当交换机2在OTV链路上看到来自ASA的ARP请求时，它将记录MAC MOVE通知，因为以前的ASA的MAC地址是通过直连接口获知的，现在它是通过OTV链路获知的。

建议

这是一个角落方案。MAC表在集群中同步，因此成员没有特定主机的条目的可能性较低。对于集群拥有的BVI MAC，偶尔MAC移动是可以接受的。

场景 2

ASA的集中式流处理，如图所示：



ASA集群中基于检测的流量分为三种类型：

- 集中式

- 已分发
- 半分布式

对于集中式检查，需要检查的任何流量都会重定向到ASA集群的主设备。如果ASA集群的辅助设备收到流量，则会通过CCL将其转发到主设备。

在早期的映像中，您使用的是集中检测协议(CIP)的SQL流量，此处描述的行为适用于任何CIP。

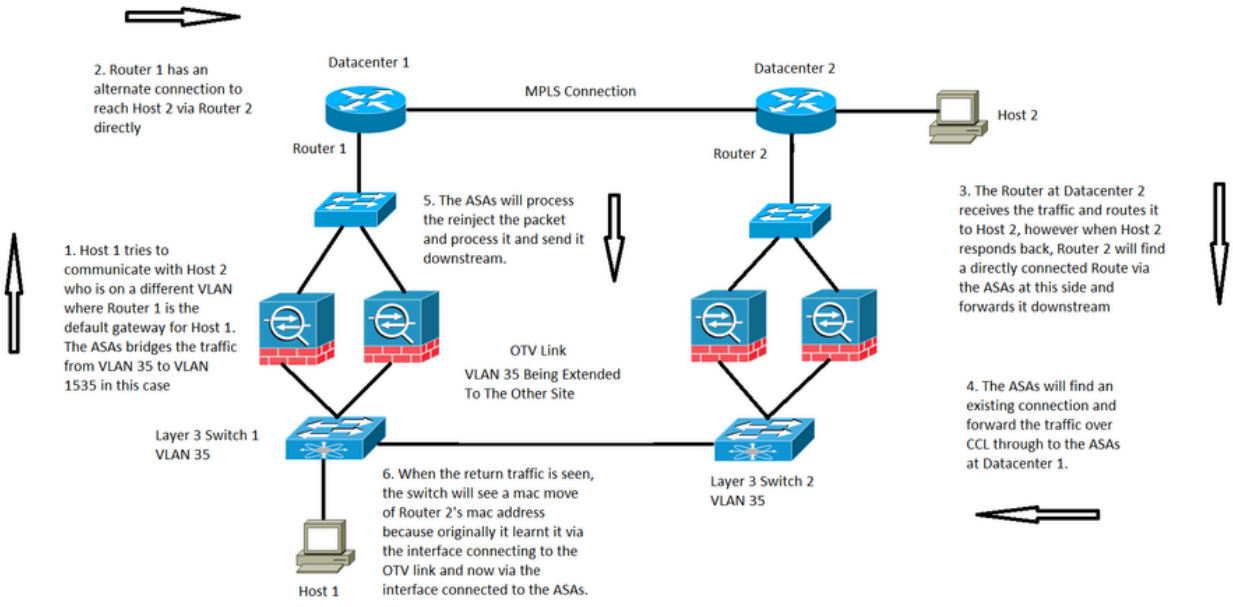
您接收数据中心2上的流量，其中只有ASA集群的辅助设备，主设备位于数据中心1，即ASA 1。

1. 数据中心2上的ISP路由器2接收流量并将其向下转发到其站点的ASA。
2. 任一ASA都可以接收此流量，一旦它确定需要检查此流量，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，处理流量并将其下游发送到SQL Server。
4. 现在，当ASA 1将流量转发到下游时，它将保留位于数据中心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，现在它看到来自连接到ASA 1的接口的流量。

建议

建议根据优先级，将集中连接路由到托管主站点的任何站点，如图所示：

场景 3



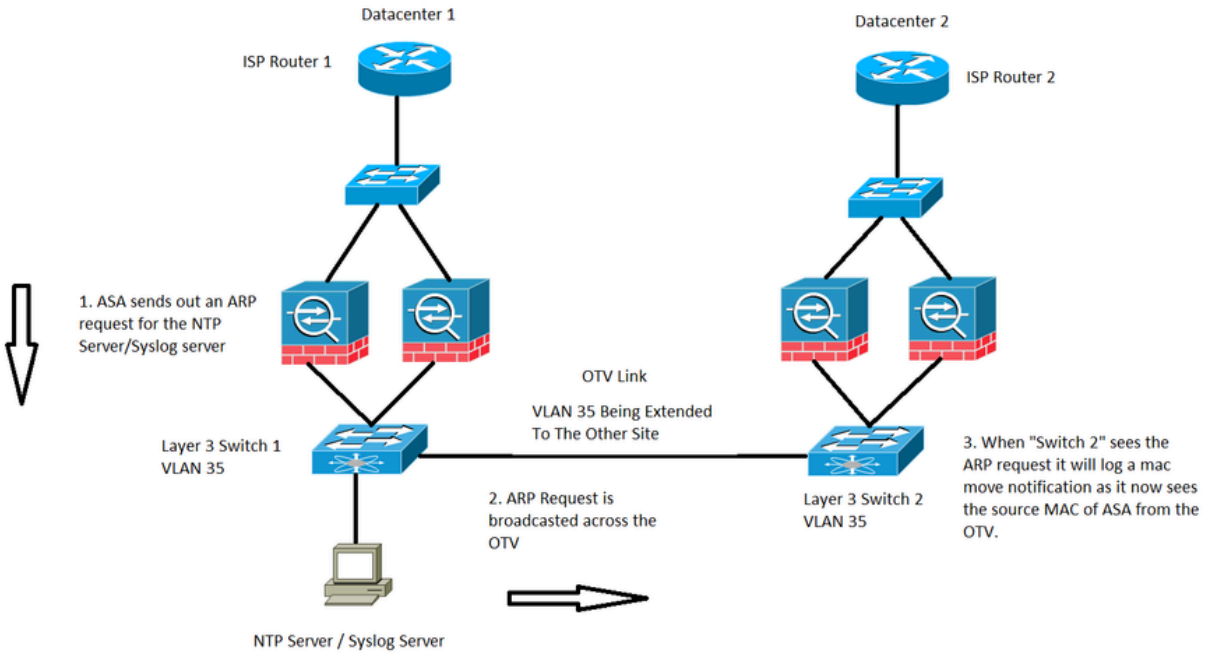
对于透明模式下的域间控制器(DC)通信，不覆盖或记录此特定流量，但从ASA流量处理的角度来看，此特定流量确实有效。但是，它可能会在交换机上产生MAC移动通知。

1. VLAN 35上的主机1尝试与另一个数据中心上的主机2通信。
2. 主机1有一个默认网关，即路由器1，而路由器1具有到达主机2的路径，它可以通过备用链路

直接与路由器2通信，在这种情况下，我们假设使用多协议标签交换(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作出响应时，路由器2收到返回流量，它通过ASA找到直接连接的路由，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。
6. 数据中心2的ASA接收返回流量并查找存在且由数据中心1的ASA建立的连接。
7. 数据中心2的ASA通过CCL将返回流量发送回数据中心1的ASA。
8. 在此阶段，数据中心1的ASA处理返回流量并将其向下发送到交换机1。数据包仍然具有与路由器2送出接口的源MAC相同的源MAC。
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链路的接口获取了路由器2的MAC地址，但在此阶段，它开始从连接到ASA的接口获取MAC地址。

场景 4

ASA生成的流量，如图所示：

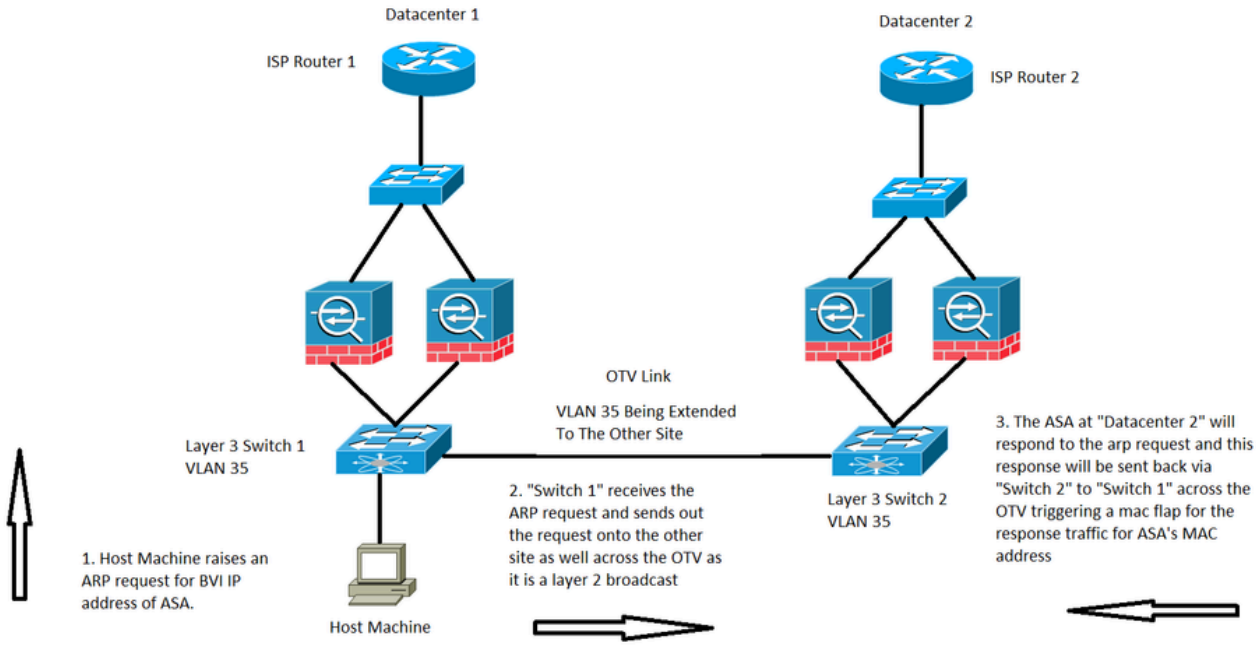


对于ASA自身生成的任何流量，将观察此特定情况。这里考虑了两种可能的情况，其中ASA尝试访问与其BVI接口位于同一子网上的网络时间协议(NTP)或系统日志服务器。但是，不仅限于这两种情况，当ASA为直接连接到BVI IP地址的任何IP地址生成流量时，都会出现这种情况。

1. 如果ASA没有NTP服务器/系统日志服务器的ARP信息，则ASA会为该服务器生成ARP请求。
2. 由于ARP请求是一个广播数据包，因此交换机1将从其ASA的已连接接口接收此数据包，并通过OTV在特定VLAN中的所有接口（包括远程站点）将其泛洪出去。
3. 远程站点交换机2将从OTV链路收到此ARP请求，并且由于ASA的源MAC，它会生成MAC抖动通知，因为同一MAC地址通过OTV的本地直连接口获知到ASA。

方案 5

从直连主机发往ASA的BVI IP地址的流量，如图所示：



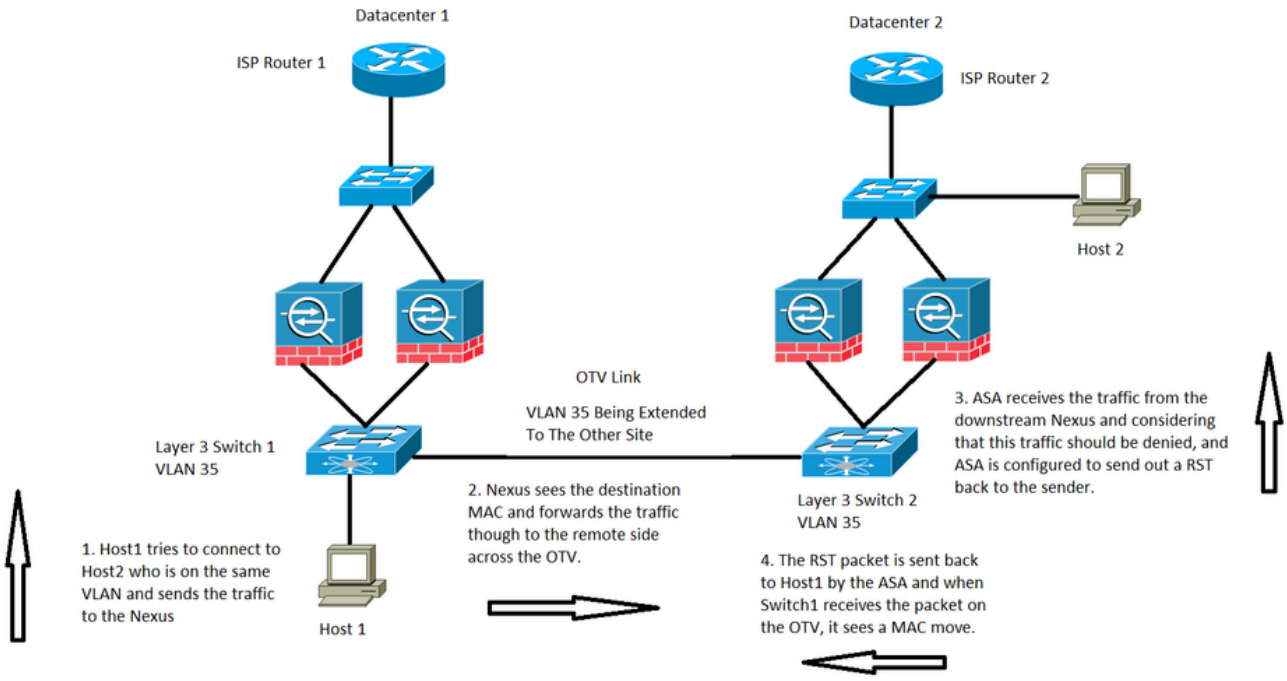
在流量发往ASA的BVI IP地址时，也可以观察MAC MOVE。

在本场景中，ASA直连网络中有一台主机，并且正在尝试连接到ASA。

1. 主机没有ASA的ARP并触发ARP请求。
2. Nexus接收流量，由于它是广播流量，因此它也会通过OTV将流量发送到另一个站点。
3. 远程数据中心2上的ASA可以响应ARP请求，并通过与远程端的交换机2、本地端的交换机1和终端主机相同的路径将流量发送回。
4. 当在本地交换机1上看到ARP响应时，它看到来自OTV链路的ASA的MAC地址时会触发MAC移动通知。

方案 6

如图所示，ASA设置为拒绝与其一起向主机发送RST的流量：



在本例中，主机Host 1位于VLAN 35中，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. 交换机2上通过连接到ASA的接口可以看到主机2MAC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，该流量沿交换机1、OTV、交换机2、数据中心2上的ASA的路径传输。
4. ASA拒绝此特定数据包，并且由于ASA配置为将RST发回主机1，因此RST数据包将返回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，因为它现在在OTV上看到MAC地址，在此之前它会从其直接连接的接口看到该地址。

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。

相关信息

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。