与ASA站点之间透明团星的常见问题

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](#)
[MAC在交换机的移动通知](#)
[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](#)

本文描述某些与被跨过的EtherChannel透明模式站点之间集群的常见问题。

Cisco

- 可适应安全工具(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

开始ASA版本9.2，支持站点之间集群， ASA单元可能查找用不同的datacenters，并且群集控制链路(CCL)在数据中心互连(DCI)连接。可能的部署方案是：

- 单个接口站点之间团星
- 被跨过的EtherChannel透明模式站点之间团星
- 被跨过的EtherChannel已路由模式站点之间团星(向前支持从9.5)

MAC移动通知

当MAC地址在内容可寻址内存(CAM)时表里更换端口， MAC移动通知生成。然而，当MAC地址从CAM表时，被添加或删除MAC移动通知没有生成。假设MAC地址x是否通过在VLAN10的接口GigabitEthernet0/1了解，并且，在一些时间同样MAC通过在VLAN10后的GigabitEthernet0/2被看到，然后MAC移动通知生成。

从交换机的Syslog ：

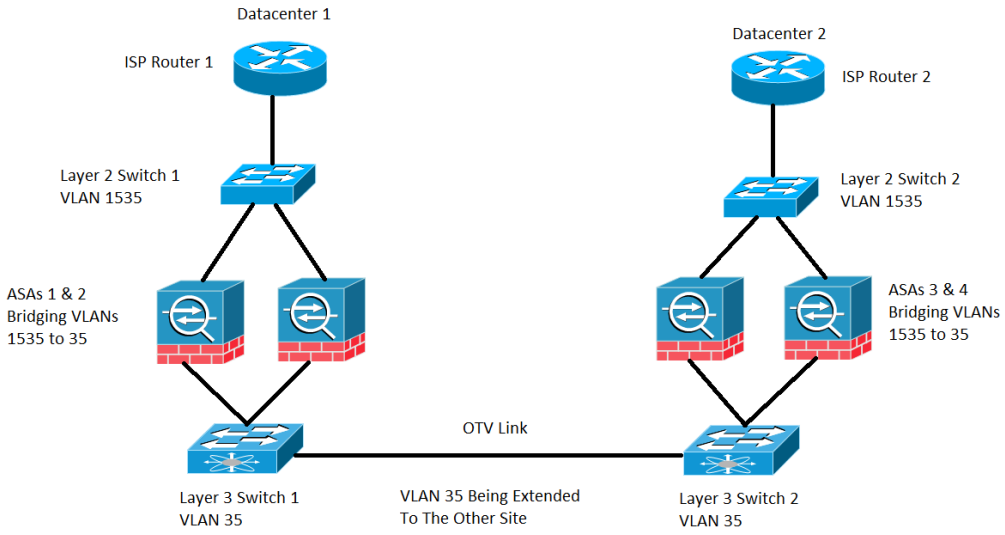
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

从ASA的Syslog ：

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

网络图

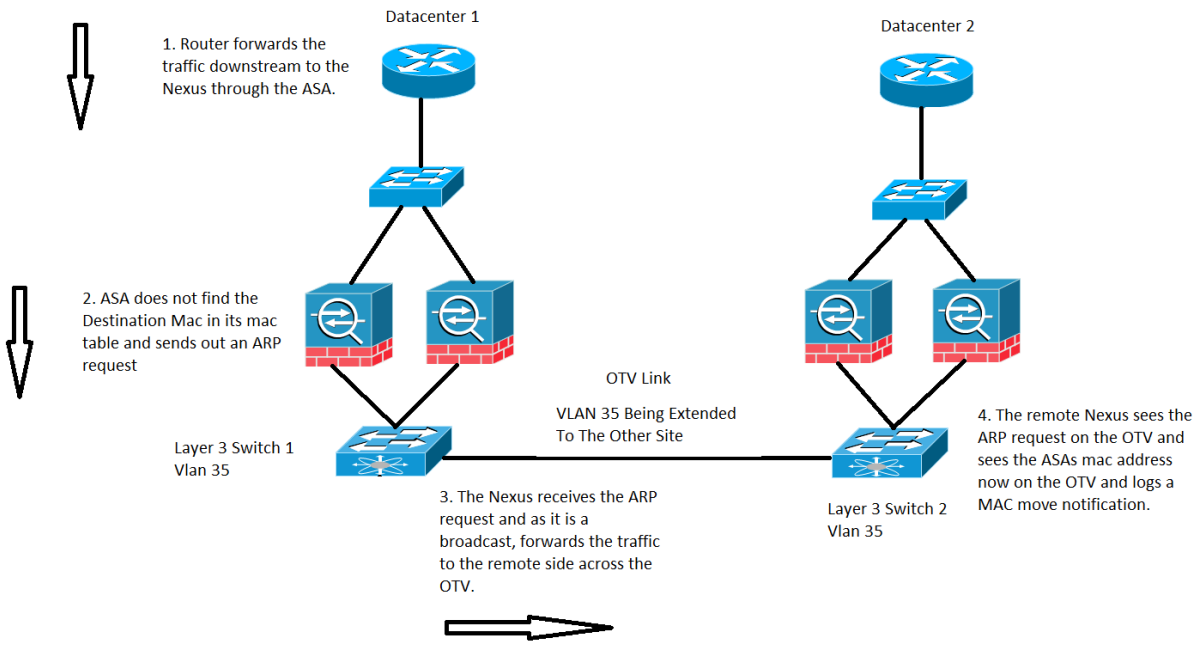
站点之间集群部署， ASA在桥接VLAN 1535和VLAN35的透明模式配置。内部的VLAN35在重叠传输虚拟化(OTV)被扩展，而外层VLAN 1535没有在OTV被扩展，如镜像所显示，



MAC在交换机的移动通知

场景 1

流量被注定对条目不是存在ASA的MAC表的MAC地址，如镜像所显示：



在透明ASA中，如果到达在ASA的数据包的目标MAC地址不在MAC地址表里，它在相同子网派出该目的地的地址解析协议(ARP)请求(如果作为BVI)或与生存时间与源MAC作为网桥虚拟接口(BVI) MAC地址和目标MAC地址的1(TTL 1)的一互联网控制消息协议(ICMP)请求作为目的地媒介访问控制器(DMAC)未命中。

在之前的案件中，您有这些通信流：

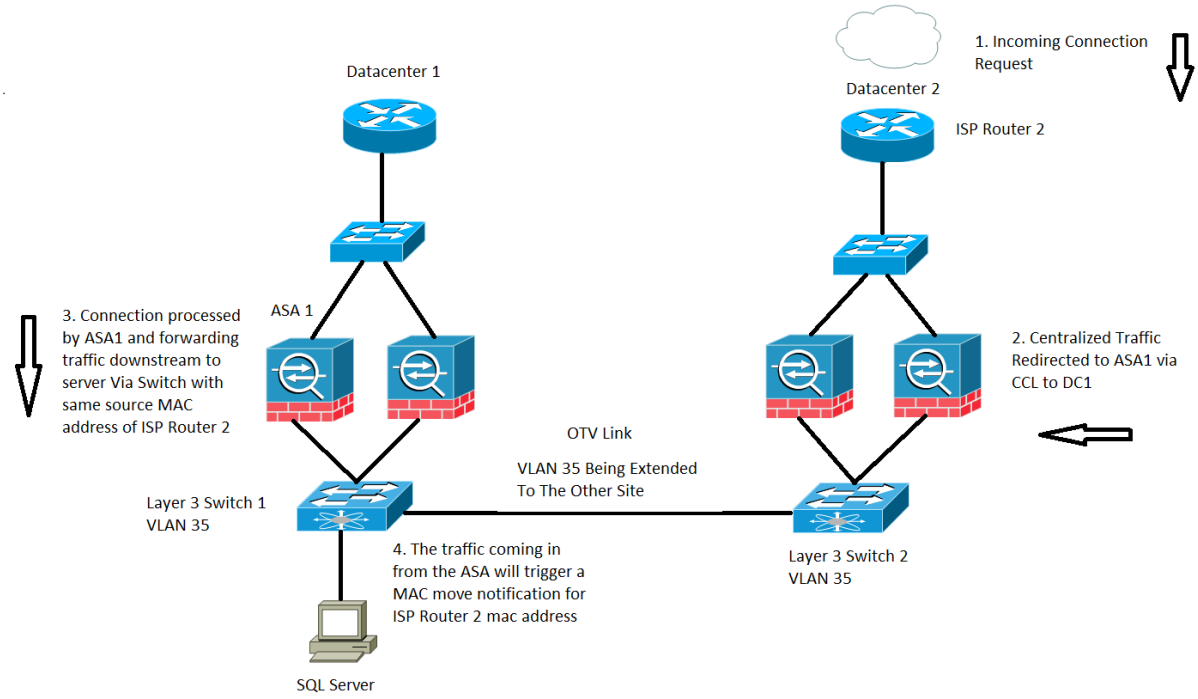
1. 在Datacenter 1的ISP路由器寄流量给是在ASA后的一个特定目的地。
2. ASA之一能收到流量，并且在这种情况下，流量的目标MAC地址不由ASA知道。
3. 现在流量的目的地IP在相同子网和那BVI和如上所述， ASA当前生成目的地IP的一个ARP请求。
4. Switch1收到流量，并且，因为请求是广播，寄流量给Datacenter 2以及在OTV链路间。
5. 当Switch2看到从ASA的ARP请求在OTV链路时，记录MAC移动通知，因为ASA的MAC地址通过连接的接口直接地以前了解，并且通过OTV链路当前了解。

建议

它是壁角方案。 MAC表在集群同步，因此没有特定主机的一个条目成员是不太可能的。团星拥有的BVI MAC的一个偶尔的MAC移动视为可接受。

场景 2

处理由ASA的集中式流，如镜像所显示：



检查在ASA集群间的基于流量分类到三个类型：

- 集中化
- 分布式
- 半分布式

一旦集中化检查，需要获得检查重定向到ASA集群的重要的单元的任何流量。如果ASA集群的一个从属单元收到流量，转发对主控通过CCL。

在更早的镜像，您与是集中化检查协议的SQL流量一起使用(CIP)，并且描述的行为此处为所有CIP是可适用的。

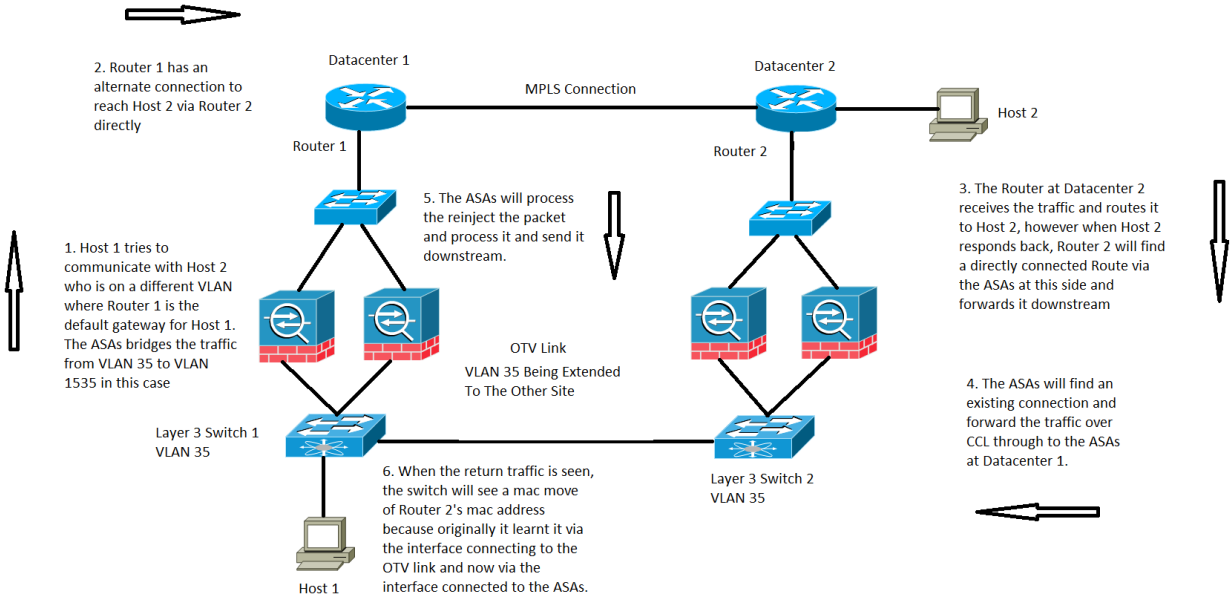
您收到在Datacenter 2的流量您只有ASA集群的从属单元的地方，重要的单元在是ASA 1.的Datacenter 1查找。

1. 在Datacenter 2的ISP Router2收到流量并且转发它下行对ASA在其站点。
2. ASA之一能收到此流量，并且，一旦确定此流量需要被检查，并且，当协议是集中化的它转发流量到重要的单元通过CCL。
3. ASA 1接收通信流通过CCL，处理流量并且发送它下行对SQL server。
4. 现在，当ASA 1转发流量下行时，它保留在Datacenter 2查找ISP Router2的初始源MAC地址并且发送它下行。
5. 当Switch1收到此特定的流量时，登陆MAC移动通知，因为最初看到ISP Router2 MAC地址通过连接对Datacenter 2的OTV链路和它当前看到自接口进来连接对ASA 1.的流量。

建议

推荐路由集中化连接对站点主机主控(根据优先级)，如镜像所显示，：

场景 3

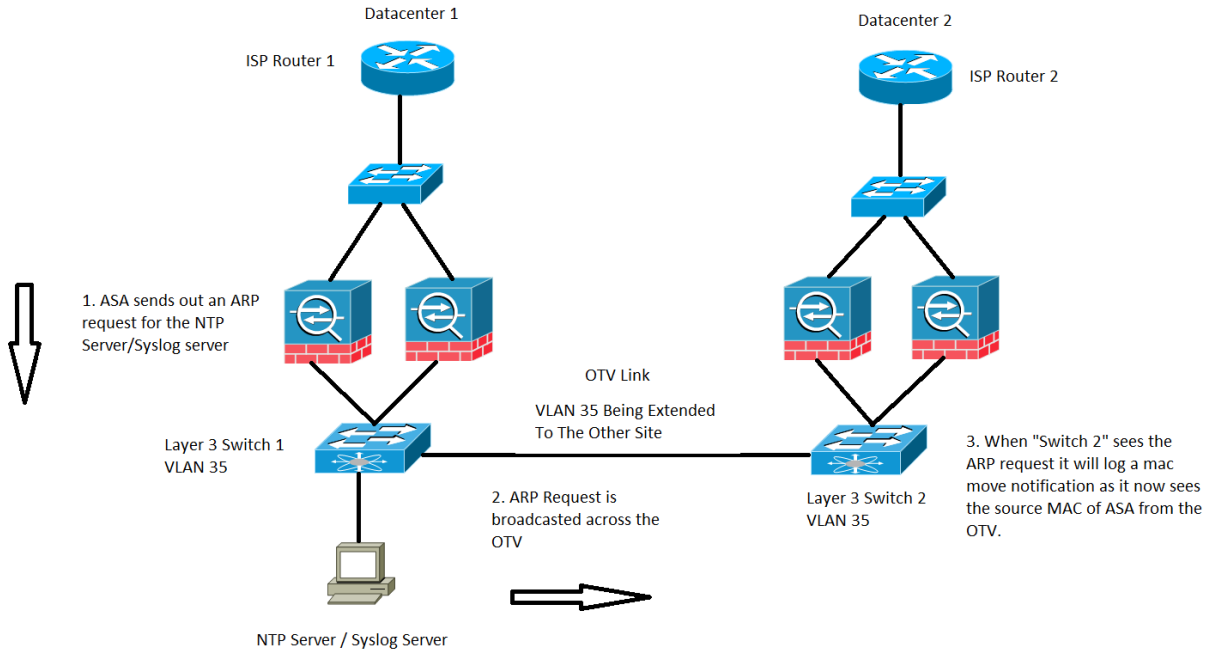


对于在透明模式的一相互域控制器(DC)通信，此特定的流量没有被覆盖或描述，但是此特定的流量从处理支架的ASA流工作。然而，它能导致MAC在交换机的移动通知。

1. 在VLAN35的Host1设法与是存在另一Datacenter的Host2联络。
2. Host1有是路由器1，并且路由器1有一个路径到达Host2由能连通与Router2直接地在备用链路间的默认网关，并且我们在这种情况下假设多协议标签交换(MPLS)和不通过ASA集群。
3. Router2收到流入的数据流并且路由它对Host2。
4. 现在，当Host2响应上一步时， Router2收到回程数据流，并且直接地查找在MPLS发送的一已连接路由通过ASA而不是流量。
5. 在此阶段，离开Router2的流量有Router2's退出接口源MAC。
6. 在Datacenter 2的ASA收到回程数据流并且查找由在Datacenter 1.的ASA存在和做的连接。
7. 在Datacenter 2的ASA送回在CCL的回程数据流到ASA在Datacenter 1。
8. 在此阶段在Datacenter 1的ASA处理回程数据流并且发送它下来往Switch1。数据包仍然有源MAC和那Router2's退出接口一样。
9. 现在，当Switch1收到数据包时，它记录MAC移动通知，因为最初了解在连接对OTV链路的接口间的Router2's MAC地址，然而在此阶段开始学习MAC地址从连接的接口对ASA。

场景 4

ASA生成的流量，如镜像所显示：

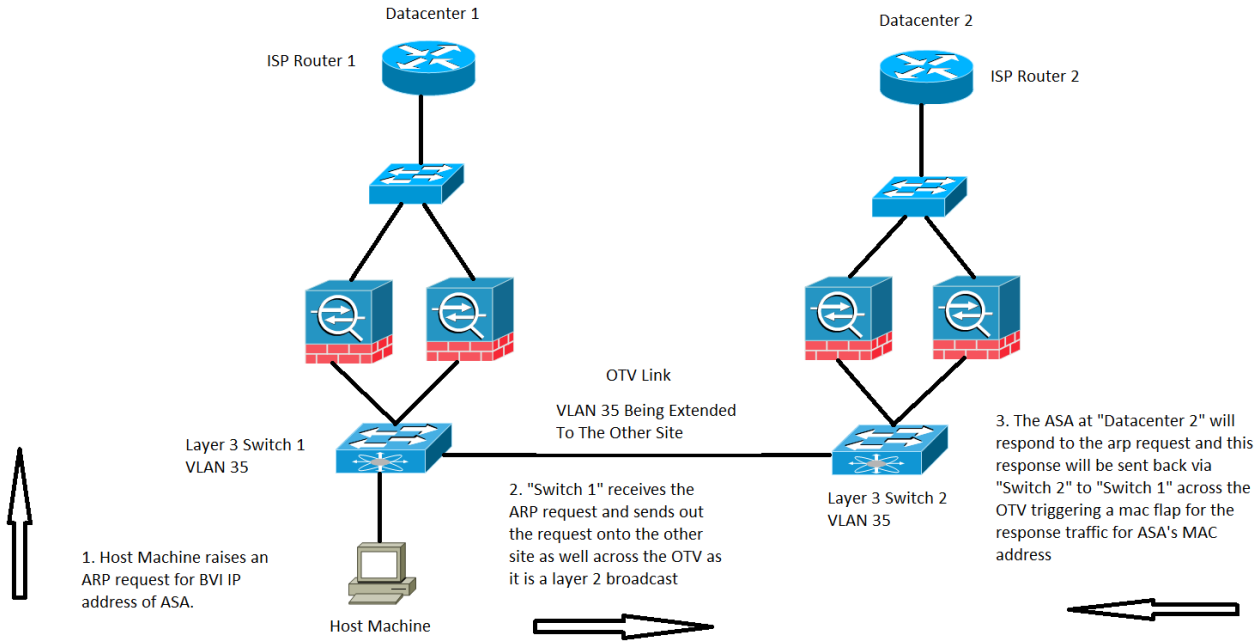


此特定案件对由ASA被生成的所有流量将被观察。此处两个可能的情况考虑， ASA设法到达网络时间协议(NTP)或系统日志服务器，在相同子网作为那其BVI接口。然而它对这两个情况不仅被限制，此情况能发生，每当流量由直接地连接对BVI IP地址的所有IP地址的ASA生成。

1. 如果ASA没有Ntp server/系统日志服务器的ARP信息，则ASA将生成该服务器的一个ARP请求。
2. 因为ARP请求是广播包， Switch1将收到从其ASA的连接的接口的此数据包并且在特定VLAN的所有接口间充斥它包括在OTV间的远程站点。
3. 远程站点Switch2将收到从OTV链路的此ARP请求，并且由于ASA的源MAC，生成MAC摆动通知，因为同一MAC地址在OTV间直接地了解通过其本地连接的接口对ASA。

方案 5

流量直接地被注定了对ASA的BVI IP地址从一台连接的主机的，如镜像所显示：



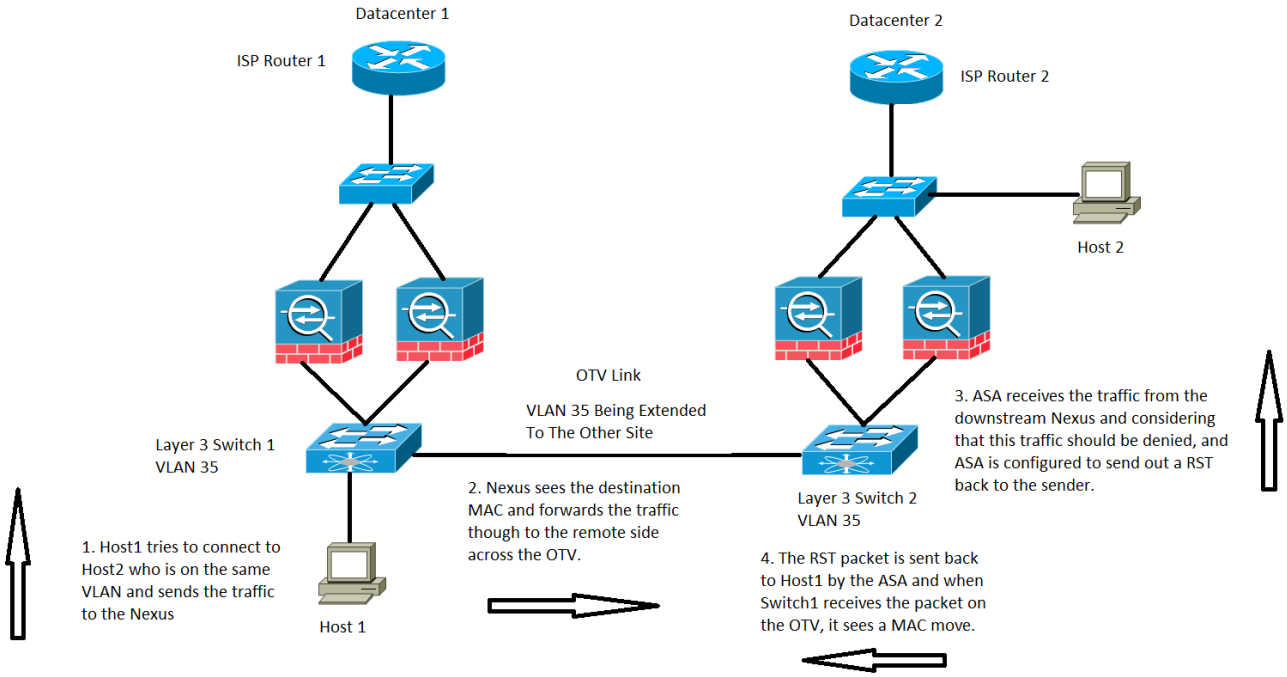
当流量被注定对ASA的BVI IP地址时， MAC移动可能时常也被观察。

在方案中，我们直接地有在ASA的一个连接的网络的一台主机和尝试连接到ASA。

1. 主机没有ASA的ARP并且触发ARP请求。
2. 连结收到流量和再，因为发送在OTV间的流量到另一个站点的它是广播数据流。
3. 在远程Datacenter 2的ASA能回答ARP请求并且退还流量到是在远端、OTV、Switch1在本地端然后终端主机的Switch2的同一个路径。
4. 当ARP响应在本地端Switch1时被看到，触发MAC移动通知，当看到自OTV链路进来ASA的MAC地址。

方案 6

如镜像所显示，设置的ASA否决一起发送RST到主机的流量与， ：



在这种情况下，我们有在VLAN35的一主机Host1，它设法通信与在同样第3层VLAN的Host2，然而，Host2实际上在Datacenter 2 VLAN 1535。

1. 主机2MAC地址在Switch2将被看到通过连接的接口对ASA。
2. Switch1通过OTV链路将看到Host2 MAC地址。
3. Host1发送流量对Host2，并且这在Datacenter 2.跟随Switch1路径，OTV，Switch2，ASA。
4. 此特定由ASA被拒绝，并且，当ASA配置退还RST到Host1，RST数据包回来与ASA的源MAC地址。
5. 当此数据包做它回到在OTV间时的Switch1，Switch1记录ASA的MAC地址的一个MAC移动通知，因为当前看到在OTV间的MAC地址，在直接地看到从其连接的接口前的地址。

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。

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