Common Issues with ASA Inter-Site Transparent Cluster

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

MAC MOVE Notifications

Network Diagram

MAC Move Notifications on Switch

- Scenario 1
  - Recommendations
- Scenario 2
  - Recommendations
- Scenario 3
- Scenario 4
- Scenario 5
- Scenario 6

Verify

Troubleshoot

Related Information

Introduction

This document describes some of the common issues with the Spanned EtherChannel Transparent Mode Inter-Site cluster.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Adaptive Security Appliance (ASA) firewall
- ASA clustering

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Starting ASA version 9.2, inter-site clustering is supported wherein the ASA units could be located in different datacenters and the Cluster Control Link (CCL) is connected over a Data Center Interconnect (DCI). The possible deployment scenarios are:

- Individual Interface Inter-Site Cluster
- Spanned EtherChannel Transparent Mode Inter-Site Cluster
- Spanned EtherChannel Routed Mode Inter-Site Cluster (supported from 9.5 onwards)

MAC MOVE Notifications

When a MAC address in the Content Addressable Memory (CAM) table changes port, a MAC MOVE notification is generated. However, a MAC MOVE notification is not generated when MAC address is added or removed from the CAM table. Suppose if a MAC address X is learned via interface GigabitEthernet0/1 in VLAN10 and after some time the same MAC is seen through GigabitEthernet0/2 in VLAN 10, then a MAC MOVE notification is generated.

Syslog from Switch:

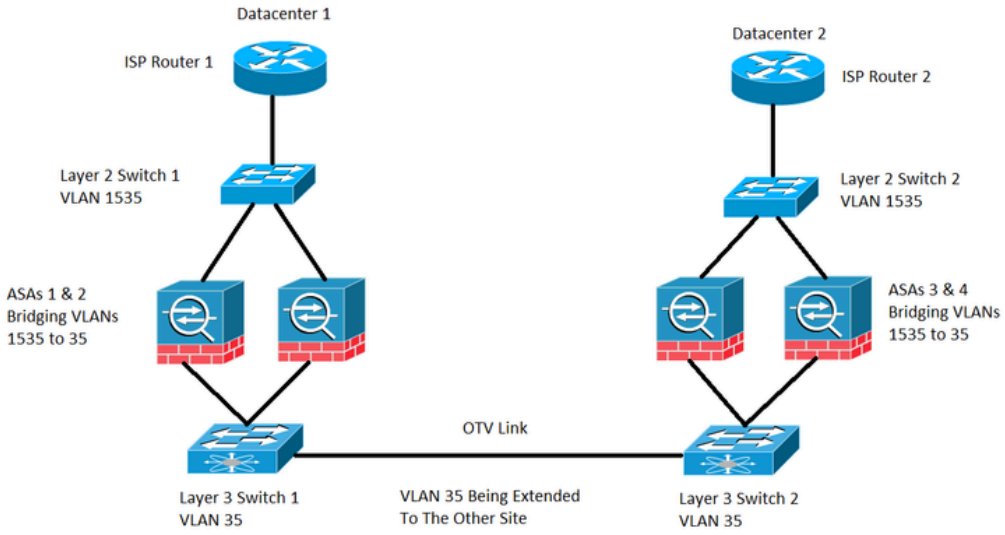
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1 to Gigab
```

Syslog from ASA:

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

Network Diagram

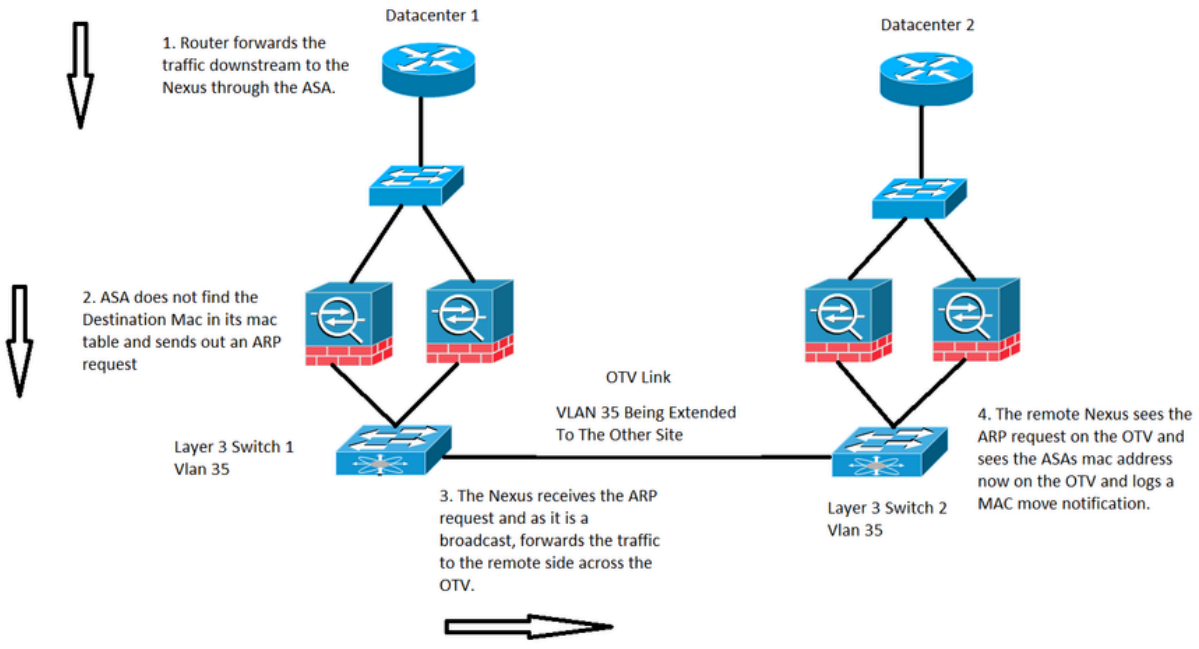
Inter-site cluster deployment wherein the ASAs are configured in transparent mode bridging VLAN 1535 and VLAN 35. The inside VLAN 35 is extended over the Overlay Transport Virtualization (OTV) whereas the outside VLAN 1535 is not extended over the OTV, as shown in the image



MAC Move Notifications on Switch

Scenario 1

Traffic destined to a MAC address whose entry is not present on the ASA's MAC table, as shown in the image:



In a transparent ASA, If the destination MAC address of the packet arriving on the ASA is not in the mac-address table, it sends out an Address resolution Protocol (ARP) request for that destination (if in the same subnet as BVI) or an Internet Control Message Protocol (ICMP) request with Time To Live 1(TTL 1) with source MAC as the Bridge Virtual Interface (BVI) MAC address and destination MAC address as Destination Media Access Controller (DMAC) is missed.

In the preceding case, you have these traffic flow:

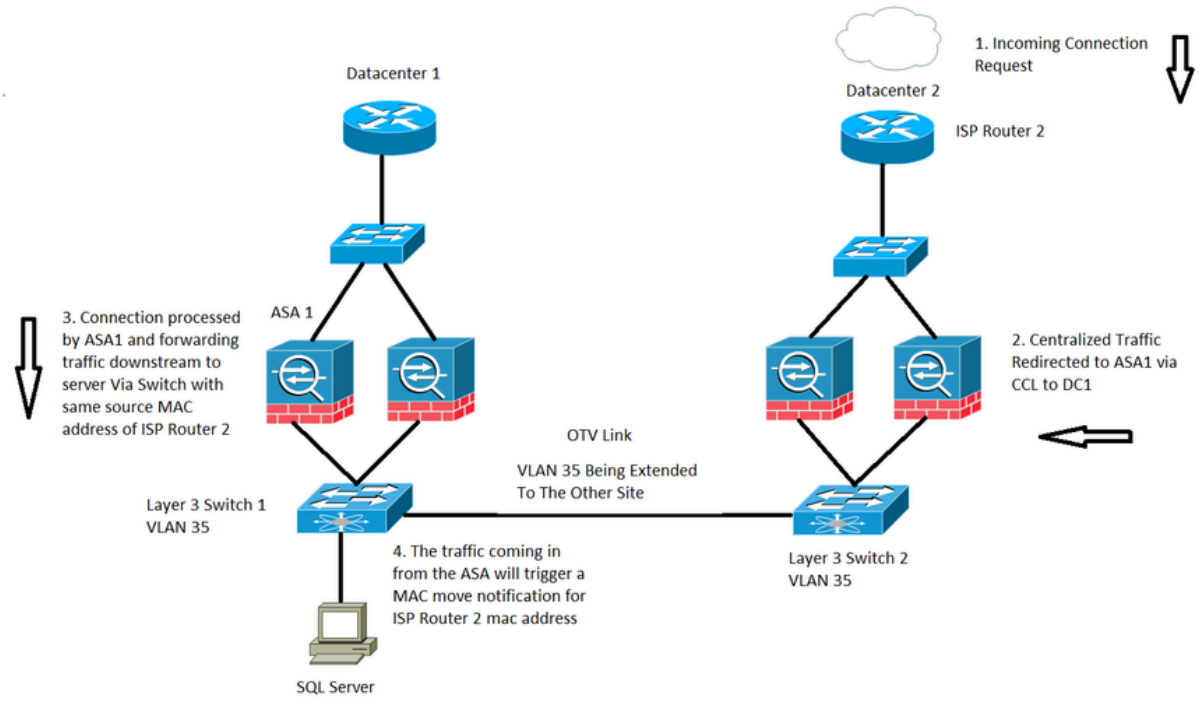
1. The ISP Router on Datacenter 1 forwards traffic to a specific destination which is behind the ASA.
2. Either of the ASA's can receive the traffic and in this case, the destination MAC address of the traffic is not known by the ASA.
3. Now the destination IP of the traffic is in the same subnet as that of the BVI and as mentioned before, ASA now generates an ARP request for the destination IP.
4. The Switch 1 receives the traffic and as the request is a broadcast, it forwards the traffic to Datacenter 2 as well as across the OTV link.
5. When Switch 2 sees the ARP request from the ASA on the OTV link, it logs a MAC MOVE notification because previously ASA's MAC address was learned via directly connected interface and now it is being learned via the OTV link.

Recommendations

It is a corner scenario. MAC tables are synchronized in clusters, so it is less likely for a member to not have an entry for a particular host. An occasional MAC-move for cluster-owned BVI MAC is deemed acceptable.

Scenario 2

Centralized flow processing by ASA, as shown in the image:



Inspection based traffic across an ASA cluster is classified into three types:

- Centralized
- Distributed
- Semi-Distributed

In the case of Centralized inspection, any traffic which needs to get inspected is redirected to the primary unit of the ASA cluster. If a secondary unit of the ASA cluster receives the traffic, it is forwarded to the primary via the CCL.

In the earlier image, you work with SQL traffic which is a Centralized Inspection Protocol (CIP) and the behavior described here is applicable for any CIP.

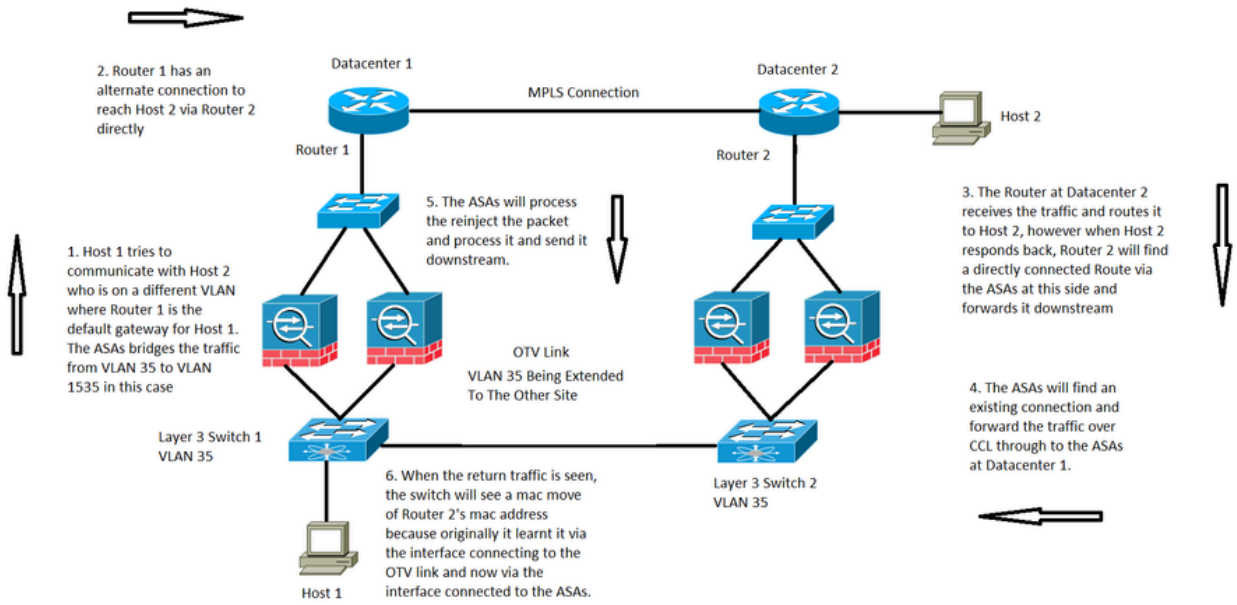
You receive the traffic on Datacenter 2 where you only have secondary units of the ASA cluster, the primary unit is located at Datacenter 1 which is ASA 1.

1. ISP Router 2 on Datacenter 2 receives the traffic and forwards it downstream to the ASAs at its site.
2. Either of the ASAs can receive this traffic and once it determines that this traffic needs to be inspected and as the protocol is centralized it forwards the traffic over to the primary unit via the CCL.
3. ASA 1 receives the traffic flow via the CCL, processes the traffic and sends it downstream to the SQL Server.
4. Now when ASA 1 forwards the traffic downstream, it retains the original source mac address of ISP Router 2 which is located at Datacenter 2 and sends it downstream.
5. When Switch 1 receives this specific traffic, it logs in a MAC MOVE notification because it originally sees ISP Router 2 MAC address via the OTV link which is connected to Datacenter 2 and now it sees the traffic which comes in from the interfaces connected to the ASA 1.

Recommendations

It is recommended to route centralized connections to whichever site hosts the primary (based on priorities), as shown in the image:

Scenario 3



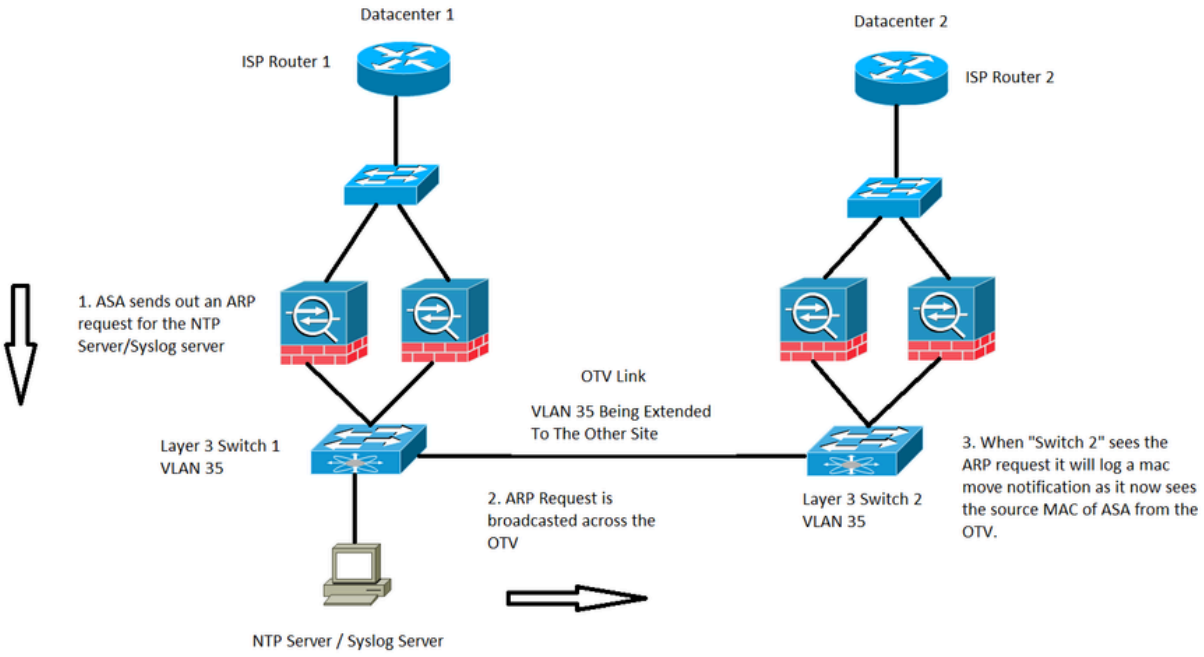
For an Inter Domain Controller (DC) communication in transparent mode, this specific traffic flow is not covered or documented but this specific traffic flow does work from an ASA flow processing standpoint.

However, it can result in MAC move notifications on the switch.

1. The Host 1 on VLAN 35 tries to communicate with Host 2 which is present on the other Datacenter.
2. The Host 1 has a default gateway which is Router 1 and Router 1 has a path to reach Host 2 by being able to communicate with Router 2 directly across an alternate link and in this case we assume Multiprotocol Label Switching (MPLS) and not through the ASA cluster.
3. Router 2 receives the incoming traffic and routes it over to Host 2.
4. Now when Host 2 responds back, Router 2 receives the return traffic and it finds a directly connected route through the ASAs instead of the traffic it sends over the MPLS.
5. At this stage, the traffic that leaves Router 2 has the source MAC of Router 2's exit interface.
6. The ASAs at Datacenter 2 receives the return traffic and finds a connection which exists and is made by the ASAs at Datacenter 1.
7. The ASAs at Datacenter 2 sends the return traffic over CCL back to the ASAs at Datacenter 1.
8. At this stage the ASAs at Datacenter 1 processes the return traffic and sends it down towards Switch 1. The packet still has the same source MAC as that of Router 2's exit interface.
9. Now when Switch 1 receives the packet, it logs a MAC move notification because initially it learned Router 2's MAC address across the interface which is connected to the OTV link, however at this stage it starts learning the MAC address from the interface connected to the ASAs.

Scenario 4

Traffic generated by the ASA, as shown in the image:



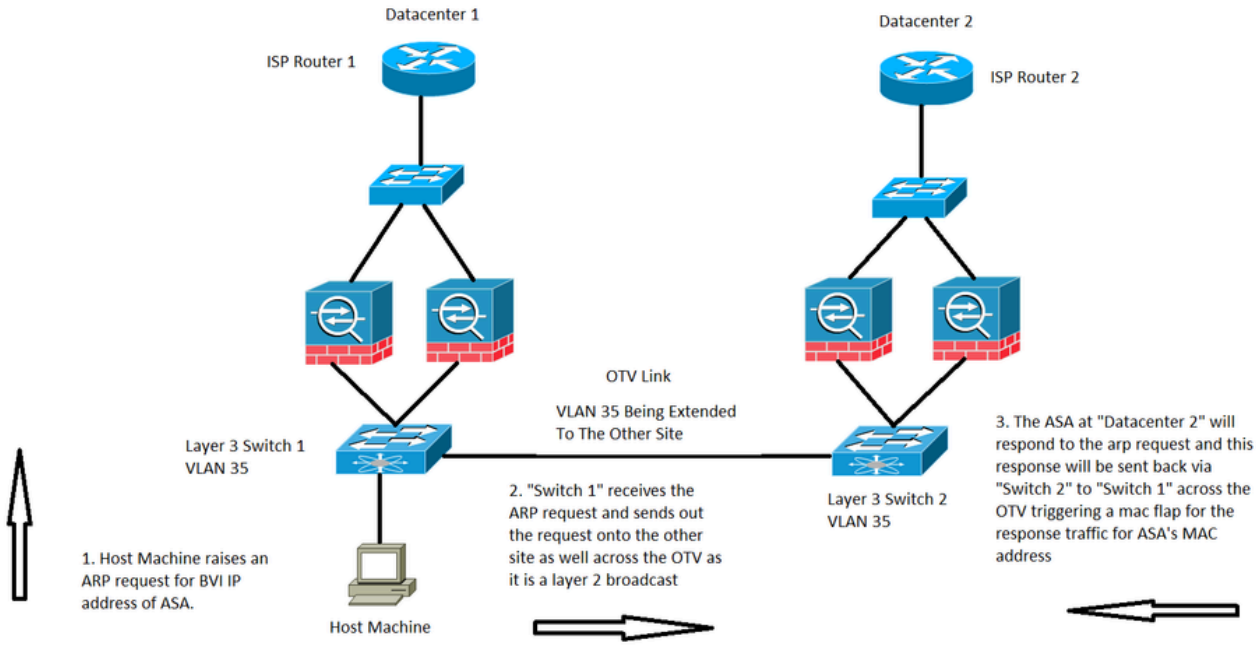
This specific case will be observed for any traffic which gets generated by the ASA itself. Here two possible situations are considered, wherein the ASA either tries to reach an Network Time Protocol (NTP) or a Syslog server, which are on the same subnet as that of its BVI interface.However it is not only limited to these two conditions, this situation can happen whenever traffic is generated by the ASA for any IP address which is directly connected to the BVI IP addresses.

1. If ASA does not have the ARP information of the NTP server/Syslog server, then the ASA will generate an ARP request for that server.

2. As the ARP request is a broadcast packet, the Switch 1 will receive this packet from its connected interface of the ASA and flood it out across all the interfaces in the specific VLAN including the remote site across the OTV.
3. The Remote site Switch 2 will receive this ARP request from the OTV link and due to the source MAC of the ASA, it generates a MAC flap notification since the same MAC address is learned across the OTV via its local directly connected interfaces to the ASA.

Scenario 5

Traffic destined to BVI IP address of the ASA from a directly connected Host, as shown in the image:



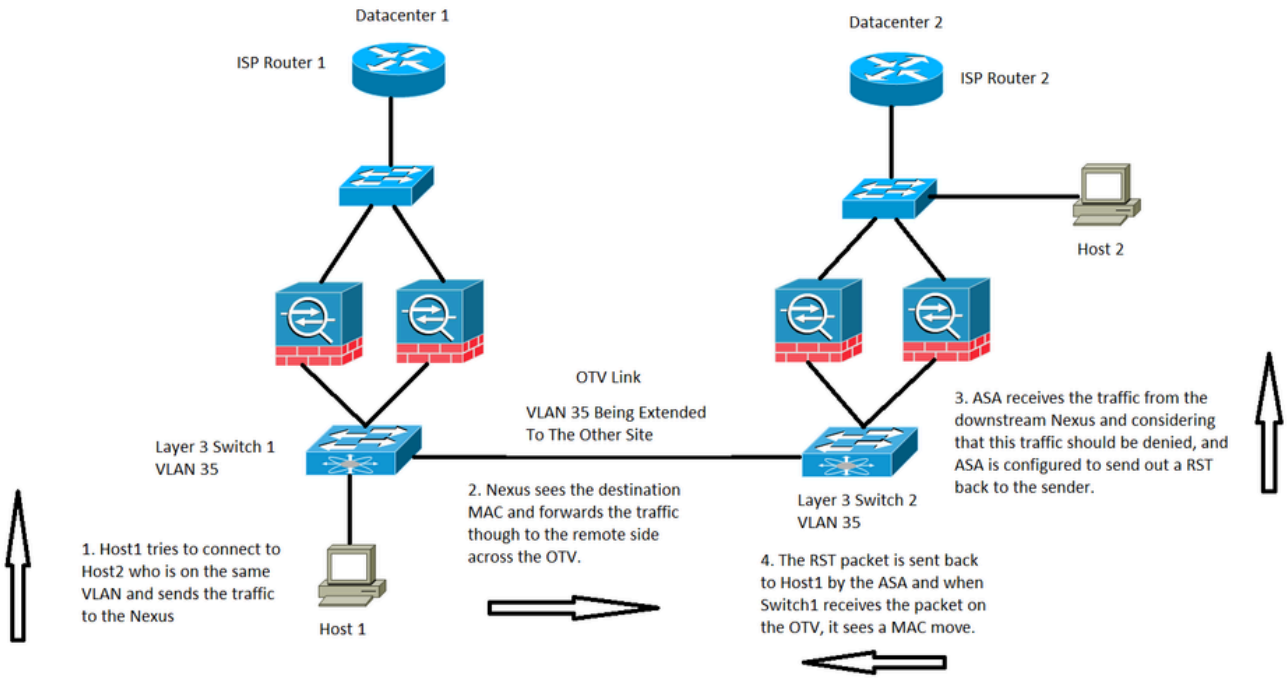
A MAC MOVE can also be observed at times when traffic is destined to the ASA's BVI IP address.

In the scenario, we have a Host machine on a directly connected network of the ASA and is trying to connect to the ASA.

1. The Host does not have the ARP of the ASA and triggers an ARP request.
2. The Nexus receives the traffic and again as it is a broadcast traffic it sends the traffic across the OTV to the other site as well.
3. The ASA on the remote Datacenter 2 can respond to the ARP request and sends the traffic back through the same path which is Switch 2 on the remote side, OTV, Switch 1 on the local side and then the end host.
4. When the ARP response is seen on the local side Switch 1, it triggers a MAC move notification as it sees the MAC address of the ASA which comes in from the OTV link.

Scenario 6

ASA set to deny traffic along with which it sends a RST to the Host, as shown in the image:



In this case, we have a host Host 1 on VLAN 35, it tries to communicate with Host 2 in the same Layer 3 VLAN, however, Host 2 is actually on Datacenter 2 VLAN 1535.

1. Host 2MAC address would be seen on Switch 2 via the interface connected to the ASAs.
2. Switch 1 would be seeing the MAC address of Host 2 via the OTV link.
3. Host 1 sends traffic to Host 2 and this follows the path of Switch 1, OTV, Switch 2, ASAs at Datacenter 2.
4. This specific gets denied by the ASA and as ASA is configured to send back a RST to Host 1, the RST packet comes back with ASA's source MAC address.
5. When this packet makes it back to Switch 1 across the OTV, Switch 1 logs a MAC MOVE notification for ASA's MAC address because it now sees the MAC address across the OTV, wherein before it sees the address from its directly connected interface.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Cisco ASA Series CLI Configuration Guide**
- **Technical Support & Documentation - Cisco Systems**