Problemas frecuentes con el cluster transparente del Inter-sitio ASA

Contenido

Introducción

Este documento describe algunos de los problemas frecuentes con el cluster atravesado del Inter-sitio del modo transparente del EtherChannel.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firewall adaptante del dispositivo de seguridad (ASA)
- Clúster ASA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Comenzando la Versión de ASA 9.2, se soporta el clúster del inter-sitio en donde las unidades ASA se podrían establecer en diversos datacenters y el link de control del cluster (CCL) está conectado sobre una interconexión del centro de datos (DCI). Los escenarios de instrumentación posibles son:

- Cluster del Inter-sitio de la interfaz individual
- Cluster atravesado del Inter-sitio del modo transparente del EtherChannel
- Cluster ruteado EtherChannel atravesado del Inter-sitio del modo (soportado del 9.5 hacia adelante)

El MAC MUEVE las notificaciones

Cuando una dirección MAC en los cambios de la tabla del Content Addressable Memory (CAM) vira hacia el lado de babor, se genera una notificación del MOVIMIENTO MAC. Sin embargo, una notificación del MOVIMIENTO MAC no se genera cuando la dirección MAC se agrega o se quita de la tabla CAM. Suponga si una dirección MAC X es docta vía la interfaz GigabitEthernet0/1 en el VLAN10 y después de una cierta hora el mismo MAC se ve con GigabitEthernet0/2 en el VLAN10, después se genera una notificación del MOVIMIENTO MAC.

Syslog del Switch:

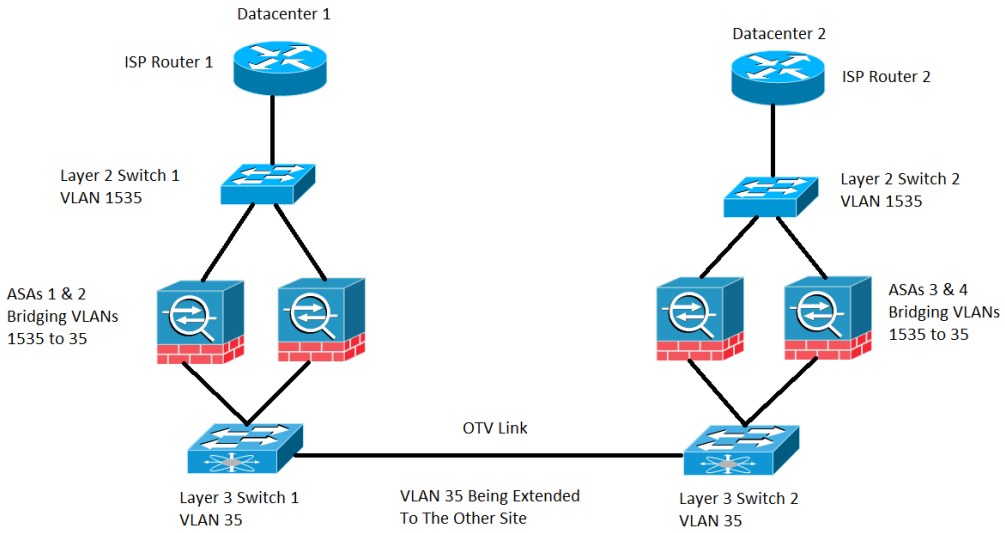
```
NEXUS7K %L2FM-4-L2FM_MAC_MOVE: Mac 000c.8142.2600 in vlan 10 has moved from GigabitEthernet0/1
to GigabitEthernet0/2
```

Syslog del ASA:

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

Diagrama de la red

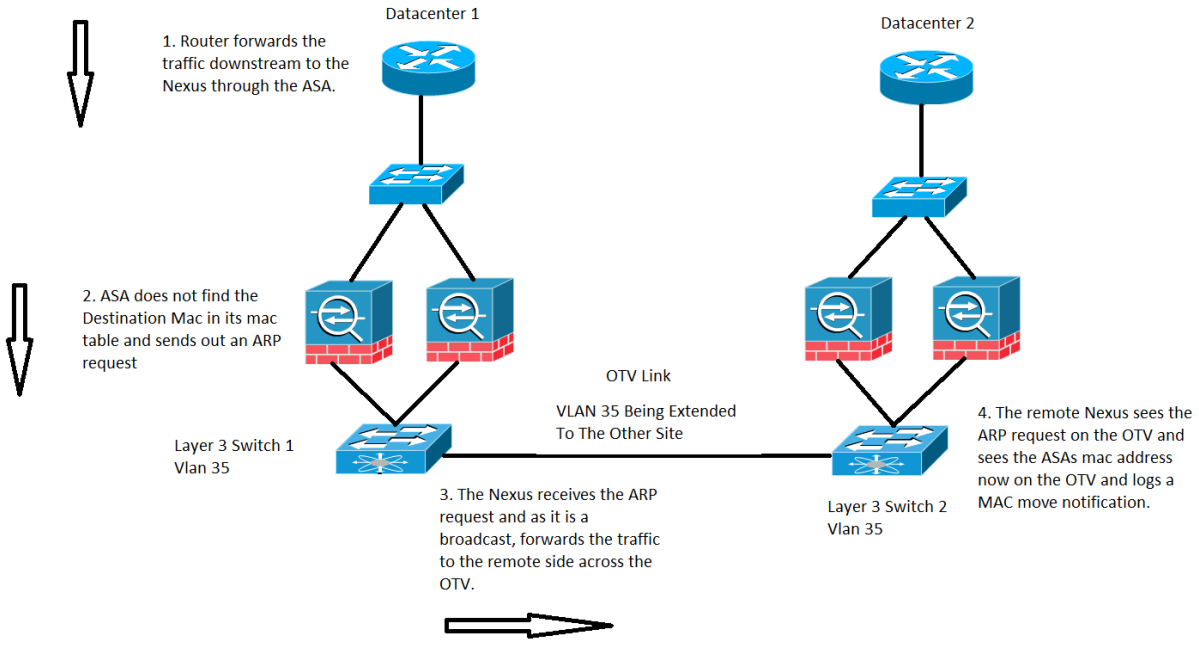
despliegue del cluster del Inter-sitio en donde los ASA se configuran en el modo transparente que interliga el VLA N 1535 y el VLA N 35. El VLA N interior 35 es extendido sobre la virtualización del transporte del recubrimiento (OTV) mientras que el VLA N exterior 1535 no es extendido sobre el OTV, tal y como se muestra en de la imagen



El MAC mueve las notificaciones en el Switch

Escenario 1

Trafique destinado a una dirección MAC cuya entrada no esté presente en la tabla MAC ASA, tal y como se muestra en de la imagen:



En un ASA transparente, si la dirección MAC del destino del paquete que llega en el ASA no está

en la tabla de direcciones MAC, envía una petición de Address Resolution Protocol (ARP) ese destino (si en la misma subred como BVI) o una petición del Internet Control Message Protocol (ICMP) con el Time to Live 1(TTL 1) con el MAC de origen como la dirección MAC del (BVI) del Interfaz Virtual de Bridge y la dirección MAC del destino como regulador del acceso de los medios de destino (DMAC) se falta.

En el caso precedente, usted tiene este flujo de tráfico:

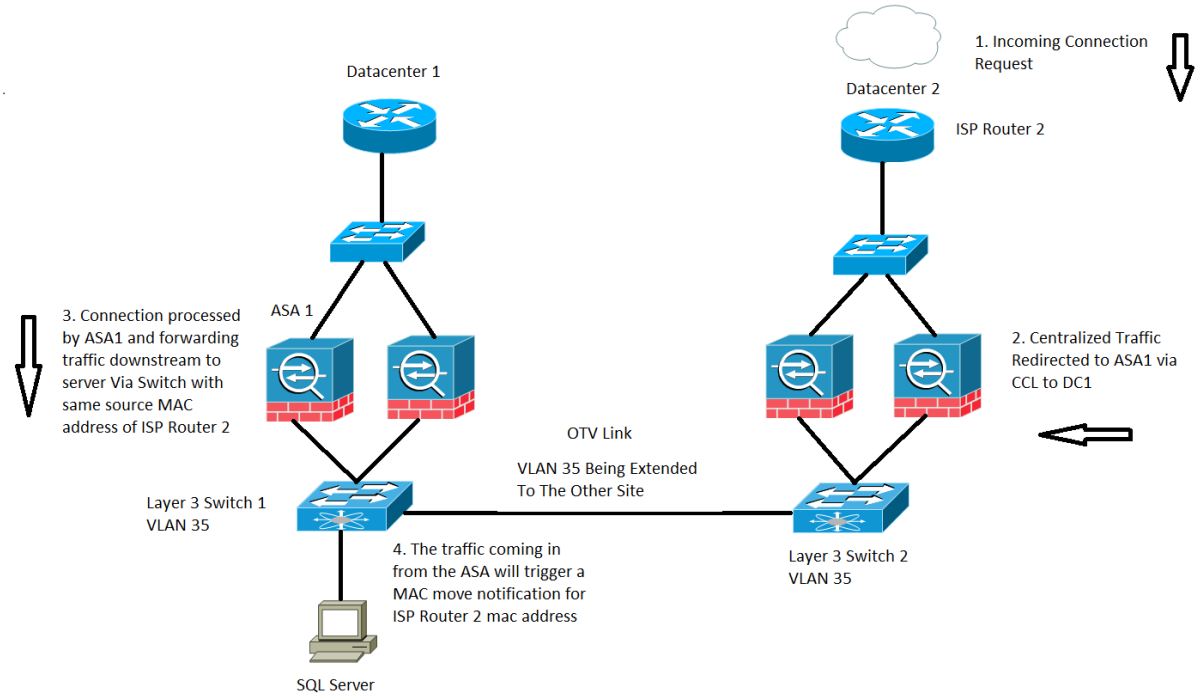
1. El router del ISP en Datacenter 1 adelante trafica a un destino específico que esté detrás del ASA.
2. Cualquiera de la poder ASA recibe el tráfico y en este caso, la dirección MAC del destino del tráfico no es sabida por el ASA.
3. Ahora el IP de destino del tráfico está en la misma subred como el del BVI y como se mencionó antes, ASA ahora genera un pedido ARP para el IP de destino.
4. El Switch1 recibe el tráfico y como la petición es un broadcast, lo adelante el tráfico a Datacenter 2 así como a través del link OTV.
5. Cuando el Switch2 ve el pedido ARP del ASA en el link OTV, registra una notificación del MOVIMIENTO MAC porque la dirección MAC ASA era previamente docta vía directamente la interfaz conectada y está siendo docta ahora vía el link OTV.

Recomendaciones

Es un escenario de la esquina. Las tablas MAC se sincronizan en los clusteres, así que es menos probable que un miembro no tenga una entrada para un host determinado. Un MAC-movimiento ocasional para BVI cluster-poseído MAC se juzga aceptable.

Escenario 2

Flujo centralizado que procesa por el ASA, tal y como se muestra en de la imagen:



El tráfico basado examen a través de un cluster ASA se clasifica en tres tipos:

- Centralizado
- Distribuido
- Semi-distribuido

En el caso del examen centralizado, cualquier tráfico que las necesidades de conseguir examinadas se reorienten a la unidad principal del cluster ASA. Si una unidad auxiliar del cluster ASA recibe el tráfico, se remite al master vía el CCL.

En la imagen anterior, usted trabaja con el tráfico SQL que es un protocolo de examen centralizado (CIP) y el comportamiento descrito aquí es aplicable para cualquier CIP.

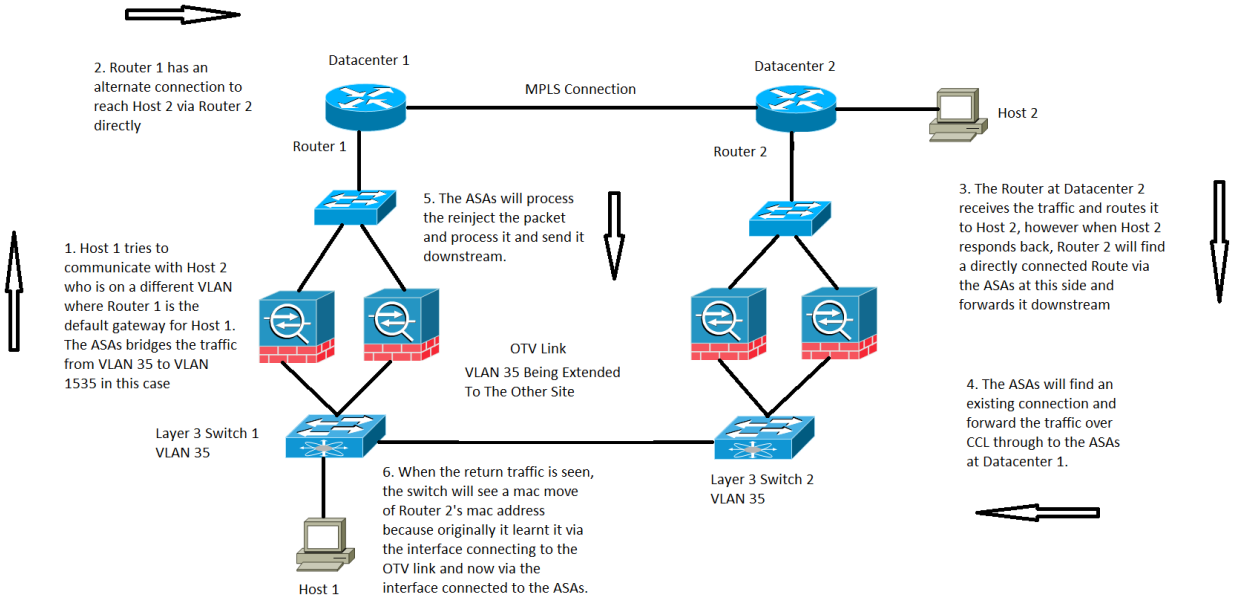
Usted recibe el tráfico en Datacenter 2 donde usted tiene solamente unidades auxiliares del cluster ASA, la unidad principal está situado en Datacenter 1 que sea ASA 1.

1. El router del ISP 2 en Datacenter 2 recibe el tráfico y adelante lo rio abajo a los ASA en su sitio.
2. Cualquiera de los ASA puede recibir este tráfico y una vez que determina que este tráfico necesita ser examinado y mientras que el protocolo se centraliza lo adelante el tráfico encima a la unidad principal vía el CCL.
3. El ASA 1 recibe el flujo de tráfico vía el CCL, procesa el tráfico y lo envía rio abajo al SQL Server.
4. Ahora en que el ASA 1 adelante el tráfico rio abajo, él conserva el MAC address de la fuente original del router del ISP 2 que está situado en Datacenter 2 y lo envía rio abajo.
5. Cuando el Switch1 recibe este tráfico específico, abre una sesión una notificación del MOVIMIENTO MAC porque considera originalmente que dirección MAC del router del ISP 2 vía el link OTV que está conectado con Datacenter 2 y ahora él ve el tráfico que viene adentro de las interfaces conectadas con el ASA 1.

Recomendaciones

Se recomienda para rutear las conexiones centralizadas a cualquier sitio recibe al master (basado en las prioridades), tal y como se muestra en de la imagen:

Escenario 3



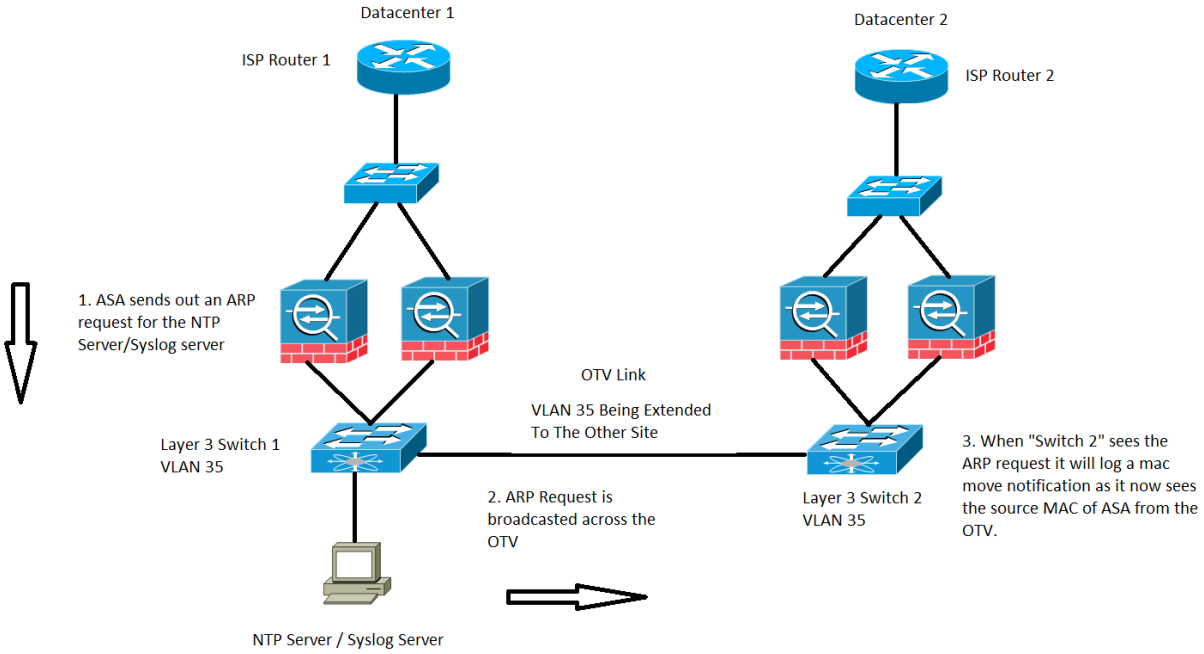
Para una comunicación inter del controlador de dominio (DC) en el modo transparente, este flujo de tráfico específico no se cubre o se documenta sino que este flujo de tráfico específico trabaja de un flujo ASA que procesa el punto de vista. Sin embargo, puede dar lugar a las notificaciones del movimiento MAC en el Switch.

1. El host 1 en el VLA N 35 intenta comunicar con el host 2 que está presente en el otro Datacenter.
2. El host 1 tiene un default gateway que sea router1 y el router1 tiene una trayectoria para alcanzar el host 2 pudiendo comunicar con el router2 directamente a través de un link alterno y en este caso asumimos el Multiprotocol Label Switching (MPLS) y no a través del cluster ASA.
3. El router2 recibe el tráfico entrante y lo rutea encima para recibir 2.
4. Ahora en que responde el host 2 detrás, el router2 recibe el tráfico de retorno y encuentra directamente un Routeconectad con los ASA en vez del tráfico que envía sobre el MPLS.
5. En esta etapa, el tráfico que deja el router2 tiene el MAC de origen de la interfaz de la salida del router 2's.
6. Los ASA en Datacenter 2 reciben el tráfico de retorno y encuentran una conexión que exista y sea hecha por los ASA en Datacenter 1.
7. Los ASA en Datacenter 2 envían el tráfico de retorno sobre el CCL de nuevo a los ASA en Datacenter 1.
8. Los ASA en Datacenter 1 procesan el tráfico de retorno y lo envían en esta etapa abajo hacia el Switch1. El paquete todavía tiene el mismo MAC de origen que el de la interfaz de la salida del router 2's.
9. Ahora en que el Switch1 recibe el paquete, registra una notificación del movimiento MAC porque inicialmente él dirección MAC docta del router 2's a través de la interfaz que está conectada con el link OTV, no obstante comienza en esta etapa a aprender la dirección

MAC de la interfaz conectada con los ASA.

Situación 4

Tráfico generado por el ASA, tal y como se muestra en de la imagen:

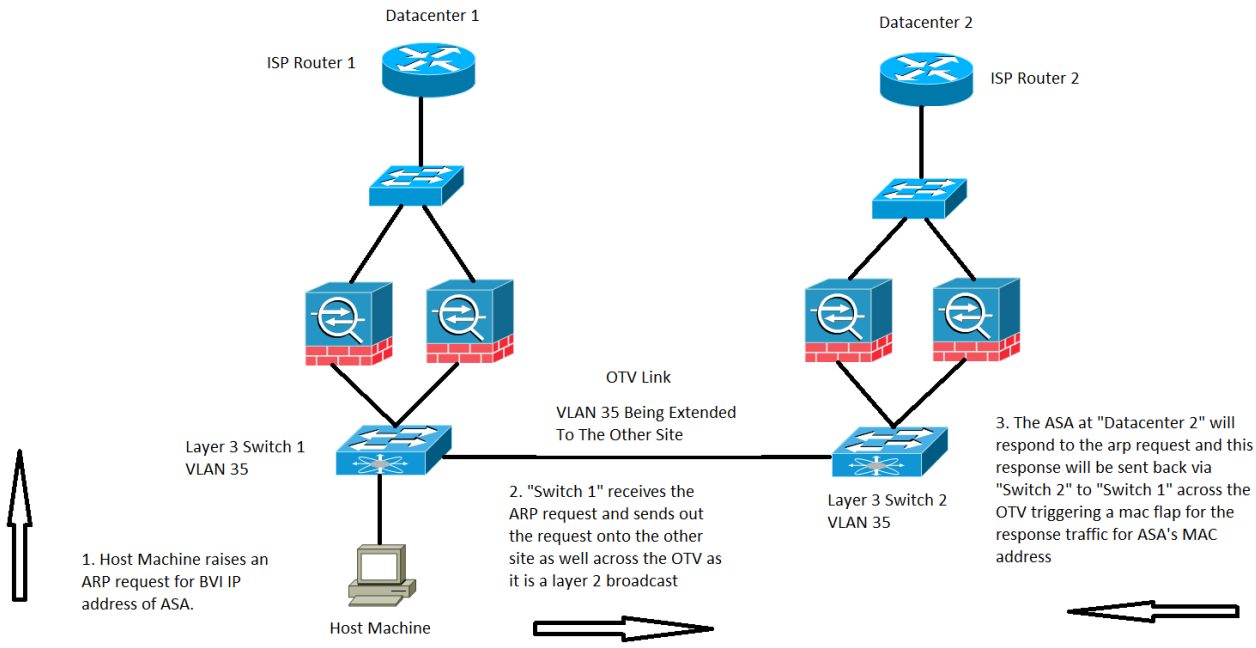


Este caso específico será observado para cualquier tráfico que consiga generado por el ASA sí mismo. Aquí dos situaciones posibles se consideran, en donde el ASA intenta alcanzar un Network Time Protocol (NTP) o a un servidor de Syslog, que están en la misma subred como el de su interfaz BVI. No obstante no sólo se limita a estas dos condiciones, esta situación puede suceder siempre que el tráfico sea generado por el ASA para cualquier dirección IP que esté conectada directamente con los IP Addresses BVI.

1. Si el ASA no tiene la información ARP del servidor NTP/del servidor de Syslog, después el ASA generará un pedido ARP para ese servidor.
2. Pues el pedido ARP es un paquete de broadcast, el Switch1 recibirá este paquete de su interfaz conectada del ASA y lo inundará hacia fuera a través de todas las interfaces en el VLA N específico incluyendo el sitio remoto a través del OTV.
3. El Switch2 del sitio remoto recibirá este pedido ARP del link OTV y debido al MAC de origen del ASA, genera una notificación del flap MAC puesto que la misma dirección MAC es docta a través del OTV vía sus interfaces conectadas del local directamente al ASA.

Situación 5

Trafique destinado a la dirección IP BVI del ASA directamente de un host conectado, tal y como se muestra en de la imagen:



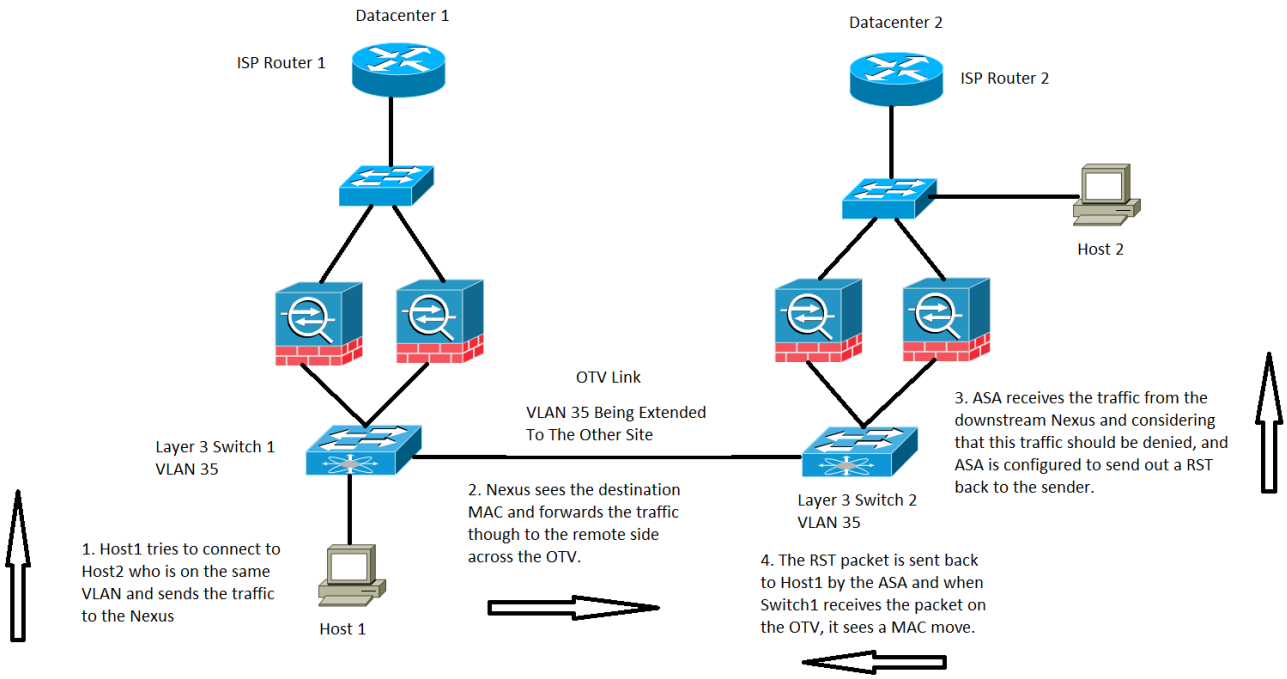
UN MOVIMIENTO MAC puede también ser observado a veces cuando el tráfico se destina a la dirección IP BVI ASA.

En el escenario, tenemos un equipo del host en directamente una red conectada del ASA y estamos intentando conectar con el ASA.

1. El host no tiene el ARP del ASA y acciona un pedido ARP.
2. El nexo recibe el tráfico y otra vez pues es un tráfico de broadcast que envía el tráfico a través del OTV al otro sitio también.
3. El ASA en el Datacenter remoto 2 puede responder al pedido ARP y devuelve el tráfico a través de la misma trayectoria que es Switch2 en el lado remoto, OTV, el Switch1 en el lado local y entonces el host extremo.
4. Cuando la respuesta ARP se considera en el Switch1 del lado local, acciona una notificación del movimiento MAC mientras que ve la dirección MAC del ASA que viene adentro del link OTV.

Situación 6

Conjunto ASA para negar el tráfico junto con el cual envía un RST al host, tal y como se muestra en de la imagen:



En este caso, tenemos un host 1 del host en el VLA N 35, él intentamos comunicar con el host 2 en el mismo VLA N de la capa 3, sin embargo, el host 2 está realmente en el VLA N 1535 de Datacenter 2.

1. El direccionamiento del host 2MAC sería considerado en el Switch2 vía la interfaz conectada con los ASA.
2. El Switch1 estaría viendo la dirección MAC del host 2 vía el link OTV.
3. El host 1 envía el tráfico para recibir 2 y éste sigue la trayectoria del Switch1, OTV, Switch2, los ASA en Datacenter 2.
4. Este específico consigue negado por el ASA y como el ASA se configura para devolver un RST para recibir 1, el paquete RST se vuelve con el MAC Address de origen ASA.
5. Cuando este paquete lo hace de nuevo al Switch1 a través del OTV, el Switch1 registra una notificación del MOVIMIENTO MAC para la dirección MAC ASA porque ahora considera la dirección MAC a través del OTV, en donde antes de que vea el direccionamiento de su directamente interfaz conectada.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración CLI de la serie de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems