Comprensión del aprendizaje de MAC inesperado en los switches Catalyst serie 9000

Contenido

Introducción

Este documento describe una situación en la que un switch de acceso Catalyst 9300 estaba aprendiendo una dirección MAC ascendente en un puerto descendente.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- LAN Switching
- Aprendizaje de direcciones MAC
- Sesiones de autenticación y comportamiento relacionado

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switches Cisco Catalyst serie 9300
- Versión del software 17.6.5

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

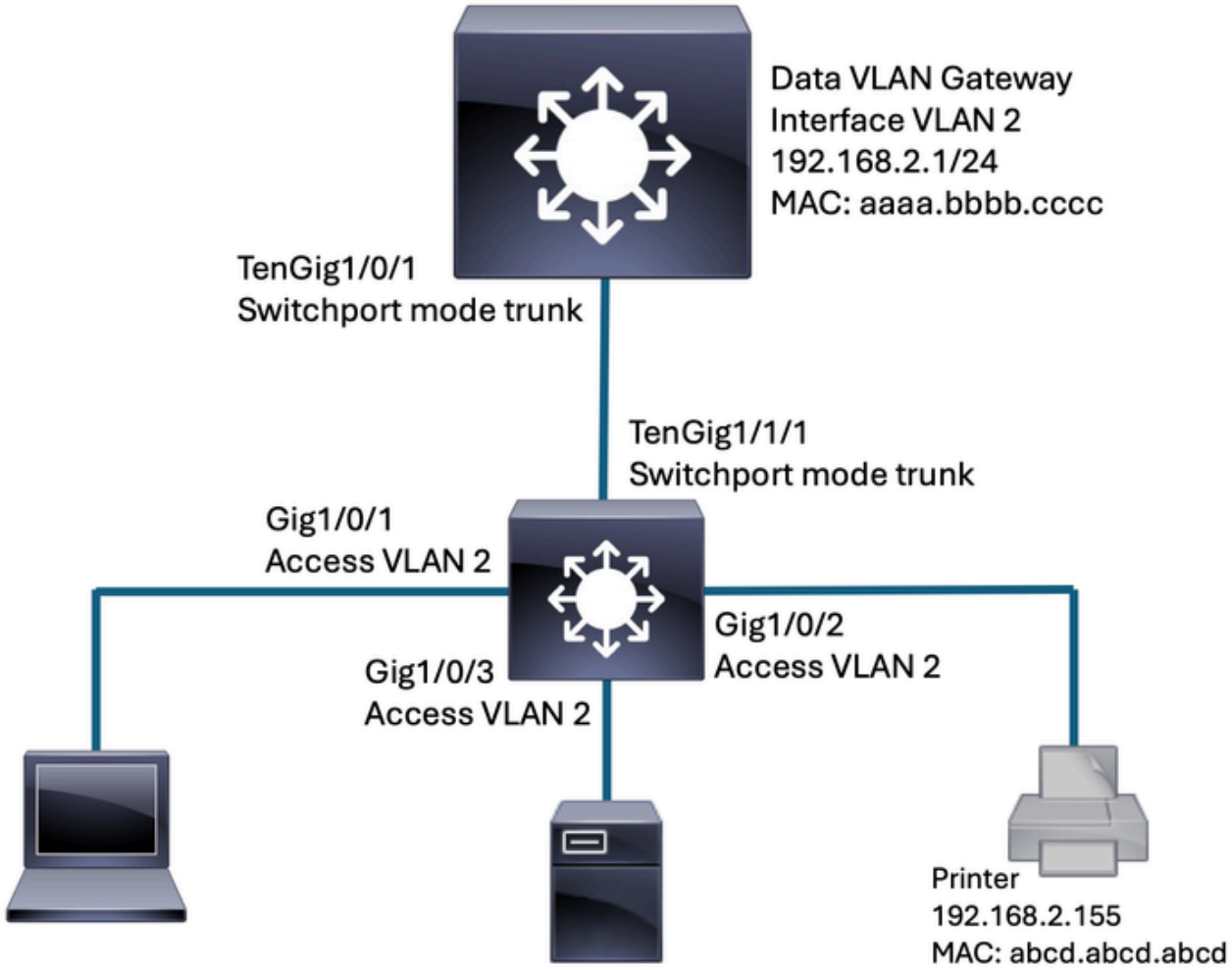
Los switches Catalyst aprenden las direcciones MAC en los puertos del switch basándose en la dirección MAC de origen (SMAC) de una trama entrante. La tabla de direcciones MAC suele ser una fuente de información fiable que guía a un ingeniero de redes hacia la ubicación de una dirección determinada. Se producen situaciones en las que el tráfico de una fuente concreta (un terminal o incluso el gateway de la red local) entra en un switch desde una dirección inesperada. Este documento describe una situación específica en la que la dirección MAC del gateway ascendente se aprendió inesperadamente en interfaces de acceso aleatorio. Los detalles se

basan en los casos de TAC resueltos por los ingenieros de TAC que trabajan en colaboración con los equipos de los clientes.

Problema

El cliente en esta situación detectó primero el problema cuando los terminales en su VLAN de datos (VLAN 2 en esta demostración) perdieron la conectividad con los hosts fuera de su subred. Tras una inspección adicional, observaron que la dirección MAC del gateway VLAN 2 se aprendía en una interfaz de usuario en lugar de en la interfaz esperada.

Al principio, el problema parecía ocurrir de forma aleatoria en una gran red compuesta por varios campus. Teniendo en cuenta lo que sabemos sobre cómo los switches aprenden las direcciones MAC, asumimos que había algún tipo de reflexión de paquetes, pero el reto era demostrar que el problema era externo al switch. Después de recopilar datos adicionales sobre otras ocasiones en que se produjo este problema, pudimos identificar una tendencia con los puertos de usuario involucrados. En cada caso intervino un modelo específico de criterio de valoración.



Segmento de la red afectada

El comando "show mac address-table <address>/<interface>" se utiliza para consultar la tabla de direcciones MAC. En el escenario normal o de trabajo, que la dirección de la gateway se aprende en Ten1/1/1 del switch donde se conectan los terminales.

<#root>

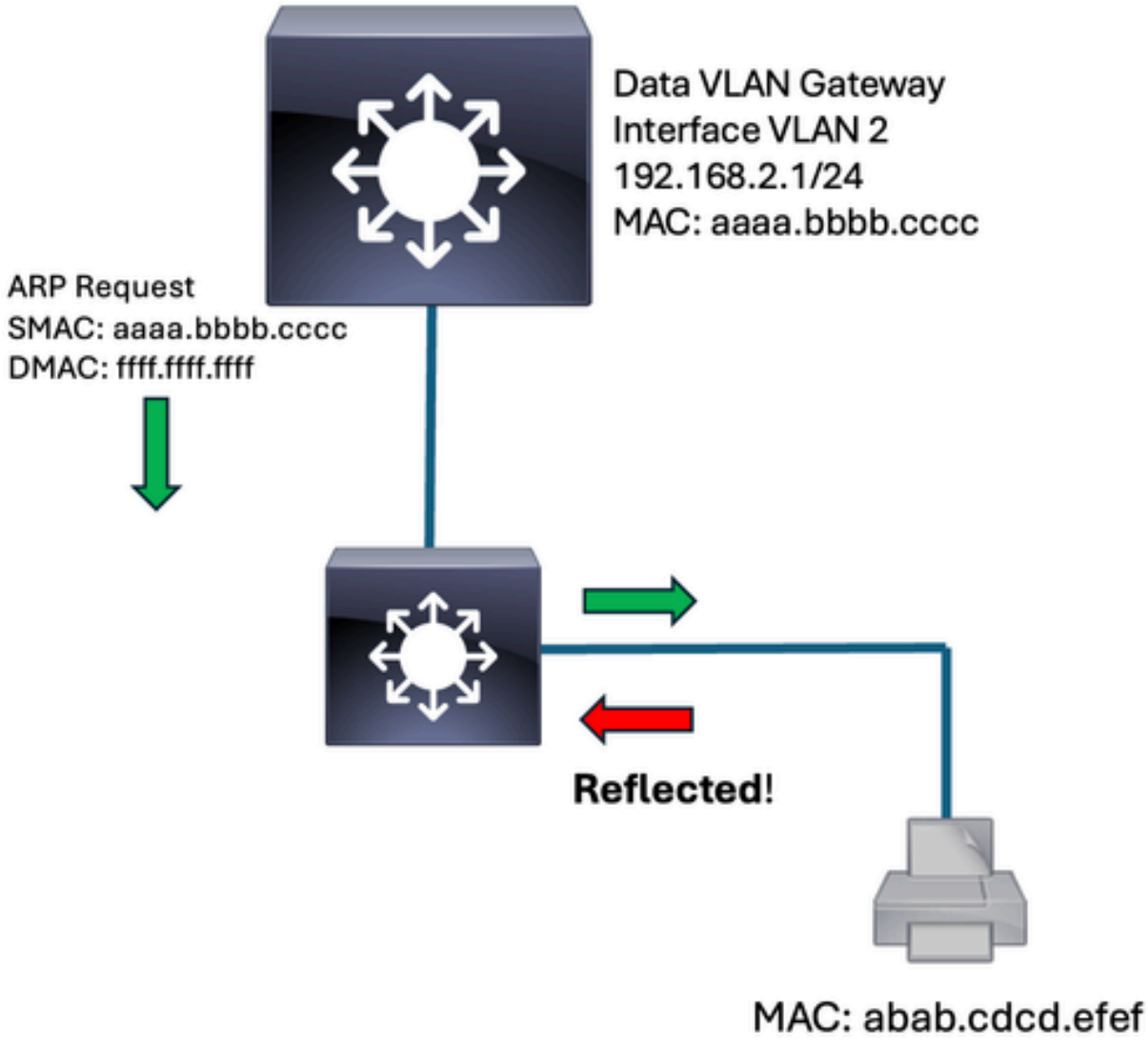
```
ACCESS-SWITCH#

show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    DYNAMIC     Ten1/1/1 <-- Notice the "type" is DYNAMIC. This means the entry w
   2    abcd.abcd.abcd    STATIC      Gig1/0/2 <-- In contrast, this MAC is STATIC. This suggests a fea
```

En el escenario roto, el MAC de la gateway se aprendió en Gi1/0/2 y no en Te1/1/1.

<#root>

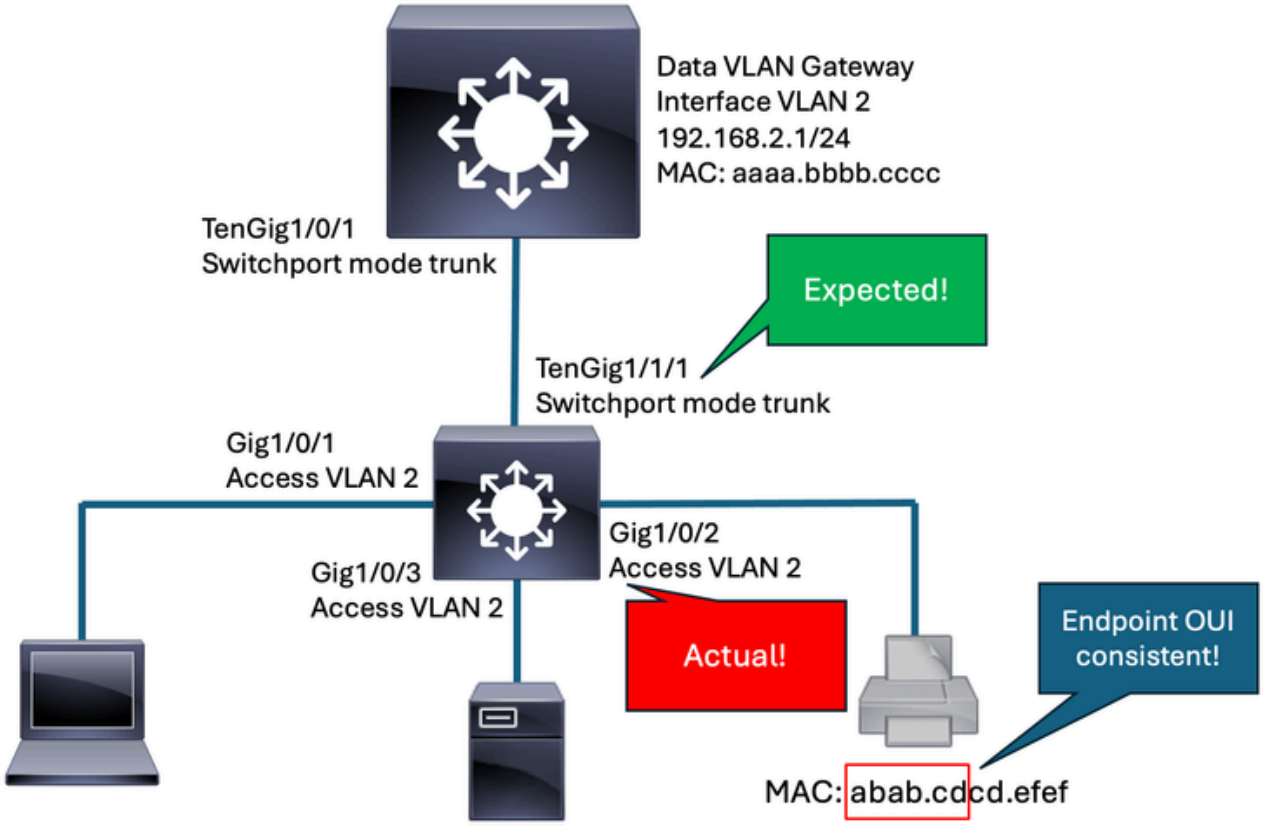
```
ACCESS-SWITCH#

show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    STATIC      Gig1/0/2 <-- Notice that the type is now STATIC.
   2    abcd.abcd.abcd    STATIC      Gig1/0/2
```

El switch de acceso en este escenario ejecuta 802.1x con repliegue MAB (derivación de autenticación MAC) en sus interfaces de acceso. Estas características clave desempeñaron un papel en el impacto global del servicio. Una vez aprendida la dirección MAC del gateway en un puerto de acceso, se convertiría en "estática" en función de la función de seguridad. La función de seguridad también impedía que la dirección MAC del gateway volviera a la interfaz correcta. La información sobre 802.1x, MAB y el concepto de "mac-move" se estudia más a fondo en la guía de configuración correspondiente.



Demostración del tráfico reflejado

La reflexión del paquete lleva al aprendizaje anormal de MAC.



Este diagrama resalta la interfaz esperada frente a la real que aprende la MAC GW.

En el ejemplo se resalta el identificador único organizativo (OUI). Esto ayudó al equipo a identificar que el terminal era de un fabricante común.

Solución

El núcleo de este problema fue el comportamiento inesperado del terminal. Nunca esperamos que un terminal refleje el tráfico de vuelta a la red.

La conclusión clave en este caso fue la tendencia con los terminales. Es difícil resolver un problema que ocurre al azar en una red grande. Esto dio al equipo un subconjunto de puertos de usuario para examinar.

Tenga en cuenta también que las funciones de seguridad implicadas, es decir, dot1x con reserva MAB, desempeñaron un papel en el impacto del servicio. Sin estas funciones que respondieran al tráfico reflejado, el impacto del servicio probablemente no habría sido tan grande.

Se aprovecharon las herramientas de captura de paquetes para identificar que el terminal reflejaba realmente el tráfico. La herramienta integrada de captura de paquetes (EPC) disponible en los switches Catalyst se puede utilizar para identificar los paquetes entrantes.

<#root>

```
Switch#
```

```
monitor capture TAC interface gi1/0/2 in match mac host aaaa.bbbb.cccc any

Switch#
monitor capture TAC start

<wait for the MAC learning to occur>
Switch#
monitor capture TAC stop
Switch#
show monitor capture TAC buffer
```

SPAN físico (analizador de puertos de switch) es una herramienta de captura de paquetes fiable que también se puede utilizar en este escenario.

<#root>

```
Switch(config)#
monitor session 1 source gi1/0/2 rx

Switch(config)#
monitor session 1 filter mac access-group MACL
 <- Since we know the source MAC of the traffic we look for, the SPAN can be filtered.
Switch(config)#
monitor session 1 destination gig1/0/48
```

El equipo pudo capturar el tráfico reflejado en un puerto al que se conectó un terminal sospechoso. En este escenario, el punto final reflejaría los paquetes ARP originados en la dirección MAC del gateway de regreso al puerto del switch. El puerto de switch con el MAB activado intentaría autenticar la dirección MAC del gateway. La implementación de seguridad del puerto del switch permitió que la MAC del gateway autorizara en la VLAN de datos. Dado que la dirección MAC se aprendió junto con la función de seguridad, se "pegaría" como una MAC ESTÁTICA en el puerto del usuario. Además, dado que la implementación de seguridad bloqueó el movimiento de direcciones MAC autorizadas, el switch no pudo olvidar el MAC en el puerto del usuario y no pudo volver a aprenderlo en la interfaz esperada. El reflejo del paquete combinado con la implementación de la seguridad condujo a una situación en la que el tráfico se vio afectado para toda la VLAN local.

Secuencia de eventos:

1. Los MAC se aprenden en las interfaces esperadas. Este es el estado normal de la red.

2. El terminal refleja el tráfico procedente de la puerta de enlace y que vuelve al puerto que se conecta al switch.

3. Debido a la implementación de seguridad del puerto del switch del terminal, el MAC reflejado activa una sesión de autenticación. El MAC está programado como una entrada ESTÁTICA.

4. Una vez que la MAC se desactualiza del puerto del switch esperado, la implementación de seguridad evita que se vuelva a aprender en el link ascendente.

5. El puerto tendría que cerrarse/descerrarse para recuperarse.

La solución definitiva para esta situación era abordar el comportamiento del terminal. En este escenario, el comportamiento ya era conocido por el proveedor del terminal y se corrigió con una actualización de firmware. El hardware del switch Catalyst, así como el software y la configuración, se comportaban de la forma esperada.

La clave de este escenario es el concepto de aprendizaje de MAC. Los switches Catalyst aprenden las direcciones MAC en el ingreso basándose en la dirección MAC de origen de la trama recibida. Si se aprende una dirección MAC en una interfaz inesperada, es seguro concluir que el puerto del switch recibió una trama al ingresar con esa dirección MAC en el campo MAC de origen.

En situaciones muy limitadas, los paquetes se pueden reflejar entre la interfaz física y el ASIC de reenvío del switch, o a través de algún otro comportamiento incorrecto interno. Si este parece ser el caso y no se encuentra ningún bug existente que explique el problema, comuníquese con el TAC para ayudar con el aislamiento.

Información Relacionada

- Configuración de la captura de paquetes: Catalyst 9300
- Configuración de SPAN y RSPAN - Catalyst 9300
- Solución de problemas de Mac Address Table Manager en switches Catalyst serie 9000
- Configuración de la Autenticación Basada en Puerto IEEE 802.1x - Catalyst 9300
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).