Entender o aprendizado inesperado de MAC nos switches Catalyst 9000 Series

Contents

Introdução

Este documento descreve um cenário em que um switch de acesso Catalyst 9300 estava aprendendo um endereço MAC de upstream em uma porta de downstream.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- LAN Switching
- Aprendizado de Endereço MAC
- Sessões de autenticação e comportamento relacionado

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switches Cisco Catalyst 9300 Series
- Software versão 17.6.5

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

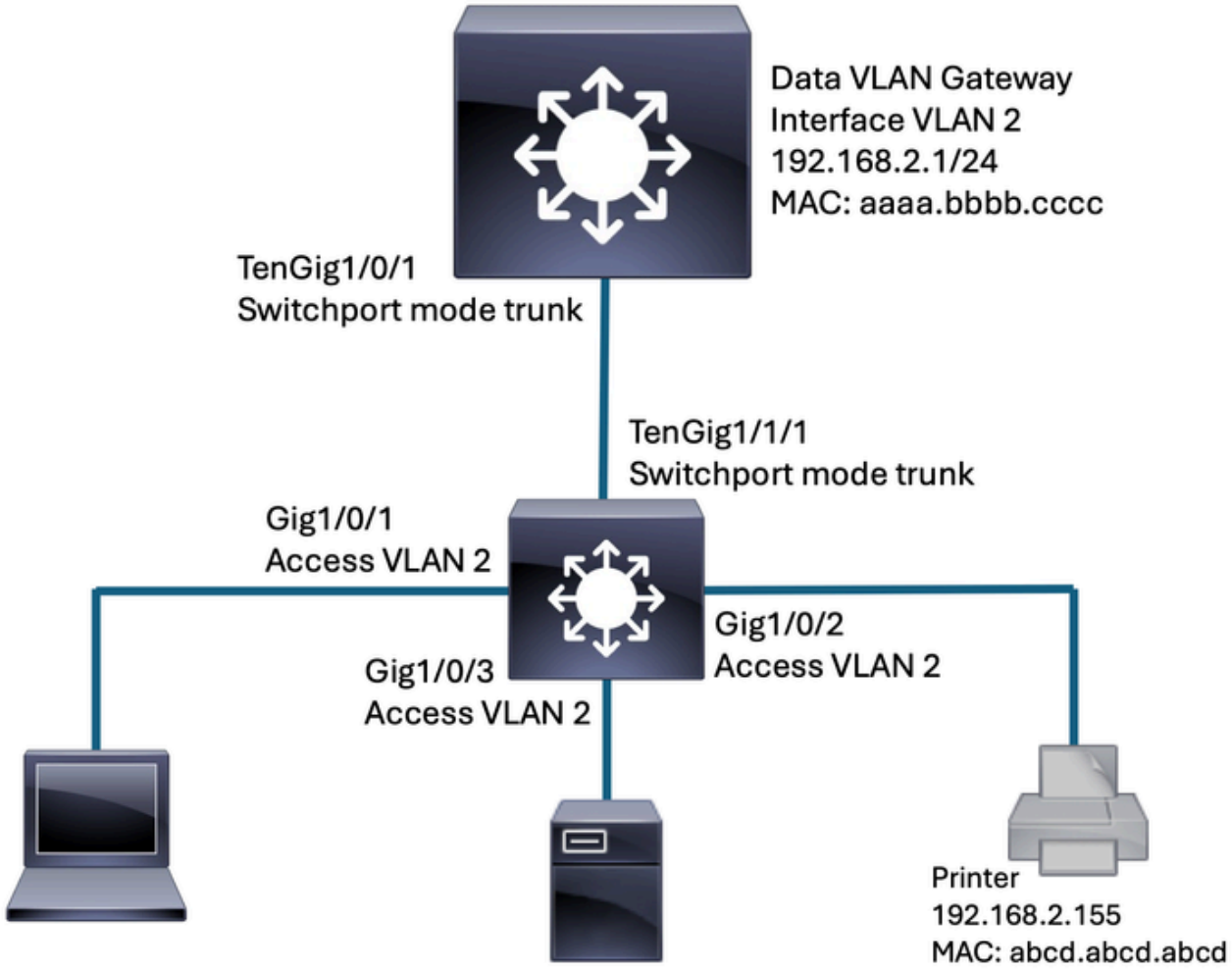
Os switches Catalyst aprendem os endereços MAC nas portas do switch com base no endereço MAC de origem (SMAC) de um quadro de entrada. A tabela de endereços MAC é geralmente uma fonte confiável de informações que guia um engenheiro de rede para a localização de um determinado endereço. As situações surgem quando o tráfego de uma determinada origem - um endpoint ou mesmo o gateway da rede local - entra em um switch de uma direção inesperada. Este documento descreve uma situação específica em que o endereço MAC do gateway de upstream foi aprendido inesperadamente em interfaces de acesso aleatório. Os detalhes são baseados em casos do TAC resolvidos por engenheiros do TAC que trabalham em parceria com

as equipes do cliente.

Problema

O cliente neste cenário percebeu o problema pela primeira vez quando os endpoints em sua VLAN de dados (VLAN 2 nesta demonstração) perderam a conectividade com hosts fora de sua sub-rede. Após uma inspeção adicional, eles observaram que o endereço MAC do gateway da VLAN 2 foi aprendido em uma interface de usuário em vez de na interface esperada.

Inicialmente, o problema parecia acontecer aleatoriamente em uma rede grande composta de vários campi. Considerando o que sabemos sobre como os switches aprendem endereços MAC, presumimos algum tipo de reflexão de pacote, mas o desafio era provar que o problema era externo ao switch. Depois de coletar dados adicionais sobre outras vezes em que esse problema ocorreu, conseguimos identificar uma tendência com as portas de usuário envolvidas. Um modelo específico de endpoint estava envolvido em cada ocorrência.



Segmento da rede afetada

O comando "show mac address-table <address>/<interface>" é usado para consultar a tabela de

endereços MAC. No cenário funcional ou normal, o endereço do gateway é aprendido em Ten1/1/1 do switch onde os endpoints se conectam.

<#root>

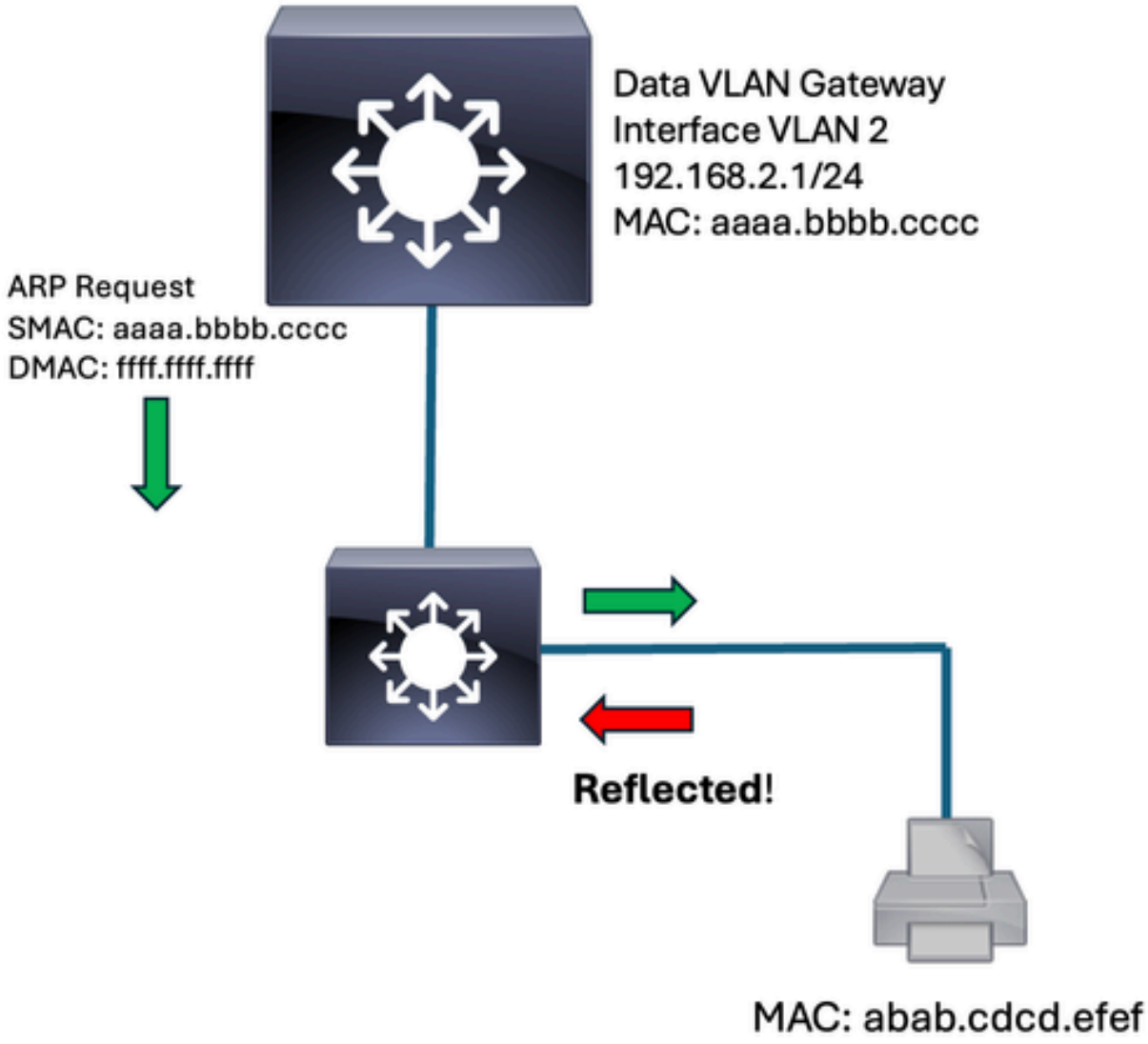
```
ACCESS-SWITCH#

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 wa
   2    abcd.abcd.abcd    STATIC      Gig1/0/2 <-- In contrast, this MAC is STATIC. This suggests a feat
```

No cenário quebrado, o MAC do gateway foi aprendido em Gi1/0/2 e não em Te1/1/1.

<#root>

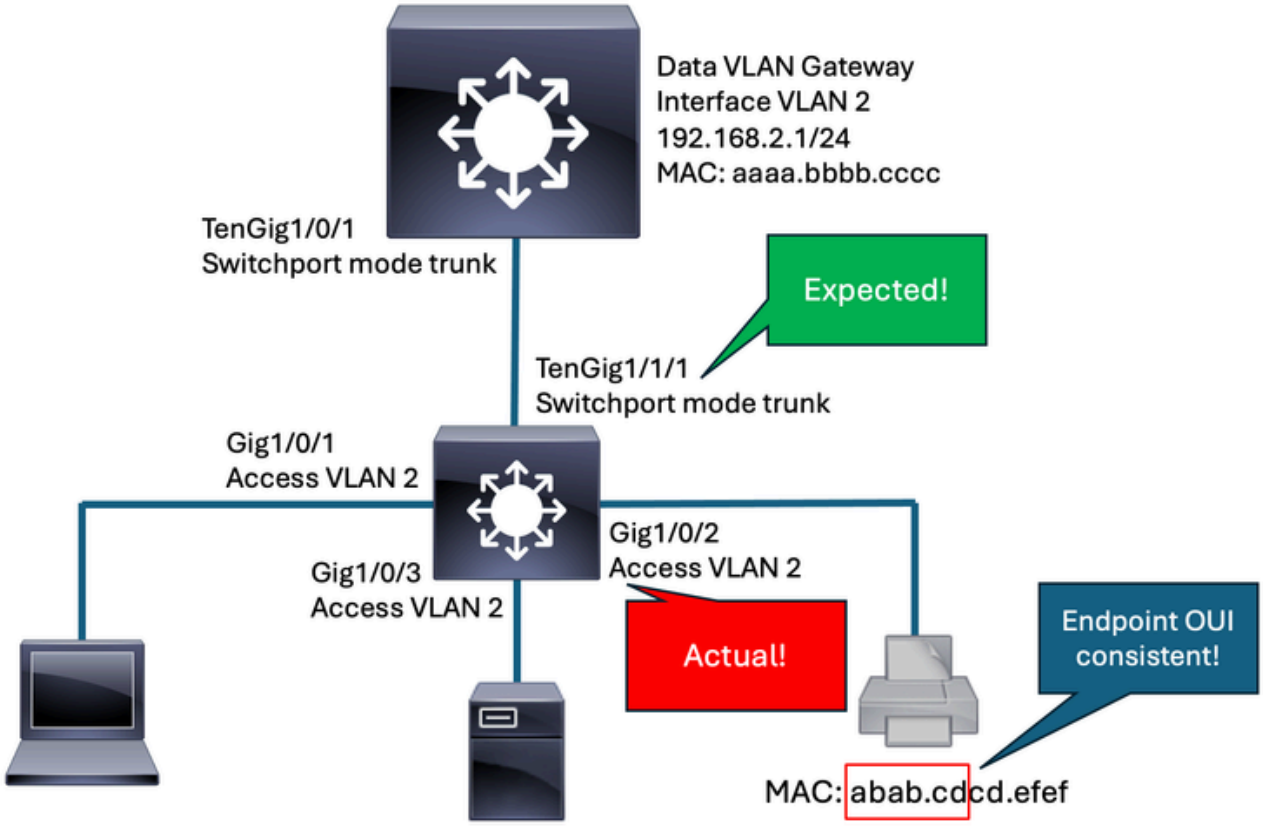
```
ACCESS-SWITCH#

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
```

O switch de acesso neste cenário executa 802.1x com fallback de MAB (desvio de autenticação MAC) em suas interfaces de acesso. Esses principais recursos tiveram um papel importante no impacto geral do serviço. Uma vez que o endereço MAC do gateway foi aprendido em uma porta de acesso, ele se tornaria 'estático' como uma função do recurso de segurança. O recurso de segurança também impediu que o endereço MAC do gateway voltasse para a interface correta. As informações sobre 802.1x, MAB e o conceito de "mac-move" são explorados mais detalhadamente no guia de configuração relevante.



Demonstração do tráfego refletido

A reflexão do pacote leva ao aprendizado anormal do MAC.



Este diagrama destaca a interface esperada versus real que aprende o GW MAC.

O exemplo destaca o identificador exclusivo da organização (OUI). Isso ajudou a equipe a identificar que o endpoint era de um fabricante comum.

Solução

O núcleo deste problema foi o comportamento inesperado do endpoint. Nunca esperamos que um endpoint reflita o tráfego de volta para a rede.

A principal descoberta neste caso foi a tendência com os endpoints. É difícil solucionar um problema que ocorre aleatoriamente em uma rede grande. Isso deu à equipe um subconjunto de portas de usuário para ser examinado.

Observe também que os recursos de segurança envolvidos, ou seja, dot1x com fallback de MAB, tiveram um papel importante no impacto do serviço. Sem esses recursos respondendo ao tráfego refletido, o impacto do serviço provavelmente não teria sido tão grande.

As ferramentas de captura de pacotes foram aproveitadas para identificar se o tráfego foi realmente refletido pelo endpoint. A ferramenta EPC (Embedded Packet Capture) disponível nos switches Catalyst pode ser usada para identificar pacotes de entrada.

<#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
```

O SPAN físico (analisador de porta do switch) é uma ferramenta confiável de captura de pacotes que também pode ser usada neste cenário.

<#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
```

A equipe conseguiu capturar o tráfego refletido em uma porta onde um endpoint suspeito estava conectado. Neste cenário, o ponto final refletiria os pacotes ARP originados do endereço MAC do gateway de volta à porta do switch. A porta do switch habilitado para MAB tentaria autenticar o endereço MAC do gateway. A implementação da segurança de porta do switch permitiu que o MAC do gateway autorizasse na VLAN de dados. Como o endereço MAC foi aprendido em conjunto com o recurso de segurança, ele "travaria" como um MAC ESTÁTICO na porta do usuário. Além disso, como a implementação de segurança bloqueou o movimento do endereço MAC dos endereços MAC autorizados, o switch não conseguiu esquecer o MAC na porta do usuário e não pôde reaprendê-lo na interface esperada. A reflexão do pacote combinada com a implementação da segurança levou a uma situação em que o tráfego foi afetado por toda a VLAN local.

Sequência de eventos:

1. Os MACs são aprendidos nas interfaces esperadas. Esse é o estado normal da rede.

2. O endpoint reflete o tráfego originado no gateway de volta para a porta que se conecta ao switch.

3. Devido à implementação da segurança de porta do switch do ponto final, o MAC refletido dispara uma sessão de autenticação. O MAC é programado como uma entrada STATIC.

4. Uma vez que o MAC expira a porta esperada do switch, a implementação da segurança impede que ele seja reaprendido no uplink.

5. A porta precisaria ser fechada/desfechada para se recuperar.

A última solução para essa situação foi lidar com o comportamento do endpoint. Neste cenário, o comportamento já era conhecido pelo fornecedor do endpoint e foi corrigido com uma atualização de firmware. O hardware do switch Catalyst, bem como o software e a configuração, estavam se comportando inteiramente conforme o esperado.

A principal conclusão desse cenário é o conceito de aprendizagem MAC. Os switches Catalyst aprendem os endereços MAC no ingresso com base no endereço MAC origem do quadro recebido. Se um endereço MAC for aprendido em uma interface inesperada, é seguro concluir que a porta do switch recebeu um quadro na entrada com esse endereço MAC no campo MAC de origem.

Em situações muito limitadas, os pacotes podem ser refletidos entre a interface física e o ASIC de encaminhamento do switch - ou através de algum outro mau comportamento interno. Se este parecer ser o caso e nenhum bug existente for encontrado que explique o problema, entre em contato com o TAC para ajudar no isolamento.

Informações Relacionadas

- Configurando a captura de pacotes - Catalyst 9300
- Configurando SPAN e RSPAN - Catalyst 9300
- Identificar e Solucionar Problemas do Gerenciador de Tabelas de Endereços Mac nos Catalyst 9000 Series Switches
- Configurando a autenticação baseada em porta IEEE 802.1x - Catalyst 9300
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.