Understand Unexpected MAC Learning on Catalyst 9000 Series Switches

Contents

Introduction

This document describes a scenario where a Catalyst 9300 access switch was learning an upstream MAC address on a downstream port.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- LAN Switching
- MAC Address Learning
- Authentication Sessions and related behavior

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalyst 9300 Series Switches
- Software Version 17.6.5

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

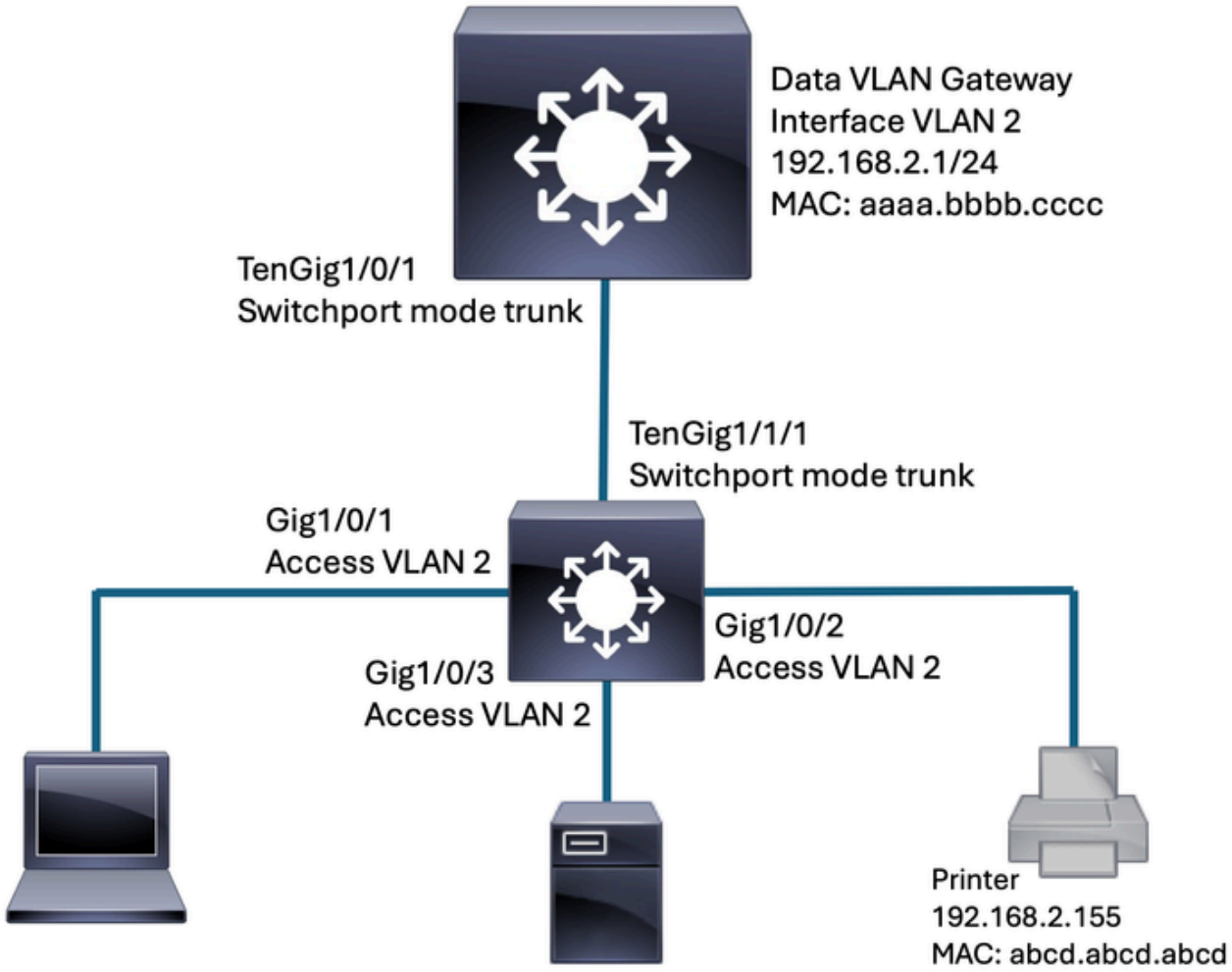
Catalyst switches learn MAC addresses on switch ports based on the source MAC address (SMAC) of an inbound frame. The MAC address table is typically a trustworthy source of information that guides a network engineer towards the location of a given address. Situations arise where traffic from a particular source- an endpoint or even the gateway of the local network- ingresses a switch from an unexpected direction. This document describes a specific situation where the upstream gateway MAC address was unexpectedly learned on random access interfaces. The details are based on TAC cases solved by TAC engineers working in partnership with customer teams.

Problem

The client in this scenario first noticed the problem when endpoints in their data VLAN (VLAN 2 in this demonstration) lost connectivity to hosts outside of their subnet. Upon further inspection, they observed that the MAC address of the VLAN 2 gateway was learned on a user interface instead of on the expected

interface.

The problem initially appeared to happen at random in a large network comprised of multiple campuses. Given what we know about how the switches learn MAC addresses, we assumed some kind of packet reflection but the challenge was proving the problem was external to the switch. After gathering additional data about other times this problem had occurred, we were able to identify a trend with the user ports involved. A specific model of endpoint was involved in every occurrence.



Segment of impacted network

The command "**show mac address-table <address>/<interface>**" is used to query the MAC address table. In the working or normal scenario, that the gateway address is learned on Ten1/1/1 of the switch where the endpoints connect.

<#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
```

In the broken scenario, the gateway MAC was learned on Gi1/0/2 and not on Te1/1/1.

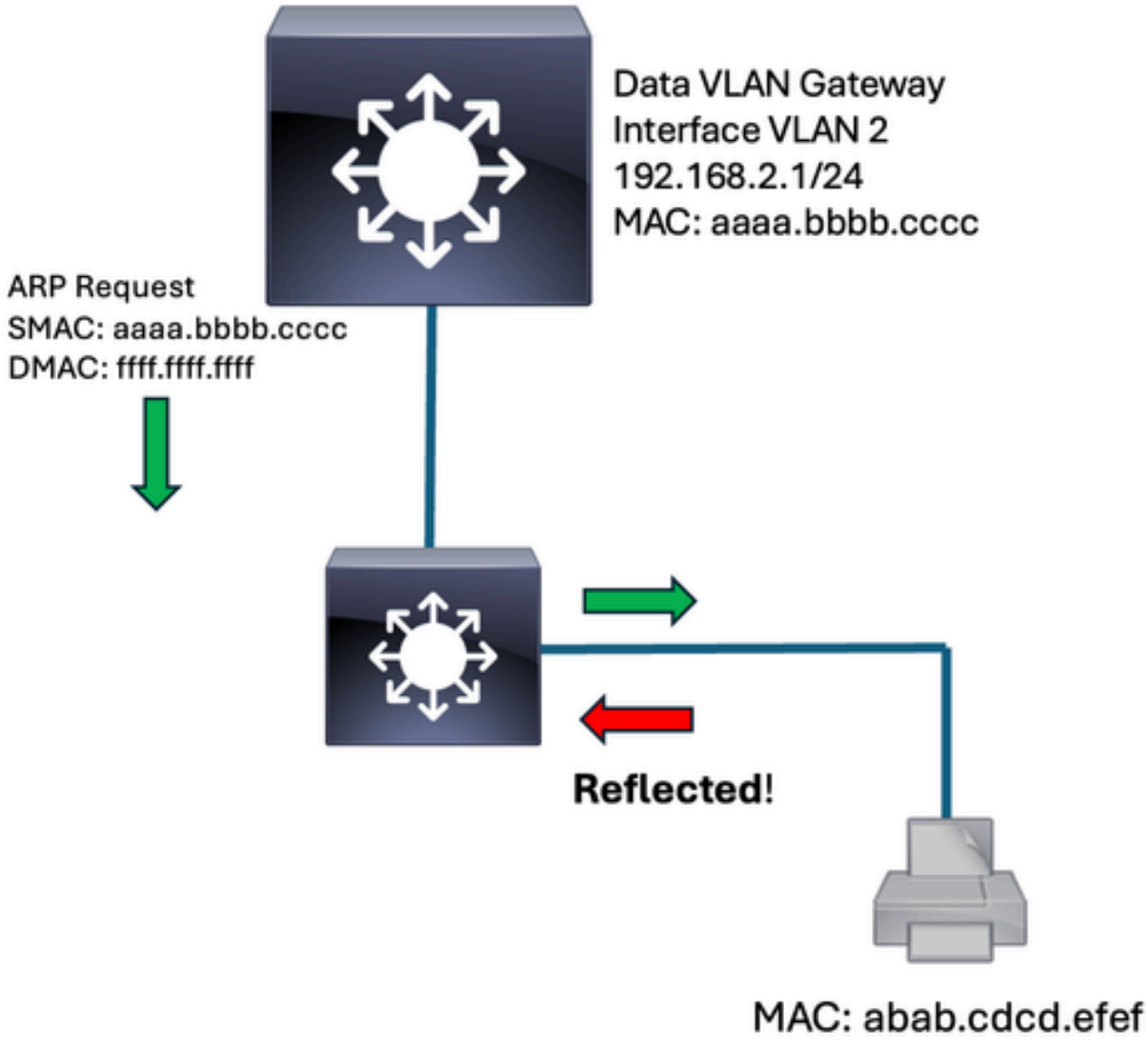
<#root>

```
ACCESS-SWITCH#
```

`show mac address-table`

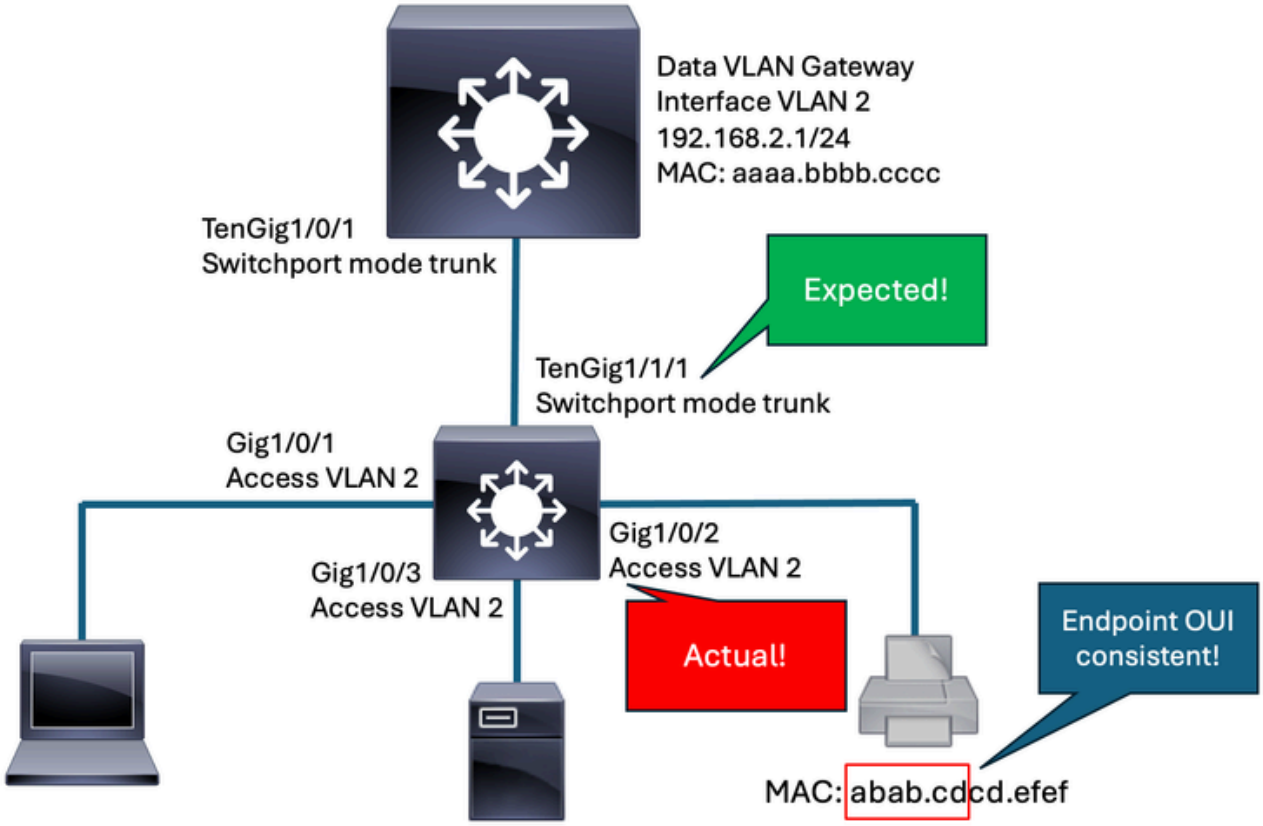
```
          Mac Address Table
-------------------------------------------

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
```

The access switch in this scenario runs 802.1x with MAB (MAC authentication bypass) fallback on its access interfaces. These key features played a role in the overall service impact. Once the gateway MAC address was learned on an access port, it would become 'static' as a function of the security feature. The security feature also prevented the gateway MAC address from moving back to the correct interface. Information on 802.1x, MAB and the concept of 'mac-move' is further explored in the relevant configuration guide.



Demonstration of reflected traffic

The packet reflection leads to the abnormal MAC learn.



This diagram highlights the expected versus actual interface that learns the GW MAC.

The example highlights the organizational unique identifier (OUI). This helped the team identify that the endpoint was of a common manufacturer.

Solution

The core of this problem was the unexpected behavior by the endpoint. We never expect an endpoint to reflect traffic back into the network.

The key finding in this case was the trend with the endpoints. It is difficult to troubleshoot a problem that occurs at random in a large network. This gave the team a subset of user ports to scrutinize.

Also note that the security features involved- namely dot1x with MAB fallback- played a role in the service impact. Without these features responding to the reflected traffic, the service impact likely would not have been as great.

Packet capture tools were leveraged to identify that traffic was truly reflected by the endpoint. The embedded packet capture (EPC) tool available on Catalyst switches can be used to identify inbound packets.

<#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 <brief/detailed>
```

Physical SPAN (switch port analyzer) is a reliable packet capture tool that can also be used in this scenario.

```
<#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
```

The team was able to capture reflected traffic on a port where a suspect endpoint connected. In this scenario, the endpoint would reflect ARP packets sourced from the gateway MAC address back into the switch port. The MAB-enabled switch port would attempt to authenticate the gateway MAC address. The switch port security implementation allowed the gateway MAC to authorize in the data VLAN. Since the MAC address was learned in conjunction with the security feature, it would "stick" as a STATIC MAC on the user port. Also, since the security implementation blocked MAC address movement of authorized MAC addresses, the switch was unable to forget the MAC on the user port and unable to re-learn it on the expected interface. The packet reflection compounded with the security implementation led to a situation where traffic was impacted for the whole local VLAN.

Sequence of Events:

1. MACs are learned on the expected interfaces. This is the normal state of the network.

2. Endpoint reflects traffic sourced from gateway back into the port connecting to the switch.

3. Due to the endpoint switch port security implementation, the reflected MAC triggers an authentication session. The MAC is programmed as a STATIC entry.

4. Once the MAC ages out of the expected switch port, the security implementation prevents it from being re-learned on the uplink.

5. The port would need to be shut/unshut to recover.

The ultimate fix for this situation was to address the endpoint behavior. In this scenario, the behavior was already known to the endpoint vendor and was fixed with a firmware update. The Catalyst switch hardware as well as the software and configuration were all behaving entirely as expected.

The key takeaway from this scenario is the concept of MAC learning. Catalyst switches learn MAC addresses on ingress based on the source MAC address of the received frame. If a MAC address is learned on an unexpected interface, it is safe to conclude that the switch port received a frame on ingress with that MAC address in the source MAC field.

In very limited situations, packets can be reflected between the physical interface and the forwarding ASIC of the switch - or through some other internal misbehavior. If this appears to be the case and no existing bug is found that explains the issue, contact TAC to assist with isolation.

Related Information

- Configuring Packet Capture - Catalyst 9300
- Configuring SPAN and RSPAN - Catalyst 9300
- Troubleshoot Mac Address Table Manager on Catalyst 9000 Series Switches
- Configuring IEEE 802.1x Port-Based Authentication - Catalyst 9300
- Cisco Technical Support & Downloads