Understand Mac Flapping Notifications on Catalyst 9000 Switches

Contents

Introduction

This document describes the key points to understand mac flapping notifications on Catalyst 9000 switches.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Mac Address learning on Catalyst switches

Component Used

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

- C9200
- C9300
- C9500
- C9400
- C9600

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.

Related Products

This document can also be used with these hardware and software versions:

- Catalyst 3650/3850 series switches with Cisco IOS® XE 16.x.

Background Information

The catalyst 9000 switches learn the source mac address of a packet received on a port. If the port is configured as access, the mac address is learned on the configured vlan. If the port is configured as trunk, the mac address is learned based on the Dot1q tag on the packet.

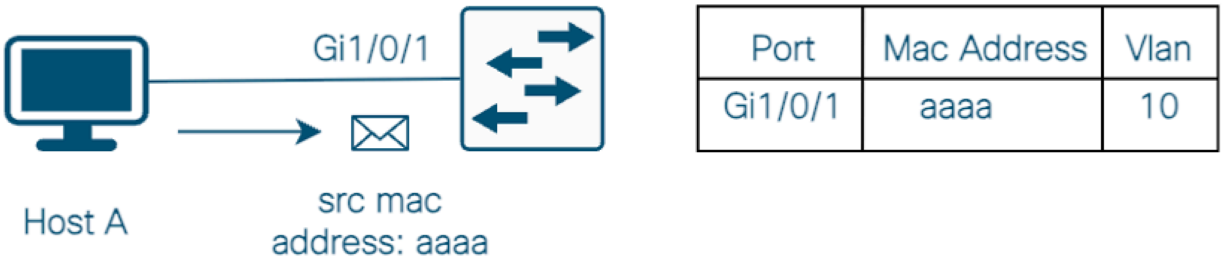
Note: The mac address can be learned in only one port at the time per vlan. It is not permitted to learn the same mac address in the same vlan on multiple ports.

What is a Mac Flap Notification

A mac flapping notification is a syslog message generated by the switch when it receives a packet with the same source mac address in the same vlan from two or more ports.

Normal Operation

As exhibited in Image No.1, you have a Host A sending packets to the switch with the source mac address aaaa in vlan 10. The switch updates this information in the mac address table and the traffic flows without interruptions.

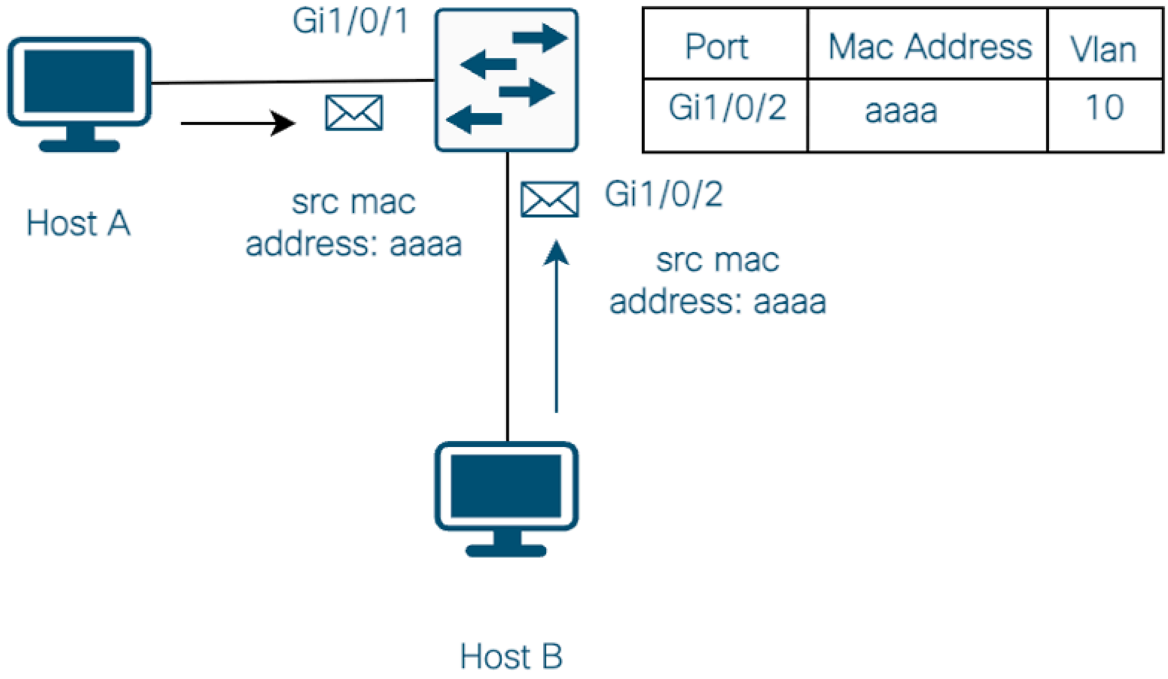


Port	Mac Address	Vlan
Gi1/0/1	aaaa	10

Image No.1

Unexpected Scenario

Now, in Image No. 2, you have Host A and Host B sending packets to the switch with the same source mac address in the same vlan.



Port	Mac Address	Vlan
Gi1/0/2	aaaa	10

Image No.2

Since it is not permitted to learn the same mac on the same vlan on multiple ports, a syslog is generated, and there is a sequence of events that occurs.

- The switch removes the mac address from the previous port on the mac address table.
- Now, the mac address is learned in the port where the packet was last received.

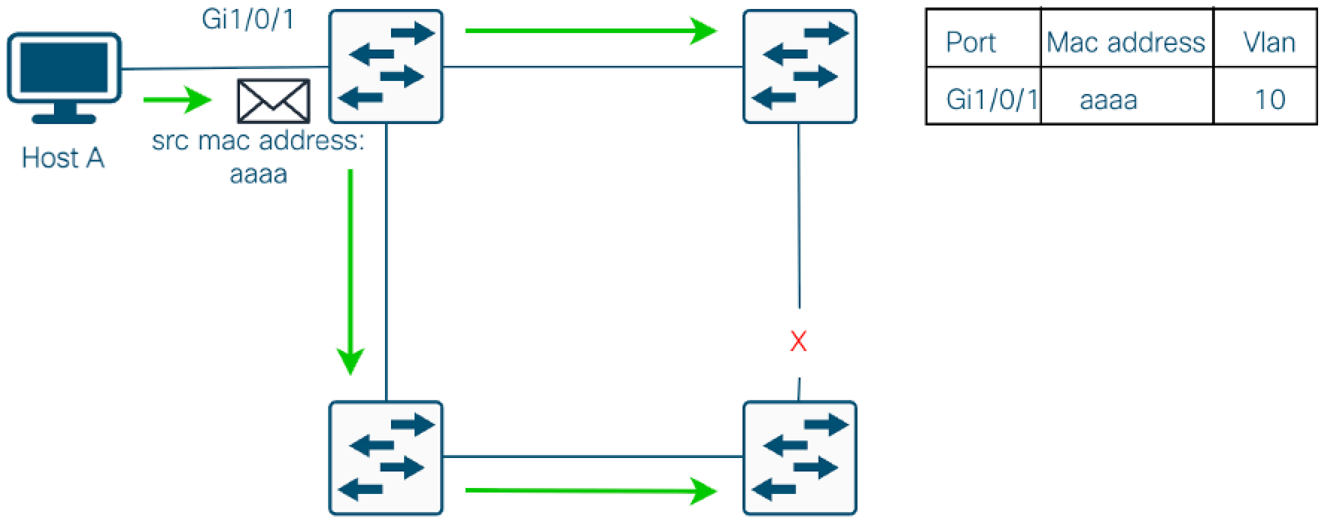
- These events are repeated as long as the switch continues to receive the traffic from both ports.

```
%SW_MATM-4-MACFLAP_NOTIF: Host aaaa.aaaa.aaaa in vlan 10 is flapping between port Gi1/0/1 and port Gi1/
```

There is traffic interruption every time the mac address changes from one port to another. When the mac address is learned on Port Gi1/0/2, the traffic destined to Host A is forwarded in this port and vice versa, resulting in packet loss.

Layer 2 Loop

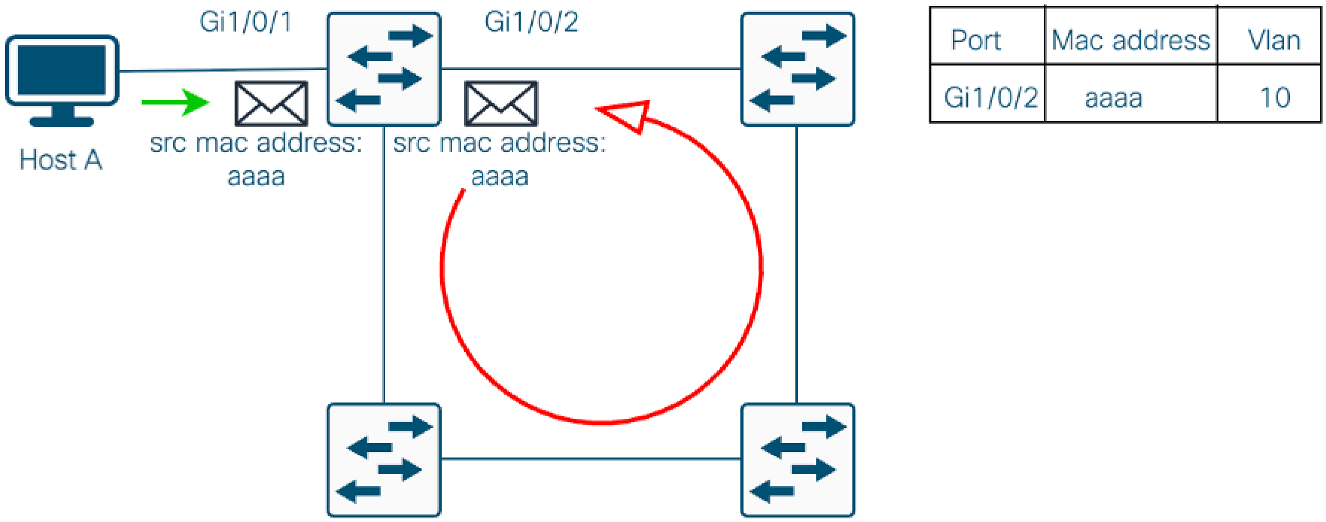
Looking at the topology in Image No. 3. you can imagine that the Host A sends a broadcast packet to the network, in normal operations, you can see that there is a redundant link blocked, so when the broadcast is sent we don't receive the packet back on the sender switch, hence, the mac address table is not altered and the traffic flows without issues.



Port	Mac address	Vlan
Gi1/0/1	aaaa	10

Image No.3

Considering topology on Image No. 4, you have a loop in the network. Now, when the Host A sends the broadcast packet to the network, you received the same packet on a different port of the switch triggering the mac flapping notification. As mentioned in previous scenario, this causes interruptions on the traffic flow.



Port	Mac address	Vlan
Gi1/0/2	aaaa	10

Image No.4

Note: There are some features, such as wireless roaming that can trigger a mac flapping on the switch, but has no impact. But, the mac flapping can be a symptom of a larger issue such as a layer 2 loop.