Troubleshoot MAC Address Flap Notification Error

Contents

Introduction

Background Information

- Description
- SyslogMessage
- MessageSample

MAC Address Flap Notification

- Impact
- Product Family

Recommendation

- Scenario Details 1
- Scenario Details 2
- Scenario Details 3
- Scenario Details 4

Commands

Introduction

This document describes how to troubleshoot MAC address flap notification errors.

Background Information

Description

This notification message is generated by the switch when it detects a MAC address flapping event on the network.

A MAC address flapping event is detected when a switch learns the same MAC address source and in the same VLAN are on two different interfaces within a short interval.

Cisco Catalyst switches notify when the same MAC address is detected on multiple switch ports, causing the switch to constantly change the port associated with the MAC address. This alert via this syslog contains the MAC address of the host, VLAN, and ports between the MAC address that is flapping. Given this behavior can be caused due to multiple reasons, identifying the underlying cause of MAC address flapping is important to ensure the stability and performance of the network.

SyslogMessage

SW_MATM-4-MACFLAP_NOTIF

MessageSample

Example: Apr 26 12:27:55 Switch-1 %SW_MATM-4-MACFLAP_NOTIF: Host **0011.2233.4455** in vlan **10** is flapping between port **Gi1/0/10

MAC Address Flap Notification

Impact

Investigate these messages to determine whether the MAC address movement is caused by expected roaming behavior, redundant system MAC movement, EtherChannel inconsistency, or a Layer 2 forwarding loop.

Product Family

- Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9200 Series Switches
- Cisco Catalyst 9500 Series Switches
- Cisco Catalyst 9600 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 3650 Series Switches
- Cisco Catalyst 6000 Series Switches
- Cisco Catalyst 6800 Series Switches
- Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 4900 Series Switches
- Cisco Catalyst 3750 Series Switches
- Cisco Catalyst 3850 Series Switches
- Cisco Catalyst 2960 Series Switches

Recommendation

There are many possible causes for this error, some that can indicate a serious network problem.

Common causes include:

- Layer-2 Loops (high network impact)
- Wireless client movement (no network impact)
- EtherChannel or port-channel misconfiguration (moderate network impact)
- Virtual MAC address movement from redundant systems or duplicated virtual machines (moderate network impact)

Scenario Details 1

Wireless client movement is often expected, and can usually be safely ignored assuming there are no service impacts observed. Clients roaming between APs that are not using CAPWAP back to a wireless controller, or roam between APs controlled by two different wireless controllers, are likely to generate this log. The time between logs generated for the same MAC address can be several seconds or several minutes apart. If you see a single MAC address moving multiple times per second, that can indicate a more serious problem and additional troubleshooting can be required.

Scenario Details 2

Some redundant systems or devices operating in an active/standby state can share a common virtual IP and MAC address, with only the active device using it at any point in time. If both devices unexpectedly become active and both begin using the virtual address, this error can be seen. Using the interfaces mentioned in the log and running the **show mac address-table address <mac-address> vlan <vlan-id>** command, trace the path of this MAC address through the network to determine where the MAC address is currently learned and which devices are generating traffic from the shared MAC address. Record the MAC address, VLAN, and interfaces reported in the syslog message, then run the command on each switch in the path. Use CDP, LLDP, interface descriptions, or the network diagram to identify the next connected device and continue tracing the MAC address until the source devices are identified. Depending on the devices generating the MAC address moves, additional troubleshooting of their redundancy state can be required.

Scenario Details 3

A common cause of MAC address flap notifications is an EtherChannel or Port-Channel misconfiguration. If the switch reports a MAC address repeatedly moving between physical links that are expected to be members of an EtherChannel, this is a strong indication the EtherChannel has not been successfully established or is not consistently formed on both ends. In this situation, one device can treat the interfaces as independent physical links while the device on the opposite end forwards traffic over them as a single logical bundle.

For example, this can occur if one switch is configured to use LACP while the peer is configured for static EtherChannel mode, or if LACP negotiation fails for another reason. On Cisco IOS or Cisco IOS XE

Catalyst switches, when LACP negotiation is unsuccessful, the interfaces do not form a port-channel. Depending on the platform, software release, and configuration, the unbundled interfaces can remain operational as individual interfaces or be placed into a suspended state. If multiple independent links remain forwarding, the switch can continuously relearn the same source MAC address on different ports and generate MAC flap notifications.

MAC flap events can also occur when there are inconsistencies in the EtherChannel configuration between the two ends of the connection. The same MAC address can appear to move between a physical interface and the logical port-channel interface, or between links that are expected to be bundled but not consistently configured. When troubleshooting this condition, verify both devices have matching EtherChannel settings, including the bundling mode, such as LACP, PAgP, or static mode. The corresponding member links assigned to the port-channel, consistent Layer 2 parameters such as trunk or access mode, VLAN membership, native VLAN, and allowed VLAN lists. Ensuring the EtherChannel is correctly negotiated and both ends have matching EtherChannel and Layer 2 configurations can eliminate these MAC address flap events when EtherChannel inconsistency is the root cause.

Scenario Details 4

Layer 2 loops often generate repeated MAC address move messages in a short period, commonly along with high input packet rates, protocol instability, and user traffic impact. Logs can typically be for a single or a small number of MAC addresses, and users can experience an impact to the network. Routing and layer 2 protocols can often fail resulting in additional logs and general instability being created.

To troubleshoot an L2 loop, run the **show interface | include is up|input rate** command and note all active interfaces that show an extremely high volume of input packets per second (generally speaking, this can be a large 6, 7, or 8+ digit number depending on the speed of the interface).

There is likely to be only 1 or 2 interfaces with an abnormally high input rate. Use **input packet rates** as the primary data point when tracing the loop path. Use spanning-tree topology changes (TCNs), root bridge state, blocked ports, and inconsistent ports as supporting data during validation. Once the high input interface is identified, use CDP, LLDP, or your interface descriptions/network diagrams to log into the neighboring device connected to that port, and run the **show interface | include is up|input rate** command again and repeat the process of tracing the interfaces with abnormal input rates. Keep track of the interfaces and hostnames as you trace them through the network.

Continue checking neighbors and look at input rates until you run out of input ports, and you run out of neighbors or end up back on the device you already checked.

One of two possible outcomes can happen during this methodology:

- If a port has no CDP, LLDP, or known neighbor and has a very high input rate, confirm operational impact, record the current interface state, and obtain authorization before administratively shutting down the interface. After shut down, wait 60 seconds and verify whether MAC flaps, high input rates,

and user impact stop. If the condition clears, keep the interface isolated until the connected device or cabling is identified. If a loop condition is still seen, keep the interface shut down and start the process over, as its possible there is a second source on the network.

- If the trace returns to a device already checked, the path contains a Layer 2 loop. Validate STP state, BPDU filter, BPDU guard events, EtherChannel consistency, trunk VLAN lists, native VLANs, unmanaged switches, and cabling to identify where loop prevention is not operating as intended. For spanning-tree networks, identify which switch in the path you traced is expected to be root, and work backwards from that device to determine which interface in the traced path is expected to block, but is currently forwarding. Once the interface that can be blocking (but is in the forwarding state) is found, administratively shut it down. Wait 60 seconds and check the network for stability. If the loop persists, keep the interface shut down and repeat this process.

Commands

Command syntax varies by platform and software release. On Cisco IOS XE, run the **show mac address-table** command. Some legacy platforms run the **show mac-address-table** syntax.

Command	Purpose
show version	Identify platform, software version, and uptime.
show logging	Review MAC flap messages and related protocol events.
show spanning-tree	Verify root bridge, port roles, port states, and topology changes.
show mac address-table address <mac-address> vlan <vlan-id>	Identify where the MAC address is currently learned.
show interfaces	Include is up.
show etherchannel summary	Verify port-channel status and member consistency.
show cdp neighbors detail / show lldp neighbors detail	Identify the neighboring device connected to an interface.