Troubleshoot MAC Flaps/Loop on Cisco Catalyst Switches

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

What is MAC Flapping?

General Troubleshooting Guidelines

Case Study 1

- Problem Description
- Topology
- Troubleshooting Steps
- Root Cause
- Resolution

Case Study 2

- Problem Description
- Topology
- Troubleshooting Steps
- Root Cause
- Resolution

Prevention

Introduction

This document describes how to troubleshoot the MAC Flaps/Loop on Cisco Catalyst Switches.

Prerequisites

Requirements

Cisco recommends that you have a fundamental knowledge of basic Switching concepts and an understanding of Spanning Tree Protocol (STP) and its features on Cisco Catalyst Switches.

Components Used

The information in this document is based on Cisco Catalyst Switches with all versions (this document is not restricted to any specific software or hardware versions).

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

This document serves as a guide that lays out a systematic approach to troubleshooting MAC flaps or loop issues on the Cisco Catalyst switches. MAC flaps/loops are disruptions in a network caused by inconsistencies in the MAC address tables of switches. This document not only provides steps to identify and resolve these issues but also includes practical examples for better understanding.

What is MAC Flapping?

A MAC flap occurs when a switch receives a frame with the same MAC source address but from a different interface than the one it initially learned it from. This causes the switch to flap between ports, updating its MAC address table with the new interface. This situation can cause instability in the network and lead to performance issues.

In a Cisco switch, MAC flapping is typically logged as a message similar to this:

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

In this example, the MAC address xxxx.xxxx.xxxx was first learned on interface port (1), then seen on interface port (2), causing a MAC flap.

The most common cause of MAC flapping is a Layer 2 loop in the network, often due to a misconfiguration of STP or issues with redundant links. Other causes can include faulty hardware, software bugs, or even security issues such as MAC spoofing.

Troubleshooting MAC flaps often involves identifying and resolving any loops in the network, checking device configurations, or updating device firmware/software.

General Troubleshooting Guidelines

- Identify the MAC Flapping: Look for logs in your switch that indicate MAC flapping. For example, in a Cisco switch, the log message looks like this:

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- Note the MAC Address and Interfaces: The log message gives you the MAC address that is flapping and the interfaces it is flapping between. Take note of these as they help in your investigation.
- Investigate the Affected Interfaces: Use the CLI of the switch in order to investigate the interfaces involved. You can use commands like show interfaces or show mac address-table in order to see which devices are connected to the interfaces and where the MAC address is being learned.
- Trace the Flapping MAC Address: MAC is learning through ports X and Y. One port leads us to where that MAC is plugged in and the other leads us to the loop. Pick a port and start working through

using `show mac address-table` command on each Layer 2 switch in the path.

- Check for Physical Loops: Look at your network topology in order to see if there are any physical loops. These can occur if multiple paths exist between switches. If a loop is found, you need to reconfigure your network in order to remove the loop.
- Check STP: STP is designed in order to prevent loops in your network by blocking certain paths. If STP is misconfigured, it does not prevent loops as it must be. Use commands like `show spanning-tree` in order to check the STP configuration. Also, check for Topology Change Notifications (TCNs) using the command `show spanning-tree detail | include ieee|occur|from|is`.
- Check for Duplicate MAC Addresses: If two devices on your network have the same MAC address (mostly seen in High Availability (HA) setup and multiple Network Interface Controller or Cards (NICs)), it can cause MAC flapping. Use the `show mac address-table` command in order to look for duplicate MAC addresses on your network.
- Check for Faulty Hardware or Cables: Faulty network cables or hardware can cause frames to be sent to the wrong interfaces, leading to MAC flapping. Check the physical condition of your cables and consider swapping out hardware in order to see if the problem persists. Interface flapping can also cause MAC flapping on switches.
- Check for Software Bugs: Sometimes, MAC flapping can be caused by bugs in the software of your network devices. Check on the Bug search tool.

Bug Search Tool: https://bst.cloudapps.cisco.com/bugsearch

Bug Search Tool Help: https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

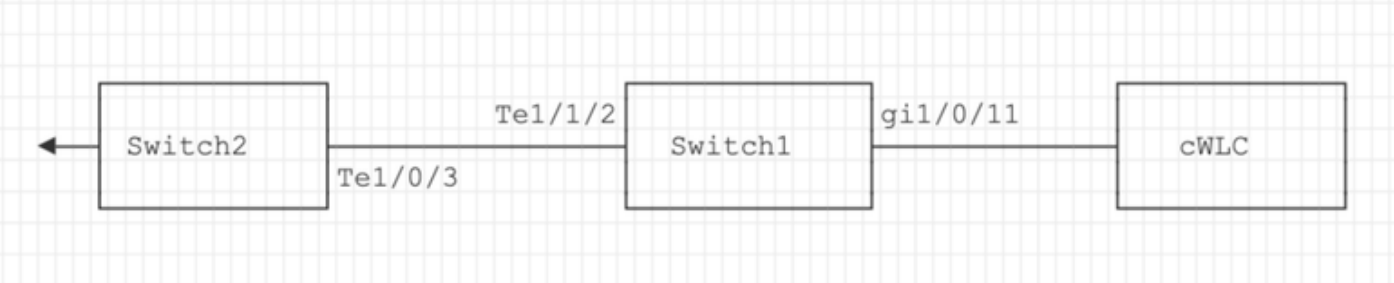
- Contact TAC Support: If you have tried everything and the problem still persists, it can be time to contact Cisco TAC support. They can provide further assistance.

Case Study 1

Problem Description

The eWLC controller is experiencing a loss of connectivity to the gateway, and packet drops are preventing APs from joining the controller.

Topology



Troubleshooting Steps

MAC flapping was identified on the switch (Switch1) that is connected to the eWLC.

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

MAC Learning:

Enter the command show mac address-table address <mac> in order to check the MAC address learned on the port.

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    DYNAMIC     Gi1/0/11

   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

Configuration of Ports Gi1/0/11 and Te1/1/2:

Enter the command show running-config interface <interface-number> in order to check the interface configuration.

<#root>

```
interface GigabitEthernet1/0/11

 switchport trunk native vlan 4
 switchport mode trunk
end

interface TenGigabitEthernet1/1/2

 switchport mode trunk
end
```

CDP Neighbors of Ports Gi1/0/11 and Te1/1/2:

Enter the command show cdp neighbors <interface-number> in order to check the details of connected devices.

<#root>

```
Switch1#show cdp neighbors gi1/0/11

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
```

```
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller



Switch1#show cdp neighbors gi1/1/2


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Switch2


                Ten 1/1/2         163             R S I  C9500-16X Ten 1/0/3 < ----- Uplink Switch
```

MAC Learning on Switch2 (Uplink Switch):

Enter the command show mac address-table address <mac> in order to check the MAC address learned on the port.

<#root>

```
Switch2#show mac address-table address 0000.5E00.0101


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC

Vl4 < ----- VRRP MAC of Vlan4


   4    0000.5e00.0101    DYNAMIC

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)
```

<#root>

```
Switch2#show vrrp  vlan 4


Vlan4 - Group 1

 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x

  Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4
```

```
  Advertisement interval is 1000 msec
```

Root Cause

It was verified that the Virtual Router Redundancy Protocol (VRRP) ID of Switch 2 and the eWLC were the same, which resulted in the generation of the same virtual MAC by the VRRP.

Resolution

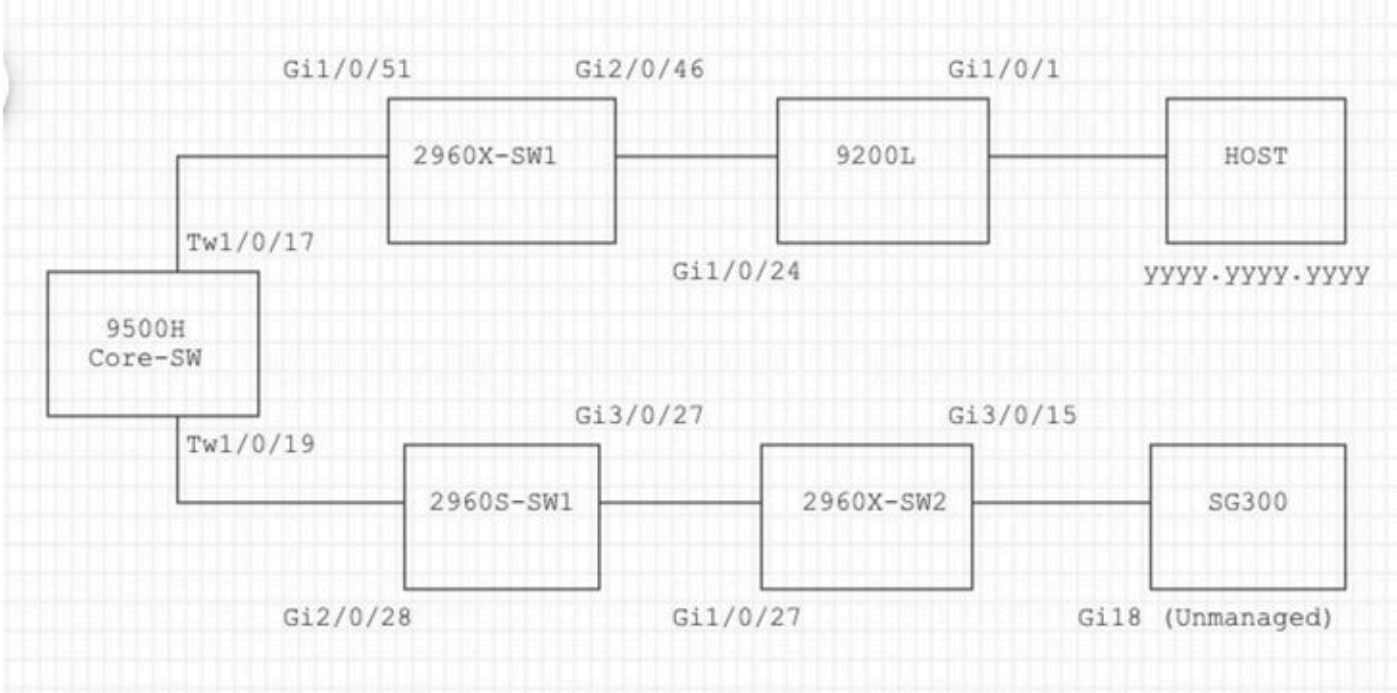
The issue was resolved after changing the VRRP instance on the WLC, which was causing a duplicate MAC on the switch leading to a loss of connectivity to the gateway and packet drops, which prevented the APs from joining the controller.

Case Study 2

Problem Description

Some of the servers are either inaccessible or experiencing significant latency/drops.

Topology



Troubleshooting Steps

1. Noticed MAC flapping occurring on the Core switch.

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2. Chosen the MAC address yyyy.yyyy.yyyy for the troubleshooting process.

MAC Learning:

Enter the command show mac address-table address <mac> in order to check the MAC address learned on the port.

<#root>

```
Core-SW#show mac address-table address yyyy.yyyy.yyyy

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Twe1/0/17
```

CDP Neighbors of Ports Twe 1/0/17 and Twe 1/0/17:

Enter the command show cdp neighbors <interface-number> in order to check the details of connected devices.

<#root>

```
Core-SW#show cdp neighbors Twe 1/0/17

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960X-SW1

                 Twe 1/0/17        162              S I   WS-C2960X Gig 1/0/51



Core-SW#show cdp neighbors Twe 1/0/19

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960S-SW1

                 Twe 1/0/19        120              S I   WS-C2960S Gig 2/0/28
```

Logs from 2960X-SW1 Connected to Core-SW Twe1/0/17:

MAC yyyy.yyyy.yyyy is flapping between port Gi1/0/51 and Gi2/0/46 (9200L).

<#root>

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Gi1/0/51
```

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46
```

2960X-SW1#show run interface gi 1/0/51

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end
```

2960X-SW1#show run interface gi 2/0/46

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

Logs from 9200L:

(This appears to be the valid port for this MAC address.)

<#root>

9200L#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1
```

9200L#show run interface gi 1/0/1

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

2960S-SW1 Connected to Core-SW Twe1/0/19:

(Appears to be a loop path.) The port on the Core-SW was shut down in order to mitigate the loop.

However, MAC flaps were still being observed on the Core-SW.

Logs from 2960S-SW1:

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G
```

2960S-SW1#show run interface gi 3/0/27

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end
```

2960S-SW1#show cdp neighbor gi 3/0/27

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW2

Gig 3/0/27 176 S I WS-C2960X Gig 1/0/27

Logs from 2960X-SW2:

<#root>

```
2960X-SW2#show run interface gi 3/0/15


Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end


2960X-SW2#show cdp neighbor gi 3/0/15


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

SG300     Gig 3/0/15        157              S I   SG300-28P gi18




2960X-SW2#config terminal


2960X-SW2(config)#interface gi 3/0/15


2960X-SW2(config-if)#shutdown
```

Root Cause

MAC flaps were seen due to the SG300 (unmanaged) switch connected to the network.

Resolution

The MAC flapping issue was resolved by shutting down the port connected to the unmanaged switch SG300.

Prevention

STP Portfast:

STP PortFast causes a Layer 2 LAN port to enter the forwarding state immediately, bypassing the listening and learning states. STP PortFast prevents the generation of STP TCNs, which are not meaningful from ports that do not receive STP Bridge Protocol Data Units (BPDUs). Configure STP PortFast only on ports that are connected to end host devices that terminate VLANs and from which the port must never receive

STP BPDUs, such as Workstations, Servers, Ports on routers that are not configured to support bridging.

BPDU Guard:

STP BPDU Guard complements the functionality of STP PortFast. On STP PortFast-enabled ports, STP BPDU Guard protects Layer 2 loops that STP cannot provide when STP PortFast is enabled. STP BPDU Guard shuts down ports that receive BPDUs.

Root Guard:

Root guard prevents ports from becoming STP root ports. Use STP Root Guard in order to prevent unsuitable ports from becoming STP root ports. An example of an unsuitable port is a port that links to a device that is outside direct network administrative control.

Loop Guard:

Loop guard is a Cisco proprietary optimization for the STP. Loop guard protects Layer 2 networks from loops that occur when something prevents the normal forwarding of BPDUs on point-to-point links (for example, a network interface malfunction or a busy CPU). Loop guard complements the protection against unidirectional link failures provided by Unidirectional Link Detection (UDLD). Loop guard isolates failures and lets STP converge to a stable topology with the failed component excluded from the STP topology.

BPDU Filter:

This disables the STP. BPDUs are neither sent nor processed upon receipt. It is common with service providers, not necessarily enterprise networks.

UDLD Aggressive:

The Cisco-proprietary UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. UDLD detects the existence of unidirectional links. UDLD can operate in either normal or aggressive mode. Normal-mode UDLD classifies a link as unidirectional if the received UDLD packets do not contain information that is correct for the neighbor device. In addition to the functionality of normal mode UDLD, aggressive mode UDLD puts ports into the err-disabled state if the relationship between two previously synchronized neighbors cannot be re-established.

Storm Control:

Traffic storm control is implemented in hardware and does not affect the overall performance of the switch. Typically, end-stations such as PCs and servers are the source of broadcast traffic that can be suppressed. In order to avoid unnecessary processing of excess broadcast traffic, enable traffic storm control for broadcast traffic on access ports that connect to end stations and on ports that connect to key network nodes.