排除Cisco Catalyst交换机上的MAC摆动/环路故障

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

什么是MAC摆动？

常见故障排除指南

案例研究1

- 问题说明
- 拓扑
- 故障排除步骤
- 根本原因
- 分辨率

案例研究2

- 问题说明
- 拓扑
- 故障排除步骤
- 根本原因
- 分辨率

预防

简介

本文档介绍如何对Cisco Catalyst交换机上的MAC摆动/环路进行故障排除。

先决条件

要求

Cisco建议您了解基本交换概念的基础知识，并了解Cisco Catalyst交换机上的生成树协议(STP)及其功能。

使用的组件

本文档中的信息基于所有版本的Cisco Catalyst交换机（本文档不限于任何特定的软件或硬件版本）。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档将作为一个指南，说明对Cisco Catalyst交换机上的MAC抖动或环路问题进行故障排除的系统方法。MAC摆动/环路是由交换机MAC地址表不一致而导致的网络中断。本文档不仅提供了识别和解决这些问题的步骤，还包括用于加深理解的实用示例。

什么是MAC摆动？

当交换机收到的MAC源地址相同，但来自不同接口的帧不同于它最初获知的帧时，就会发生MAC抖动。这会导致交换机在端口之间摆动，使用新接口更新其MAC地址表。这种情况会导致网络不稳定，并导致性能问题。

在Cisco交换机中，MAC抖动通常记录为类似于以下内容的消息：

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

在本示例中，MAC地址首先在接口端口(1)上获取，然后在接口端口(2)上查看，从而导致MAC摆动xxxx.xxxx.xxxx。

MAC抖动最常见的原因是网络中的第2层环路，通常是由于STP配置错误或冗余链路问题。其他原因可能包括硬件故障、软件错误，甚至包括MAC欺骗等安全问题。

对MAC抖动进行故障排除通常涉及识别和解决网络中的任何环路、检查设备配置或更新设备固件/软件。

常见故障排除指南

- 确定MAC抖动：在交换机中查找指示MAC抖动的日志。例如，在Cisco交换机中，日志消息如下所示：

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

- 注意MAC地址和接口：日志消息为您提供了抖动的MAC地址以及它在其间摆动的接口。请注意这些信息，因为它们有助于您的调查。
- 检查受影响的接口：使用交换机的CLI检查所涉及的接口。您可以使用类似或show interfacesshow mac address-table 命令查看哪些设备连接到接口以及获取MAC地址的位置。
- 跟踪抖动的MAC地址：MAC通过端口X和Y学习。一个端口将我们引向该MAC的插入位置，另一个则引向环路。选取一个端口，然后在该路径中show mac address-table的每台第2层交换机上使用

命令开始工作。

- 检查物理环路：查看网络拓扑，以查看是否存在任何物理环路。如果交换机之间存在多条路径，则会发生这种情况。如果发现环路，则必须重新配置网络以删除该环路。
- 检查STP:STP旨在通过阻塞某些路径来防止网络中的环路。如果STP配置错误，它不会像必须的那样防止环路。使用类似show spanning-tree的命令检查STP配置。此外，使用命令检查拓扑更改通知(TCNshow spanning-tree detail | include ieee|occur|from|is)。
- 检查重复的MAC地址：如果网络中的两台设备具有相同的MAC地址(主要在高可用性(HA)设置和多个网络接口控制器或网卡(NIC)中可见)，则可能导致MAC摆动。使用show mac address-table命令查找网络上的重复MAC地址。
- 检查有故障的硬件或电缆：网络电缆或硬件故障可能导致帧发送到错误的接口，从而导致MAC摆动。检查电缆的物理状况，并考虑换出硬件以查看问题是否仍然存在。接口抖动也可能导致交换机上的MAC抖动。
- 检查软件错误：有时，MAC抖动可能是由网络设备的软件中的漏洞引起的。检查Bug搜索工具。

漏洞搜索工具：https://bst.cloudapps.cisco.com/bugsearch

Bug 搜索工具帮助:https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

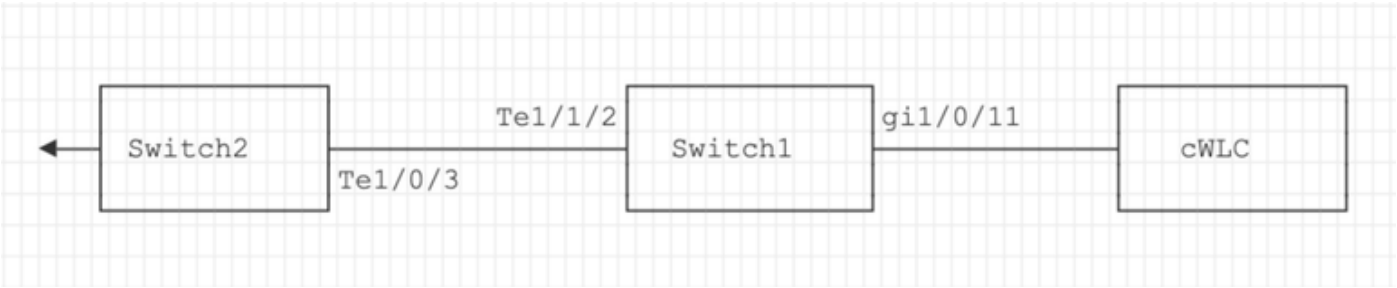
- 联系TAC支持：如果您已经尝试了所有方法，但问题依然存在，那么是时候联系Cisco TAC支持了。它们可以提供进一步的援助。

案例研究1

问题说明

eWLC控制器与网关的连接丢失，丢包阻止AP加入控制器。

拓扑



故障排除步骤

在连接到eWLC的交换机（交换机1）上识别出MAC抖动。

```
*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学习：

输入命令show mac address-table address
，检查端口上获取的MAC地址。

<#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
```

端口Gi1/0/11和Te1/1/2的配置：

输入命令show running-config interface
，检查接口配置。

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

端口Gi1/0/11和Te1/1/2的CDP邻居：

输入命令show cdp neighbors
，检查所连接设备的详细信息。

<#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

Switch2上的MAC学习（上行链路交换机）：

输入命令show mac address-table address
，检查端口上获取的MAC地址。

<#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
```

根本原因

经验证交换机2的虚拟路由器冗余协议(VRRP)ID与eWLC相同，导致VRRP生成相同的虚拟MAC。

分辨率

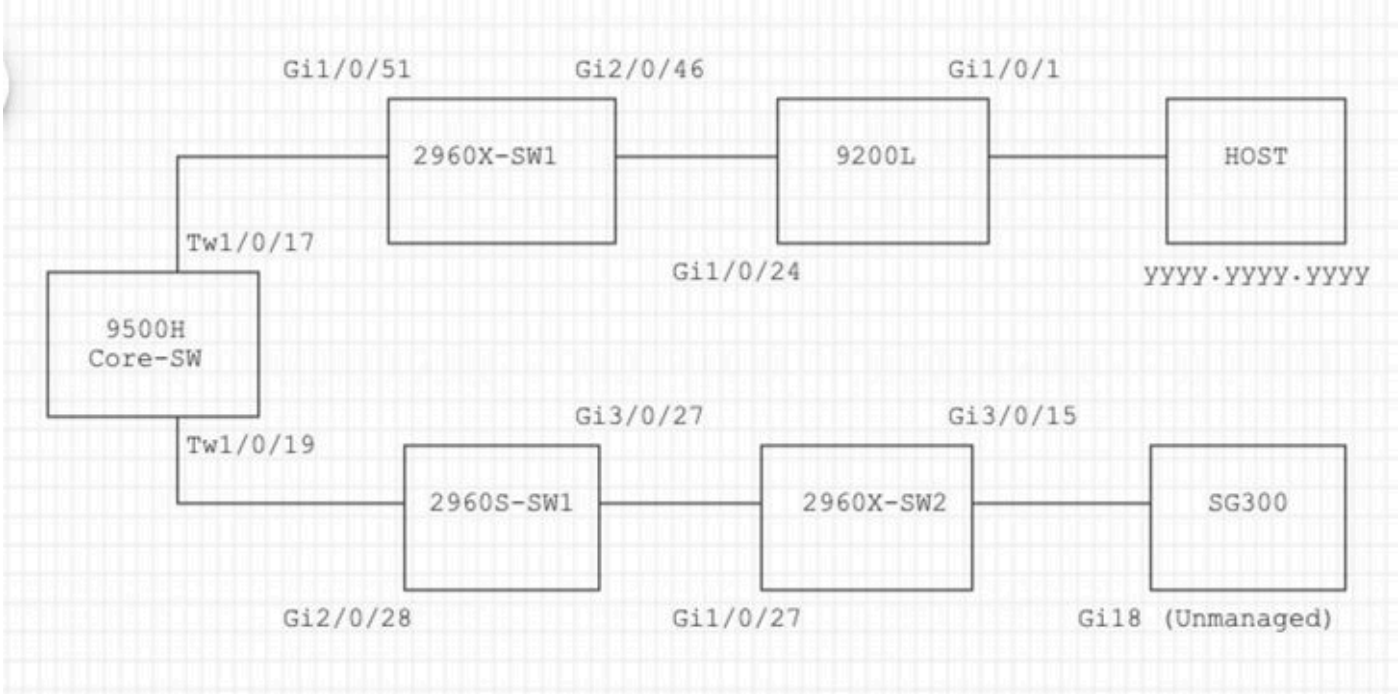
更改WLC上的VRRP实例后，问题得到解决，该问题导致交换机上出现重复的MAC，导致与网关的连接中断和丢包，从而阻止AP加入控制器。

案例研究2

问题说明

有些服务器无法访问，或遇到严重延迟/丢弃。

拓扑



故障排除步骤

1.注意到核心交换机上发生了MAC抖动。

```
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.选择用于故障排除yyyy.yyyy.yyyy过程的MAC地址。

MAC学习：

输入命令show mac address-table address
，检查端口上获取的MAC地址。

<#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
```

端口Twe 1/0/17和Twe 1/0/19的CDP邻居：

输入命令show cdp neighbors
，检查所连接设备的详细信息。

<#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

从2960X-SW1连接到核心 — SW Twe1/0/17的日志：

MAC$_{yyyy.yyyy.yyyy}$在端口Gi1/0/51和Gi2/0/46(9200L)之间摆动。

<#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
```

来自9200L的日志：

（这似乎是此MAC地址的有效端口。）

<#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连接到Core-SW Twe1/0/19:

（似乎为循环路径。）为了缓解环路，Core-SW上的端口已关闭。

但是，在Core-SW上仍然观察到MAC摆动。

2960S-SW1的日志：

<#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
```

2960X-SW2的日志：

<#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
```

根本原因

由于连接到网络的SG300（非托管）交换机，出现MAC摆动。

分辨率

通过关闭连接到非托管交换机SG300的端口解决了MAC抖动问题。

预防

STP Portfast:

STP PortFast会使第2层LAN端口立即进入转发状态，从而绕过侦听和学习状态。STP PortFast可防止生成STP TCN，对于未接收STP网桥协议数据单元(BPDU)的端口而言，STP TCN没有意义。 仅在连接到端接VLAN的终端主机设备的端口上配置STP PortFast，并且端口绝不能从中接收STP BPDU，例如未配置为支持桥接的路由器上的工作站、服务器和端口。

BPDU 防护:

STP BPDU防护补充了STP PortFast的功能。在启用了STP PortFast的端口上，STP BPDU防护可保护STP在启用STP PortFast时无法提供的第2层环路。STP BPDU防护会关闭接收BPDU的端口。

根保护:

根防护可防止端口成为STP根端口。使用STP根防护可防止不适当的端口成为STP根端口。例如，不合适的端口会链接到直接网络管理控制之外的设备。

环路防护:

环路防护是Cisco专有的STP优化。环路防护可防止第2层网络在点对点链路上出现BPDU正常转发时出现的环路（例如，网络接口故障或CPU繁忙）。 环路防护是对单向链路检测(UDLD)提供的单向链路故障防护的补充。 环路防护可隔离故障并使STP收敛到稳定的拓扑，故障组件将从STP拓扑中排除。

BPDU过滤器：

这将禁用STP。BPDU在接收时既不发送也不处理。这在服务提供商中很常见，不一定是企业网络。

UDLD主动：

Cisco专有的UDLD协议监控支持UDLD的设备和端口之间的链路的物理配置。UDLD检测是否存在单向链路。UDLD可以在正常或主动模式下运行。如果收到的UDLD数据包不包含对邻居设备正确的信息，正常模式UDLD会将链路分类为单向链路。除了正常模式UDLD的功能外，如果无法重新建立两个先前同步的邻居之间的关系，主动模式UDLD会将端口置于err-disabled状态。

风暴控制:

流量风暴控制在硬件中实施，不会影响交换机的整体性能。通常，PC和服务器等终端站是可以被抑制的广播流量的来源。为了避免不必要的过度广播流量处理，请在连接到终端站的接入端口和连接到关键网络节点的端口上启用广播流量风暴控制。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。