Resolución de Problemas de MAC Flaps/Loop en Switches Cisco Catalyst

Contenido

Introducción

Este documento describe cómo resolver problemas de MAC Flaps/Loop en los Cisco Catalyst Switches.

Prerequisites

Requirements

Cisco recomienda que tenga un conocimiento fundamental de los conceptos básicos de switching y una comprensión del protocolo de árbol de extensión (STP) y sus funciones en los switches Catalyst de Cisco.

Componentes Utilizados

La información de este documento se basa en los switches Catalyst de Cisco con todas las versiones (este documento no se limita a ninguna versión específica de software o hardware).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento sirve como guía que establece un enfoque sistemático para la resolución de problemas de inestabilidad MAC o problemas de loop en los switches Cisco Catalyst. Los flaps/loops MAC son interrupciones en una red causadas por inconsistencias en las tablas de direcciones MAC de los switches. Este documento no solo proporciona pasos para identificar y resolver estos problemas, sino que también incluye ejemplos prácticos para una mejor comprensión.

¿Qué es la inestabilidad MAC?

Una inestabilidad MAC ocurre cuando un switch recibe una trama con la misma dirección MAC de origen pero desde una interfaz diferente de la que inicialmente aprendió. Esto hace que el switch aletee entre los puertos, actualizando su tabla de direcciones MAC con la nueva interfaz. Esta situación puede provocar inestabilidad en la red y problemas de rendimiento.

En un switch de Cisco, la inestabilidad de MAC se registra generalmente como un mensaje similar a este:

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

En este ejemplo, la dirección MAC`xxxx.xxxx.xxxx`se aprendió primero en el puerto de interfaz (1) y luego se vio en el puerto de interfaz (2), lo que provocó una inestabilidad de MAC.

La causa más común de inestabilidad de MAC es un loop de Capa 2 en la red, a menudo debido a una configuración incorrecta de STP o problemas con links redundantes. Otras causas pueden incluir hardware defectuoso, errores de software o incluso problemas de seguridad como la suplantación de MAC.

La resolución de problemas de inestabilidad MAC a menudo implica la identificación y resolución de cualquier loop en la red, la comprobación de las configuraciones del dispositivo o la actualización del firmware/software del dispositivo.

Pautas generales para la solución de problemas

- Identificación de la inestabilidad de MAC: Busque registros en el switch que indiquen

inestabilidad de MAC. Por ejemplo, en un switch de Cisco, el mensaje de registro tiene el siguiente aspecto:

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

- Tenga en cuenta la dirección MAC y las interfaces: El mensaje de registro le da la dirección MAC que está inestable y las interfaces entre las que está inestable. Tome nota de estos como ayuda en su investigación.
- Investigue las interfaces afectadas: Utilice la CLI del switch para investigar las interfaces involucradas. Puede utilizar comandos como`show interfaces`o`show mac address-table`para ver qué dispositivos están conectados a las interfaces y dónde se está aprendiendo la dirección MAC.
- Seguimiento de la dirección MAC inestable: MAC está aprendiendo a través de los puertos X e Y. Un puerto nos lleva a donde está conectado ese MAC y el otro nos lleva al loop. Elija un puerto y comience a trabajar a través del uso`show mac address-table`del comando en cada switch de Capa 2 en la trayectoria.
- Comprobar si hay bucles físicos: Observe su topología de red para ver si hay algún loop físico. Esto puede ocurrir si existen varias trayectorias entre los switches. Si se encuentra un loop, debe reconfigurar su red para quitar el loop.
- Comprobar STP: STP está diseñado para prevenir loops en su red mediante el bloqueo de ciertas trayectorias. Si el STP está mal configurado, no evita los loops como debe ser. Utilice comandos como`show spanning-tree`para verificar la configuración STP. Además, compruebe las notificaciones de cambio de topología (TCN) mediante el comando`show spanning-tree detail | include ieee|occur|from|is`.
- Comprobar si hay direcciones MAC duplicadas: Si dos dispositivos de la red tienen la misma dirección MAC (que se ve principalmente en la configuración de alta disponibilidad (HA) y varias tarjetas o controladores de interfaz de red (NIC)), puede provocar intermitencias de MAC. Utilice el`show mac address-table`comando para buscar direcciones MAC duplicadas en su red.
- Compruebe si hay hardware o cables defectuosos: Los cables de red o el hardware defectuosos pueden hacer que las tramas se envíen a las interfaces incorrectas, lo que provoca inestabilidad de MAC. Compruebe el estado físico de los cables y considere cambiar el hardware para ver si el problema continúa. La inestabilidad de la interfaz también puede provocar inestabilidad de MAC en los switches.
- Buscar errores de software: A veces, los fallos de MAC pueden deberse a errores en el software de los dispositivos de red. Consulte la herramienta de búsqueda de errores.

Herramienta de búsqueda de errores: https://bst.cloudapps.cisco.com/bugsearch

Ayuda con la herramienta de búsqueda de errores: https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

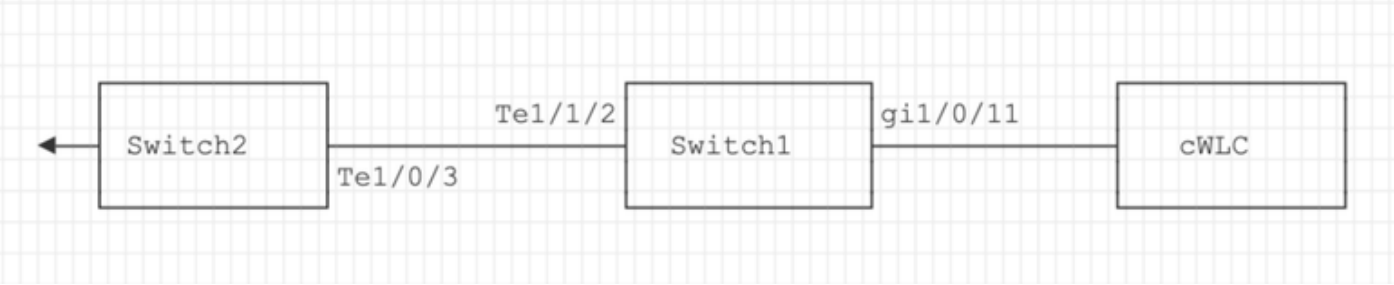
- Póngase en contacto con el soporte de TAC: Si lo ha intentado todo y el problema persiste, puede que sea el momento de ponerse en contacto con el soporte técnico del Cisco TAC. Pueden proporcionar más asistencia.

Caso Práctico 1

Descripción de problemas

El controlador eWLC está experimentando una pérdida de conectividad con el gateway, y las caídas de paquetes están impidiendo que los AP se unan al controlador.

Topología



Pasos para la resolución de problemas

Se identificó la inestabilidad de MAC en el switch (Switch1) que está conectado al 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
```

Aprendizaje de MAC:

Ingrese el comando`show mac address-table address`
para verificar la dirección MAC aprendida en el puerto.

<#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
```

Configuración de los Puertos Gi1/0/11 y Te1/1/2:

Ingrese el comando`show running-config interface`
para verificar la configuración de la interfaz.

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

Vecinos CDP de los puertos Gi1/0/11 y Te1/1/2:

Ingrese el comando`show cdp neighbors`
para verificar los detalles de los dispositivos conectados.

<#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
```

Aprendizaje de MAC en Switch2 (conmutador de enlace ascendente):

Ingrese el comando`show mac address-table address`
para verificar la dirección MAC aprendida en el puerto.

<#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
```

Causa raíz

Se verificó que el ID de Virtual Router Redundancy Protocol (VRRP) del Switch 2 y el eWLC eran iguales, lo que resultó en la generación del mismo MAC virtual por parte del VRRP.

Resolución

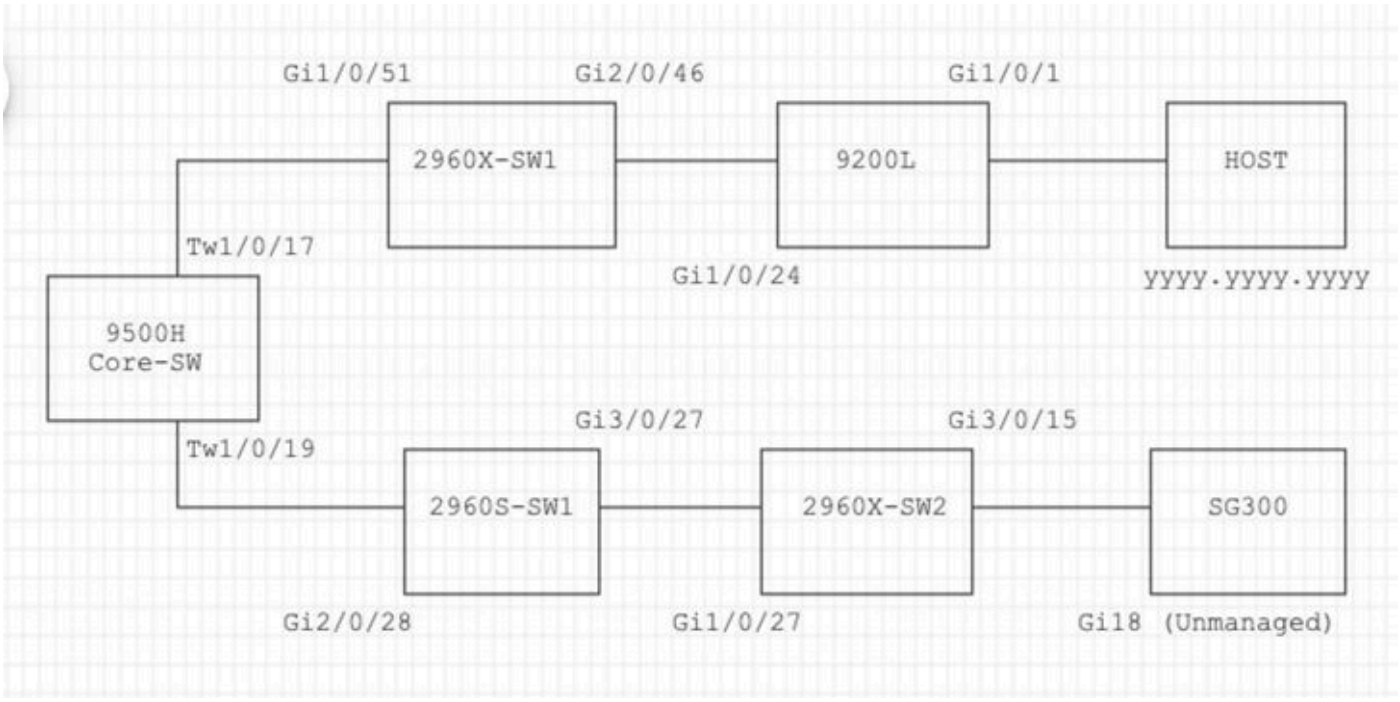
El problema se resolvió después de cambiar la instancia de VRRP en el WLC, lo que estaba causando una MAC duplicada en el switch que conducía a una pérdida de conectividad con el gateway y caídas de paquetes, lo que impedía que los AP se unieran al controlador.

Caso Práctico 2

Descripción de problemas

Algunos de los servidores son inaccesibles o experimentan una latencia o caídas significativas.

Topología



Pasos para la resolución de problemas

1. Se ha observado un aleteo de MAC en el switch principal.

```
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. Elija la dirección MAC`yyyy.yyyy.yyyy`para el proceso de resolución de problemas.

Aprendizaje de MAC:

Ingrese el comando`show mac address-table address`
para verificar la dirección MAC aprendida en el puerto.

<#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
```

Vecinos CDP de puertos Twe 1/0/17 y Twe 1/0/19:

Ingrese el comando`show cdp neighbors`
para verificar los detalles de los dispositivos conectados.

<#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
```

Registros de 2960X-SW1 conectados a Core-SW1/0/17:

MAC`yyyy.yyyy.yyyy`es inestable entre el puerto Gi1/0/51 y 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
```

Registros desde 9200L:

(Este parece ser el puerto válido para esta dirección MAC.)

<#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 conectado a Core-SW1/0/19:

(Parece ser una ruta de bucle.) El puerto en el Core-SW fue apagado para mitigar el loop.

Sin embargo, todavía se observaban flaps MAC en el Core-SW.

Registros de 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

Registros de 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
```

Causa raíz

Se observaron inestabilidad de MAC debido al switch SG300 (no gestionado) conectado a la red.

Resolución

El problema de inestabilidad de MAC se resolvió apagando el puerto conectado al switch no administrado SG300.

Prevención

STP Portfast:

STP PortFast hace que un puerto LAN de Capa 2 ingrese al estado de reenvío inmediatamente, omitiendo los estados de escucha y aprendizaje. STP PortFast evita la generación de TCN STP, que no son significativas de los puertos que no reciben las Unidades de datos de protocolo de puente STP (BPDU). Configure STP PortFast solamente en los puertos que están conectados a los dispositivos host extremos que terminan las VLAN y desde los cuales el puerto nunca debe recibir STP BPDU, como estaciones de trabajo, servidores, puertos en los routers que no están configurados para soportar el bridging.

Protección BPDU:

STP BPDU Guard complementa la funcionalidad de STP PortFast. En los puertos con STP PortFast habilitado, STP BPDU Guard protege los loops de Capa 2 que STP no puede proporcionar cuando STP PortFast está habilitado. La protección STP BPDU apaga los puertos que reciben BPDU.

Protección de Raíz:

La protección de raíz evita que los puertos se conviertan en puertos raíz STP. Utilice STP Root Guard para evitar que los puertos no adecuados se conviertan en puertos raíz STP. Un ejemplo de puerto no adecuado es un puerto que enlaza con un dispositivo que está fuera del control administrativo directo de la red.

Protección de loop:

La protección contra loops es una optimización propietaria de Cisco para el STP. La protección contra loops protege las redes de Capa 2 de loops que ocurren cuando algo impide el reenvío normal de BPDU en links punto a punto (por ejemplo, un mal funcionamiento de la interfaz de red o una CPU ocupada). La protección contra loops complementa la protección contra fallas de link unidireccional proporcionada por la Detección de Link Unidireccional (UDLD). La protección contra loops aísla fallas y permite que el STP converja a una topología estable con el componente fallido excluido de la topología del STP.

Filtro BPDU:

Esto inhabilita el STP. Las BPDU no se envían ni se procesan al recibirlas. Es común con los proveedores de servicios, no necesariamente con las redes empresariales.

UDLD agresivo:

El protocolo UDLD propiedad de Cisco monitorea la configuración física de los links entre los dispositivos y los puertos que soportan UDLD. UDLD detecta la existencia de links unidireccionales. El UDLD puede funcionar en modo normal o agresivo. El UDLD de modo normal clasifica un link como unidireccional si los paquetes UDLD recibidos no contienen información correcta para el dispositivo vecino. Además de la funcionalidad del UDLD de modo normal, el UDLD de modo agresivo pone los puertos en el estado err-disabled si la relación entre dos vecinos previamente sincronizados no se puede restablecer.

Control de tormentas:

El control de tormentas de tráfico se implementa en el hardware y no afecta al rendimiento general del switch. Normalmente, las estaciones finales, como los PC y los servidores, son el origen del tráfico de difusión que se puede suprimir. Para evitar el procesamiento innecesario del exceso de tráfico de difusión, habilite el control de tormentas de tráfico para el tráfico de difusión en los puertos de acceso que se conectan a las estaciones finales y en los puertos que se conectan a los nodos de red clave.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).