Identificar e Solucionar Problemas de Flaps/Loop MAC em Switches Cisco Catalyst

Contents

Introdução

Este documento descreve como solucionar problemas de Flaps/Loop MAC em Cisco Catalyst Switches.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha um conhecimento fundamental dos conceitos básicos de switching e uma compreensão do Spanning Tree Protocol (STP) e seus recursos nos Cisco Catalyst Switches.

Componentes Utilizados

As informações neste documento são baseadas nos Cisco Catalyst Switches com todas as versões (este documento não está restrito a nenhuma versão específica de software ou hardware).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento serve como um guia que estabelece uma abordagem sistemática para a solução de problemas de oscilações MAC ou problemas de loop nos switches Cisco Catalyst. Flaps/loops de MAC são interrupções em uma rede causadas por inconsistências nas tabelas de endereços MAC dos switches. Este documento não apenas fornece etapas para identificar e resolver esses problemas, mas também inclui exemplos práticos para melhor compreensão.

O que é oscilação de MAC?

Uma oscilação de MAC ocorre quando um switch recebe um quadro com o mesmo endereço MAC de origem, mas de uma interface diferente daquela com a qual ele o aprendeu inicialmente. Isso faz com que o switch oscile entre as portas, atualizando sua tabela de endereços MAC com a nova interface. Essa situação pode causar instabilidade na rede e levar a problemas de desempenho.

Em um switch Cisco, a oscilação de MAC é normalmente registrada como uma mensagem semelhante a esta:

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

Neste exemplo, o endereço`xxxx.xxxx.xxxx`MAC foi primeiramente aprendido na porta de interface (1) e, em seguida, visto na porta de interface (2), causando um flap MAC.

A causa mais comum da oscilação de MAC é um loop de Camada 2 na rede, geralmente devido a uma configuração incorreta do STP ou a problemas com links redundantes. Outras causas podem incluir falhas de hardware, bugs de software ou até mesmo problemas de segurança, como falsificação de MAC.

A identificação e solução de problemas de oscilações de MAC geralmente envolve a identificação e a resolução de quaisquer loops na rede, a verificação das configurações do dispositivo ou a atualização do firmware/software do dispositivo.

Diretrizes gerais de solução de problemas

- Identifique a oscilação de MAC: Procure registros em seu switch que indiquem oscilação de MAC. Por exemplo, em um switch da Cisco, a mensagem de log é semelhante a esta:

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

- Observe o endereço MAC e as interfaces: A mensagem de registro fornece o endereço MAC que está oscilando e as interfaces entre as quais ele está oscilando. Anote-os, pois eles ajudarão em sua investigação.
- Investigue as interfaces afetadas: Use o CLI do switch para investigar as interfaces envolvidas. Você pode usar comandos como`show interfaces`ou`show mac address-table`para ver quais dispositivos estão conectados às interfaces e onde o endereço MAC está sendo aprendido.
- Rastreie o endereço MAC não sincronizado: O MAC está aprendendo através das portas X e Y. Uma porta nos leva ao local onde o MAC está conectado e a outra nos leva ao loop. Escolha uma porta e comece a trabalhar usando`show mac address-table`comandos em cada switch de Camada 2 no caminho.
- Verificar Loops Físicos: Examine sua topologia de rede para ver se há algum loop físico. Isso pode ocorrer se existirem vários caminhos entre os switches. Se um loop for encontrado, você deverá reconfigurar sua rede para removê-lo.
- Verificar STP: O STP foi projetado para evitar loops na sua rede, bloqueando certos caminhos. Se o STP estiver configurado incorretamente, ele não impedirá loops como deve ser. Use comandos como`show spanning-tree`para verificar a configuração do STP. Além disso, verifique as TCNs (Topology Change Notifications, Notificações de alteração de topologia) usando o comando`show spanning-tree detail | include ieee|occur|from|is`.
- Verifique se há endereços MAC duplicados: Se dois dispositivos na rede tiverem o mesmo endereço MAC (visto principalmente na configuração de alta disponibilidade (HA) e em várias placas ou controladores de interface de rede (NICs)), isso poderá causar oscilação de MAC. Use o comando`show mac address-table`para procurar endereços MAC duplicados em sua rede.
- Verifique se há falha de hardware ou de cabos: Cabos de rede ou hardware defeituosos podem fazer com que os quadros sejam enviados para as interfaces erradas, levando à oscilação de MAC. Verifique a condição física dos cabos e considere a troca do hardware para ver se o problema persiste. A oscilação de interface também pode causar oscilação de MAC nos switches.
- Verificar bugs de software: Às vezes, a oscilação de MAC pode ser causada por bugs no software dos dispositivos de rede. Verifique a ferramenta de pesquisa de bugs.

Ferramenta de pesquisa de erros: 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

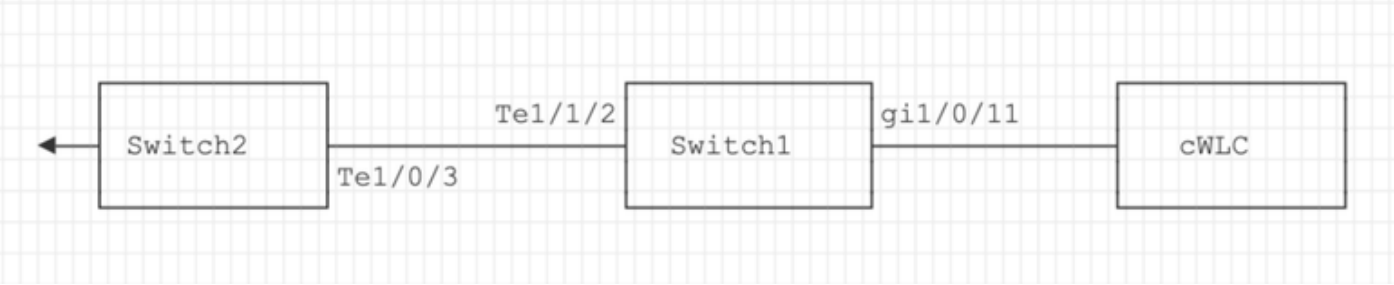
- Entre em contato com o suporte do TAC: Se você tentou tudo e o problema ainda persistir, pode ser o momento de entrar em contato com o suporte do TAC da Cisco. Eles podem oferecer assistência adicional.

Casos Práticos 1

Descrição do problema

O controlador eWLC está enfrentando uma perda de conectividade com o gateway e as quedas de pacotes estão impedindo que os APs se juntem ao controlador.

Topologia



Passos de Troubleshooting

A oscilação de MAC foi identificada no switch (Switch1) conectado ao 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
```

Aprendizagem MAC:

Insira o comando`show mac address-table address`
para verificar o endereço MAC aprendido na porta.

<#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
```

Configuração das Portas Gi1/0/11 e Te1/1/2:

Insira o comando show running-config interface
para verificar a configuração da interface.

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

Vizinhos CDP das Portas Gi1/0/11 e Te1/1/2:

Insira o comando show cdp neighbors
para verificar os detalhes dos 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
```

Aprendizado de MAC no Switch2 (Switch de uplink):

Insira o comando`show mac address-table address`
para verificar o endereço MAC aprendido na porta.

<#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 raiz

Verificou-se que o ID do Virtual Router Redundancy Protocol (VRRP) do Switch 2 e o eWLC eram os mesmos, o que resultou na geração do mesmo MAC virtual pelo VRRP.

Resolução

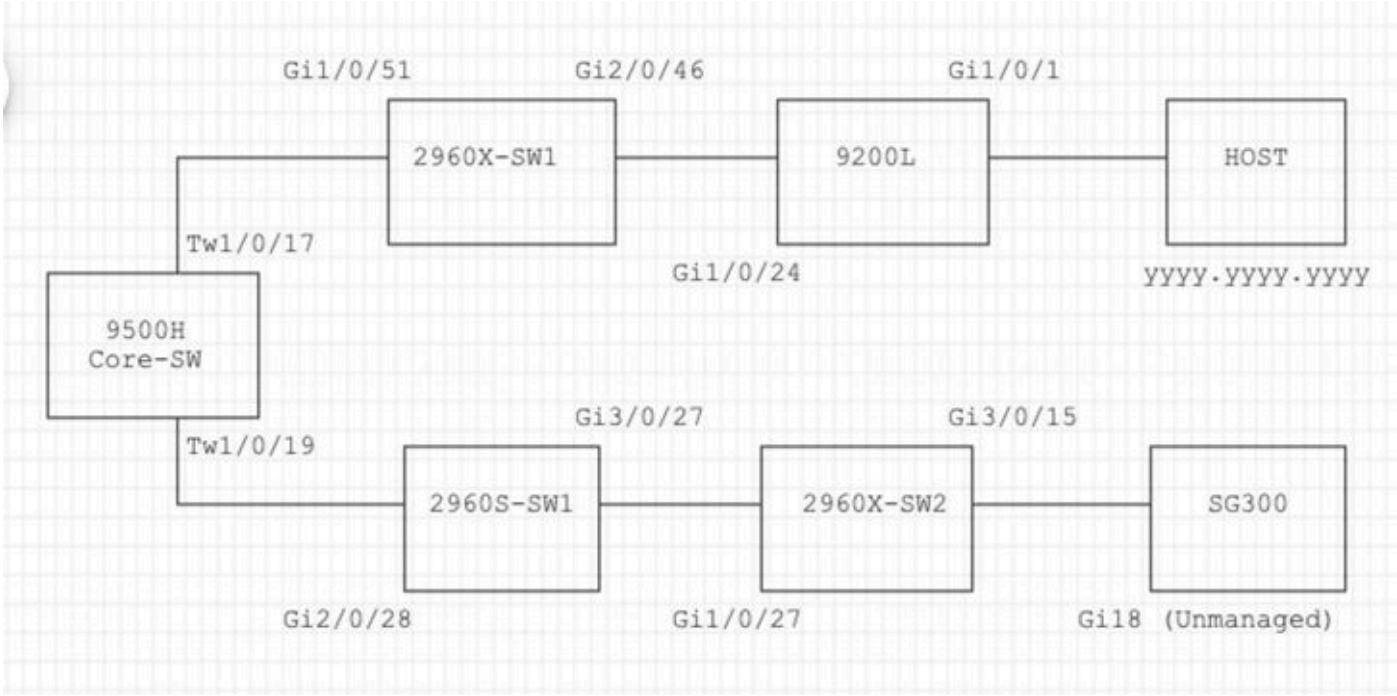
O problema foi resolvido após a alteração da instância de VRRP no WLC, que estava causando uma duplicação de MAC no switch, levando a uma perda de conectividade com o gateway e quedas de pacotes, o que impediu que os APs se unissem ao controlador.

Casos Práticos 2

Descrição do problema

Alguns dos servidores estão inacessíveis ou apresentam latência/quedas significativas.

Topologia



Passos de Troubleshooting

1. Ocorreu uma oscilação de MAC observada no switch central.

```
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. Escolhido o endereço`yyyy.yyyy.yyyy`MAC para o processo de identificação e solução de problemas.

Aprendizagem MAC:

Insira o comando`show mac address-table address`
para verificar o endereço MAC aprendido na porta.

<#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
```

Vizinhos CDP das Portas Twe 1/0/17 e Twe 1/0/19:

Insira o comando`show cdp neighbors`
para verificar os detalhes dos 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
```

Logs do 2960X-SW1 conectados ao Core-SW Twe1/0/17:

O MAC`yyyy.yyyy.yyyy`está oscilando entre a porta Gi1/0/51 e 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 de 9200L:

(Essa parece ser a porta válida para esse endereço 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 ao Core-SW Twe1/0/19:

(Parece ser um caminho de loop.) A porta no Core-SW foi desativada para mitigar o loop.

No entanto, as oscilações de MAC ainda estavam sendo observadas no Core-SW.

Registros do 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 do 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 raiz

As oscilações de MAC foram observadas devido ao switch SG300 (não gerenciado) conectado à rede.

Resolução

O problema de oscilação de MAC foi resolvido com o desligamento da porta conectada ao switch SG300 não gerenciado.

Prevenção

Portfast STP:

O STP PortFast faz com que uma porta LAN de Camada 2 entre imediatamente no estado forwarding, ignorando os estados listening e learning. O STP PortFast impede a geração de STP TCNs, que não são significativos a partir de portas que não recebem STP Bridge Protocol Data Units (BPDUs). Configure o STP PortFast somente em portas conectadas a dispositivos de host final que terminam VLANs e das quais a porta nunca deve receber BPDUs de STP, como

Estações de Trabalho, Servidores, Portas em roteadores que não estejam configurados para suportar bridging.

Protetor de BPDU:

O STP BPDU Guard complementa a funcionalidade do STP PortFast. Em portas ativadas para STP PortFast, o STP BPDU Guard protege os loops de Camada 2 que o STP não pode fornecer quando o STP PortFast está ativado. O STP BPDU Guard desliga as portas que recebem BPDUs.

protetor de raiz:

O protetor de raiz impede que as portas se tornem portas raiz STP. Use o protetor de raiz STP para evitar que portas inadequadas se tornem portas de raiz STP. Um exemplo de uma porta inadequada é uma porta que se conecta a um dispositivo que está fora do controle administrativo direto da rede.

Protetor de loop:

O protetor de loop é uma otimização proprietária da Cisco para o STP. O protetor de loop protege as redes de Camada 2 contra loops que ocorrem quando algo impede o encaminhamento normal de BPDUs em links ponto a ponto (por exemplo, um mau funcionamento da interface de rede ou uma CPU ocupada). O protetor de loop complementa a proteção contra falhas de link unidirecional fornecida pelo Unidirectional Link Detection (UDLD). O protetor de loop isola falhas e permite que o STP convirja para uma topologia estável com o componente com falha excluído da topologia do STP.

Filtro de BPDU:

Isso desabilita o STP. As BPDUs não são enviadas nem processadas após o recebimento. É comum com provedores de serviços, não necessariamente redes corporativas.

UDLD Agressivo:

O protocolo UDLD proprietário da Cisco monitora a configuração física dos links entre dispositivos e portas que suportam UDLD. O UDLD detecta a existência de links unidirecionais. O UDLD pode operar no modo normal ou agressivo. O UDLD de modo normal classifica um link como unidirecional se os pacotes UDLD recebidos não contiverem informações corretas para o dispositivo vizinho. Além da funcionalidade do UDLD de modo normal, o UDLD de modo agressivo coloca as portas no estado desabilitado por erro se a relação entre dois vizinhos sincronizados anteriormente não puder ser restabelecida.

Controle de Tempestade:

O controle de tempestade de tráfego é implementado no hardware e não afeta o desempenho geral do switch. Geralmente, estações finais, como PCs e servidores, são a origem do tráfego de broadcast que pode ser suprimido. Para evitar o processamento desnecessário de excesso de tráfego de broadcast, habilite o controle de tempestade de tráfego para tráfego de broadcast nas portas de acesso que se conectam a estações finais e em portas que se conectam a nós de rede importantes.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.