# Solucionar problemas de erro de notificação de falha de endereço MAC

## Contents



## Notificação de Flap de Endereço MAC

### SeveridadeICS

5 - Aviso

### Impacto

Essas mensagens podem ser investigadas para garantir que um loop de encaminhamento não exista.

### Descrição

Essa mensagem de notificação é gerada pelo switch quando ele detecta um evento de oscilação de endereço MAC na rede. Um evento de oscilação de endereço MAC é detectado quando um switch recebe pacotes do mesmo endereço MAC de origem em duas interfaces diferentes. Os switches Cisco Catalyst notificam quando o mesmo endereço MAC é detectado em várias portas de switch, fazendo com que o switch altere constantemente a porta associada ao endereço MAC e emita alertas através desse syslog que contém o endereço MAC do host, VLAN e portas entre as quais o endereço MAC está oscilando. Como esse comportamento pode ser causado por vários motivos, identificar a causa subjacente da oscilação de endereços MAC é importante para garantir a estabilidade e o desempenho da rede.

### MensagemSyslog

```
SW_MATM-4-MACFLAP_NOTIF
```

## Exemplo deMensagem

```
Apr 26 12:27:55 <> %SW_MATM-4-MACFLAP_NOTIF: Host mac address in vlan X is flapping between port PoX an
```

## Famíliade produtos

- Switches 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
- Cisco Catalyst 6000 Series Switches
- Switches Cisco Catalyst 6800 Series
- Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 4900 Series Switches
- Switches Cisco Catalyst 3750-X Series
- Switches Cisco Catalyst 3850-X Series
- Cisco Catalyst 2960 Series Switches

## Regex

N/A

## Recomendação

Há muitas causas possíveis para esse erro, algumas das quais podem indicar um problema sério de rede. Os 3 mais comuns são explicados em detalhes abaixo:

1. Movimento do cliente sem fio (sem impacto na rede).

2. Movimentação de endereços virtuais de sistemas redundantes ou máquinas virtuais duplicadas (impacto moderado na rede).

3. Loops de Camada 2 (alto impacto na rede)

Detalhes do #1: o movimento do cliente sem fio é geralmente esperado e pode ser ignorado com segurança, supondo que não haja impactos no serviço observados. Os clientes em roaming entre APs que não estão usando CAPWAP de volta para um controlador sem fio, ou em roaming entre APs controlados por dois controladores sem fio diferentes, provavelmente gerarão esse registro. O tempo entre os logs gerados para o mesmo endereço MAC pode estar a vários segundos ou minutos de distância. Se você vir que um único endereço mac está se movendo várias vezes por

segundo, isso pode indicar um problema mais sério e pode ser necessária uma solução de problemas adicional.

Detalhes do #2: alguns sistemas ou dispositivos redundantes que operam em um estado ativo/standby podem compartilhar um endereço IP e mac virtual comum, com apenas o dispositivo ativo usando-o em qualquer momento. Se ambos os dispositivos se tornarem inesperadamente ativos e começarem a usar o endereço virtual, esse erro poderá ser visto. Usando uma combinação das interfaces mencionadas no registro e o comando show mac address-table address vlan rastrear o caminho desse mac através da rede para determinar onde e quais dispositivos estão gerando tráfego do mac compartilhado. Dependendo da natureza dos dispositivos que geram as movimentações, pode ser necessária a solução de problemas adicionais de seus estados de redundância. Detalhes do #3: os loops L2 geralmente geram um grande número de erros de movimentação mac em um período de tempo muito curto (pelo menos um por segundo, muitas vezes mais). Os registros geralmente podem ser para um único endereço MAC ou para um pequeno número de endereços MAC, e os usuários podem experimentar um impacto na rede. O roteamento e os protocolos da camada 2 podem falhar frequentemente, resultando em registros adicionais e instabilidade geral sendo criados. Para solucionar problemas de um loop L2, execute o comando show int | in é up|taxa de entrada e observe todas as interfaces ativas que mostram um volume extremamente alto de pacotes de entrada por segundo (em geral, esse pode ser um número muito grande de 6, 7 ou 8+ dígitos, dependendo da velocidade da interface). É provável que haja apenas 1 ou 2 interfaces com uma taxa de entrada anormalmente alta. Não se concentre nas taxas de saída e não se concentre nos TCNs de spanning-tree. Depois que a interface de entrada alta for identificada, use CDP, LLDP ou suas descrições de interface/diagrama de rede para fazer login no dispositivo vizinho conectado a essa porta e execute o comando show int | in is up|input rate novamente e repita o processo de rastrear as interfaces com taxas de entrada anormais. Controle as interfaces e os nomes de host à medida que você os rastreia pela rede. Continue verificando os vizinhos e observando as taxas de entrada até que você fique sem portas de entrada e fique sem vizinhos ou termine no dispositivo que você já verificou. Um dos dois possíveis resultados pode acontecer durante essa metodologia: se você acabar com uma porta que não tem CDP, LLDP ou vizinho conhecido, mas tem uma taxa de entrada muito alta, desligue-a administrativamente. Essa interface é provavelmente a origem final ou contribui para o loop. Aguarde 60 segundos para que a rede se estabilize e, se uma condição de loop ainda for vista, mantenha a interface desligada e inicie o processo novamente, já que é possível que haja uma segunda origem na rede. Se você terminar em um dispositivo que você já verificou, isso indica que o protocolo de prevenção de loop em uso (Spanning-Tree é o mais comum) falhou em algum lugar. Para redes spanning-tree, identifique qual switch no caminho que você rastreou deve ser raiz e trabalhe de volta a partir desse dispositivo para determinar qual interface pode estar em um estado de bloqueio dentro do seu caminho rastreado. Quando a interface que pode estar bloqueando (mas está no estado forwarding) for encontrada, desligue-a administrativamente. Aguarde 60 segundos e verifique a estabilidade da rede. Se o loop persistir, mantenha a interface desligada e repita esse processo.

## Comandos

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

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.