Troubleshooting de MAC Address Flap Notification Error

Contenido

Notificación de inestabilidad de dirección MAC

ICSeverity

5 - Aviso

Impacto

Estos mensajes se pueden investigar para asegurarse de que no exista un loop de reenvío.

Descripción

Este mensaje de notificación es generado por el switch cuando detecta un evento de inestabilidad de dirección MAC en la red. Se detecta un evento de inestabilidad de dirección MAC cuando un switch recibe paquetes de la misma dirección MAC de origen en dos interfaces diferentes. Los switches Cisco Catalyst notifican cuando se detecta la misma dirección MAC en varios puertos de switch, lo que hace que el switch cambie constantemente el puerto asociado con la dirección MAC, y alerta a través de este syslog que contiene la dirección MAC del host, la VLAN y los puertos entre los que la dirección MAC es inestable. Dado que este comportamiento puede deberse a varias razones, es importante identificar la causa subyacente de la inestabilidad de la dirección MAC para garantizar la estabilidad y el rendimiento de la red.

MensajeSyslog

```
SW_MATM-4-MACFLAP_NOTIF
```

EjemploMensaje

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

FamiliaDeProductos

- Switches Cisco Catalyst serie 9300
- Switches Cisco Catalyst serie 9400
- Switches Cisco Catalyst serie 9200
- Switches Cisco Catalyst serie 9500
- Switches Cisco Catalyst serie 9600
- Switches Cisco Catalyst serie 3850
- Switches Cisco Catalyst serie 3650
- Cisco Catalyst 6000 Series Switches
- Switches Cisco Catalyst serie 6800
- Cisco Catalyst 4500 Series Switches
- Cisco Catalyst 4900 Series Switches
- Switches Cisco Catalyst serie 3750-X
- Switches Cisco Catalyst serie 3850-X
- Cisco Catalyst 2960 Series Switches

Regex

N/A

Recomendación

Existen muchas causas posibles para este error, algunas de las cuales pueden indicar un problema grave de la red. Los 3 más comunes se explican en detalle a continuación:

1. Movimiento del cliente inalámbrico (sin impacto en la red).

2. Movimiento de direcciones virtuales desde sistemas redundantes o máquinas virtuales duplicadas (impacto moderado en la red).

3. Bucles de capa 2 (gran impacto en la red)

#1 Details: A menudo se espera el movimiento del cliente inalámbrico, y por lo general se puede ignorar de forma segura si no se observan impactos en el servicio. Los clientes que se desplazan entre los AP que no están utilizando CAPWAP de nuevo a un controlador inalámbrico, o que se desplazan entre los AP controlados por dos controladores inalámbricos diferentes, es probable que generen este registro. El tiempo entre los registros generados para la misma dirección MAC puede ser de varios segundos o varios minutos de diferencia. Si ve que una sola dirección MAC

se mueve varias veces por segundo, eso puede indicar un problema más serio y puede ser necesario un troubleshooting adicional.

#2 Details: Algunos sistemas o dispositivos redundantes que funcionan en un estado activo/en espera pueden compartir una dirección MAC e IP virtual común, y solo el dispositivo activo puede usarla en cualquier momento. Si ambos dispositivos se activan inesperadamente y comienzan a usar la dirección virtual, se puede ver este error. Usando una combinación de las interfaces mencionadas en el registro y el comando show mac address-table address vlan traza la trayectoria de este mac a través de la red para determinar dónde y qué dispositivos están generando tráfico desde el mac compartido. Dependiendo de la naturaleza de los dispositivos que generan los movimientos, puede ser necesario un troubleshooting adicional de sus estados de redundancia. #3 Details: Los loops L2 a menudo generan una gran cantidad de errores de movimiento de mac en un período de tiempo muy corto (al menos uno por segundo, a menudo más). Los registros pueden ser normalmente para una sola o un pequeño número de direcciones MAC, y los usuarios pueden experimentar un impacto en la red. Los protocolos de routing y capa 2 a menudo pueden fallar, lo que puede dar lugar a la creación de registros adicionales e inestabilidad general. Para resolver problemas de un loop L2, ejecute el comando show int | in es up|input rate y observe todas las interfaces activas que muestran un volumen extremadamente alto de paquetes de entrada por segundo (generalmente hablando, este puede ser un número muy grande de 6, 7 u 8+ dígitos dependiendo de la velocidad de la interfaz). Es probable que sólo haya 1 o 2 interfaces con una velocidad de entrada anormalmente alta. No se centre en las tasas de producción y no se centre en las TCN de árbol de extensión. Una vez identificada la interfaz de entrada alta, utilice CDP, LLDP o su diagrama de red/descripciones de interfaz para iniciar sesión en el dispositivo vecino conectado a ese puerto, y ejecute el comando show int | in es up|input rate y repita el proceso de seguimiento de las interfaces con velocidades de entrada anormales. Realice un seguimiento de las interfaces y los nombres de host a medida que los rastrea a través de la red. Continúe comprobando los vecinos y observando las velocidades de entrada hasta que se quede sin puertos de entrada y se quede sin vecinos o termine de nuevo en el dispositivo que ya ha comprobado. Uno de los dos posibles resultados puede ocurrir durante esta metodología: Si termina con un puerto que no tiene CDP, LLDP o vecino conocido, pero una velocidad de entrada muy alta, administrativamente apáguelo. Esta interfaz es probablemente el origen final, o es un contribuidor del loop. Espere 60 segundos para que la red se estabilice y, si se sigue viendo una condición de loop, mantenga la interfaz apagada e inicie el proceso de nuevo, ya que es posible que haya una segunda fuente en la red. Si termina en un dispositivo que ya ha verificado, esto indica que el protocolo de prevención de loops en uso (el árbol de expansión es el más común) ha fallado en algún lugar. Para las redes de árbol de expansión, identifique qué switch de la trayectoria que rastreó se espera que sea raíz y trabaje hacia atrás desde ese dispositivo para determinar qué interfaz puede estar en un estado de bloqueo dentro de su trayectoria rastreada. Una vez que se encuentre la interfaz que puede estar bloqueando (pero que está en estado de reenvío), ciérrela administrativamente. Espere 60 segundos y compruebe la estabilidad de la red. Si el loop persiste, mantenga la interfaz apagada y repita este proceso.

Comandos

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

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).