# Dépanner une erreur de notification de battement d'adresse MAC

## Table des matières



## Notification d'affollement d'adresse MAC

### Gravité ICS

5 - Avis

### Incidence

Ces messages peuvent être examinés pour s'assurer qu'il n'existe pas de boucle de transfert.

### Description

Ce message de notification est généré par le commutateur lorsqu'il détecte un événement de battement d'adresse MAC sur le réseau. Un événement de battement d'adresse MAC est détecté lorsqu'un commutateur reçoit des paquets de la même adresse MAC source dans deux interfaces différentes. Les commutateurs Cisco Catalyst signalent la détection d'une même adresse MAC sur plusieurs ports de commutation, ce qui entraîne la modification constante du port associé à l'adresse MAC et l'envoi d'alertes via ce syslog qui contient l'adresse MAC de l'hôte, du VLAN et des ports entre lesquels l'adresse MAC est instable. Étant donné que ce comportement peut être dû à plusieurs raisons, il est important d'identifier la cause sous-jacente du battement des adresses MAC pour garantir la stabilité et les performances du réseau.

### MessageSyslog

```
SW_MATM-4-MACFLAP_NOTIF
```

## MessageÉchantillon

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

## Gamme de produits

- Commutateurs de la gamme Cisco Catalyst 9300
- Commutateurs de la gamme Cisco Catalyst 9400
- Commutateurs de la gamme Cisco Catalyst 9200
- Commutateurs de la gamme Cisco Catalyst 9500
- Commutateurs de la gamme Cisco Catalyst 9600
- Commutateurs de la gamme Cisco Catalyst 3850
- Commutateurs de la gamme Cisco Catalyst 3650
- Commutateurs de la gamme Cisco Catalyst 6000
- Commutateurs de la gamme Cisco Catalyst 6800
- Commutateurs de la gamme Cisco Catalyst 4500
- Commutateurs de la gamme Cisco Catalyst 4900
- Commutateurs Cisco Catalyst, série 3750-X
- Commutateurs Cisco Catalyst, série 3850-X
- Commutateurs Cisco Catalyst, série 2960

## Regex

S/O

## Recommandation

Il existe de nombreuses causes possibles à cette erreur, dont certaines peuvent indiquer un problème de réseau grave. Les 3 plus courantes sont expliquées en détail ci-dessous :

1. Déplacement du client sans fil (aucun impact sur le réseau).

2. Déplacement des adresses virtuelles à partir de systèmes redondants ou de machines virtuelles dupliquées (impact modéré sur le réseau).

3. Boucles de couche 2 (impact élevé sur le réseau)

#1 Détails : Le déplacement du client sans fil est souvent prévu et peut généralement être ignoré en toute sécurité, en supposant qu'aucun impact sur le service n'ait été observé. Les clients qui se déplacent entre des points d'accès qui n'utilisent pas CAPWAP vers un contrôleur sans fil, ou qui se déplacent entre des points d'accès contrôlés par deux contrôleurs sans fil différents, sont susceptibles de générer ce journal. L'intervalle entre les journaux générés pour la même adresse MAC peut être de quelques secondes ou de quelques minutes. Si vous voyez qu'une seule

adresse MAC se déplace plusieurs fois par seconde, cela peut indiquer un problème plus grave et un dépannage supplémentaire peut être nécessaire.

#2 Détails : Certains systèmes ou périphériques redondants fonctionnant dans un état actif/veille peuvent partager une adresse IP et MAC virtuelle commune, seul le périphérique actif l'utilisant à un moment donné. Si les deux périphériques deviennent inopinément actifs et commencent tous deux à utiliser l'adresse virtuelle, cette erreur est visible. À l'aide d'une combinaison des interfaces mentionnées dans le journal et de la commande show mac address-table address vlan, tracez le chemin de ce mac à travers le réseau pour déterminer où et quels périphériques génèrent du trafic à partir du mac partagé. En fonction de la nature des périphériques générant les déplacements, un dépannage supplémentaire de leurs états de redondance peut être nécessaire. #3 Détails : Les boucles L2 génèrent souvent un grand nombre d'erreurs de déplacement MAC dans un laps de temps très court (au moins une par seconde, souvent plus). Les journaux peuvent en général concerner une seule adresse MAC ou un petit nombre d'adresses MAC, et les utilisateurs peuvent ressentir un impact sur le réseau. Les protocoles de routage et de couche 2 peuvent souvent échouer, ce qui entraîne la création de journaux supplémentaires et une instabilité générale. Pour dépanner une boucle L2, exécutez la commande show int | in is up|input rate et notez toutes les interfaces actives qui affichent un volume extrêmement élevé de paquets d'entrée par seconde (en général, il peut s'agir d'un très grand nombre de 6, 7 ou 8 chiffres en fonction de la vitesse de l'interface). Il est probable qu'il y ait seulement 1 ou 2 interfaces avec un débit d'entrée anormalement élevé. Ne vous concentrez pas sur les débits de sortie et ne vous concentrez pas sur les TCN Spanning Tree. Une fois que l'interface d'entrée haute est identifiée, utilisez CDP, LLDP ou vos descriptions d'interface/schéma de réseau pour vous connecter au périphérique voisin connecté à ce port, et exécutez la commande show int | dans la commande is up|input rate et répétez le processus de suivi des interfaces avec des débits d'entrée anormaux. Suivez les interfaces et les noms d’hôte pendant que vous les suivez sur le réseau. Continuez à vérifier les voisins et à examiner les débits d'entrée jusqu'à ce que vous soyez à court de ports d'entrée et que vous soyez à court de voisins ou retourniez sur le périphérique que vous avez déjà vérifié. L'un des deux résultats possibles peut se produire au cours de cette méthodologie : si vous vous retrouvez avec un port qui n'a pas de CDP, LLDP ou voisin connu, mais un taux d'entrée très élevé, arrêtez-le administrativement. Cette interface est probablement la source ultime ou contribue à la boucle. Attendez 60 secondes que le réseau se stabilise. Si une condition de boucle est toujours présente, arrêtez l’interface et recommencez le processus, car il est possible qu’il y ait une deuxième source sur le réseau. Si vous vous retrouvez sur un périphérique que vous avez déjà vérifié, cela indique que le protocole de prévention des boucles utilisé (Spanning Tree étant le plus courant) a échoué quelque part. Pour les réseaux Spanning Tree, identifiez quel commutateur du chemin que vous avez suivi est censé être racine et remontez à partir de ce périphérique pour déterminer quelle interface peut être dans un état de blocage dans votre chemin suivi. Une fois que l'interface qui peut être bloquante (mais qui est en état de transmission) est trouvée, arrêtez-la administrativement. Patientez 60 secondes et vérifiez la stabilité du réseau. Si la boucle persiste, maintenez l’interface hors tension et répétez ce processus.

## Commandes

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.