Dépanner une erreur de notification de battement d'adresse MAC

Table des matières

Introduction

Informations générales

- Description
- MessageSyslog
- MessageÉchantillon

Notification d'affollement d'adresse MAC

- Incidence
- Gamme de produits

Recommandation

- Détails du scénario 1
- Détails du scénario 2
- Détails du scénario 3
- Détails du scénario 4

Commandes

Introduction

Ce document décrit comment dépanner les erreurs de notification de battement d'adresse MAC.

Informations générales

Description

Ce message de notification est généré par le commutateur lorsqu'il détecte un événement de battement d'adresse MAC sur le réseau.

Un évènement de battement d'adresse MAC est détecté lorsqu'un commutateur apprend que la même source d'adresse MAC et le même VLAN se trouvent sur deux interfaces différentes dans un court intervalle.

Les commutateurs Cisco Catalyst signalent la détection d'une même adresse MAC sur plusieurs

ports de commutation, ce qui entraîne une modification constante du port associé à l'adresse MAC. Cette alerte via ce syslog contient l'adresse MAC de l'hôte, du VLAN et des ports entre l'adresse MAC qui 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

Example: Apr 26 12:27:55 Switch-1 %SW_MATM-4-MACFLAP_NOTIF: Host **0011.2233.4455** in vlan **10** is flapping between port **Gi1/0/10

Notification d'affollement d'adresse MAC

Incidence

Étudiez ces messages pour déterminer si le déplacement de l'adresse MAC est provoqué par un comportement d'itinérance attendu, un déplacement MAC système redondant, une incohérence EtherChannel ou une boucle de transfert de couche 2.

Gamme de produits

- Commutateurs Cisco Catalyst, série 9300
- Commutateurs Cisco Catalyst, série 9400
- Commutateurs Cisco Catalyst, série 9200
- Commutateurs Cisco Catalyst, série 9500
- Commutateurs Cisco Catalyst, série 9600
- Commutateurs Cisco Catalyst, série 3850
- Commutateurs Cisco Catalyst, série 3650
- Commutateurs Cisco Catalyst, série 6000

- Commutateurs Cisco Catalyst, série 6800
- Commutateurs Cisco Catalyst, série 4500
- Commutateurs Cisco Catalyst, série 4900
- Commutateurs Cisco Catalyst, série 3750
- Commutateurs Cisco Catalyst, série 3850
- Commutateurs Cisco Catalyst, série 2960

Recommandation

Il existe de nombreuses causes possibles à cette erreur, certaines pouvant indiquer un problème réseau grave.

Causes courantes :

- Boucles de couche 2 (impact élevé sur le réseau)
- Déplacement du client sans fil (sans impact sur le réseau)
- Mauvaise configuration d'EtherChannel ou de port-channel (impact modéré sur le réseau)
- Déplacement des adresses MAC virtuelles à partir de systèmes redondants ou de machines virtuelles dupliquées (impact modéré sur le réseau)

Détails du scénario 1

Le déplacement du client sans fil est souvent prévu et peut généralement être ignoré en toute sécurité si aucun impact sur le service n'est 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 une seule adresse MAC se déplace plusieurs fois par seconde, cela peut indiquer un problème plus grave et un dépannage supplémentaire peut être nécessaire.

Détails du scénario 2

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 des interfaces mentionnées dans le journal et en exécutant la commande show mac address-table address <mac-address> vlan

<vlan-id>, tracez le chemin de cette adresse MAC à travers le réseau pour déterminer où l’adresse MAC est actuellement apprise et quels périphériques génèrent du trafic à partir de l’adresse MAC partagée. Notez l'adresse MAC, le VLAN et les interfaces indiqués dans le message syslog, puis exécutez la commande sur chaque commutateur du chemin. Utilisez les protocoles CDP, LLDP, les descriptions d’interface ou le schéma de réseau pour identifier le périphérique connecté suivant et continuer à suivre l’adresse MAC jusqu’à ce que les périphériques sources soient identifiés. En fonction des périphériques générant les déplacements d'adresses MAC, un dépannage supplémentaire de leur état de redondance peut être nécessaire.

Détails du scénario 3

Une erreur de configuration EtherChannel ou Port-Channel est souvent à l'origine des notifications de battement d'adresse MAC. Si le commutateur signale une adresse MAC se déplaçant à plusieurs reprises entre des liaisons physiques qui sont censées être membres d'un EtherChannel, cela indique fortement que l'EtherChannel n'a pas été correctement établi ou n'est pas formé de manière cohérente aux deux extrémités. Dans cette situation, un périphérique peut traiter les interfaces comme des liaisons physiques indépendantes, tandis que le périphérique situé à l'autre extrémité transfère le trafic sur ces interfaces comme un seul ensemble logique.

Par exemple, cela peut se produire si un commutateur est configuré pour utiliser LACP alors que l'homologue est configuré pour le mode EtherChannel statique, ou si la négociation LACP échoue pour une autre raison. Sur les commutateurs Cisco IOS ou Cisco IOS XE Catalyst, lorsque la négociation LACP échoue, les interfaces ne forment pas de canal de port. En fonction de la plate-forme, de la version du logiciel et de la configuration, les interfaces dégroupées peuvent rester opérationnelles en tant qu'interfaces individuelles ou être suspendues. Si plusieurs liaisons indépendantes restent en cours de transmission, le commutateur peut réapprendre en permanence la même adresse MAC source sur différents ports et générer des notifications de battement MAC.

Les événements de battement MAC peuvent également se produire en cas d'incohérence dans la configuration EtherChannel entre les deux extrémités de la connexion. La même adresse MAC peut sembler se déplacer entre une interface physique et l'interface port-canal logique, ou entre des liaisons qui sont censées être regroupées mais pas configurées de manière cohérente. Lors du dépannage de cette condition, vérifiez que les deux périphériques ont des paramètres EtherChannel correspondants, y compris le mode de regroupement, tel que LACP, PAgP ou le mode statique. Les liaisons membres correspondantes affectées au port-channel, les paramètres de couche 2 cohérents tels que le mode trunk ou d'accès, l'appartenance au VLAN, le VLAN natif et les listes de VLAN autorisés. S'assurer que l'EtherChannel est correctement négocié et que les deux extrémités ont des configurations EtherChannel et de couche 2 correspondantes peut éliminer ces événements de battement d'adresse MAC lorsque l'incohérence EtherChannel est la cause première.

Détails du scénario 4

Les boucles de couche 2 génèrent souvent des messages de déplacement d’adresse MAC répétés sur une courte période, généralement avec des débits de paquets d’entrée élevés, une instabilité de protocole et un impact sur le trafic utilisateur. Les journaux peuvent généralement concerner un seul ou un petit nombre d’adresses MAC, et les utilisateurs peuvent subir 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 interface | include 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 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. Utilisez **taux de paquets en entrée** comme point de données principal lors du suivi du chemin de boucle. Utilisez les modifications de topologie Spanning Tree (TCN), l’état du pont racine, les ports bloqués et les ports incohérents comme données de prise en charge lors de la validation. Une fois que l'interface d'entrée haute est identifiée, utilisez CDP, LLDP ou vos descriptions d'interface/diagrammes de réseau pour vous connecter au périphérique voisin connecté à ce port, et exécutez la commande show interface | include 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 observez 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 un port n'a pas de CDP, LLDP ou voisin connu et a un taux d'entrée très élevé, confirmez l'impact opérationnel, enregistrez l'état actuel de l'interface et obtenez l'autorisation avant d'arrêter administrativement l'interface. Après l'arrêt, patientez 60 secondes et vérifiez si les battements MAC, les débits d'entrée élevés et l'impact sur l'utilisateur s'arrêtent. Si le problème disparaît, conservez l’interface isolée jusqu’à ce que le périphérique ou le câblage connecté soit identifié. Si un problème de boucle est toujours détecté, maintenez l’interface hors tension et recommencez le processus, car il est possible qu’il y ait une seconde source sur le réseau.
- Si la trace retourne à un périphérique déjà vérifié, le chemin contient une boucle de couche 2. Validez l'état STP, le filtre BPDU, les événements de protection BPDU, la cohérence EtherChannel, les listes de VLAN trunk, les VLAN natifs, les commutateurs non gérés et le

câblage pour identifier les emplacements où la prévention des boucles ne fonctionne pas comme prévu. 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 du chemin suivi est censée bloquer, mais est en cours de transfert. Une fois que l'interface qui peut être bloquante (mais qui est à l'état de transmission) est trouvée, arrêtez-la administrativement. Patientez 60 secondes et vérifiez la stabilité du réseau. Si la boucle persiste, arrêtez l'interface et répétez ce processus.

Commandes

La syntaxe des commandes varie selon la plate-forme et la version du logiciel. Sur Cisco IOS XE, exécutez la commande show mac address-table. Certaines plates-formes héritées exécutent la syntaxe show mac-address-table.

Commande	Objectif
show version	Identifiez la plate-forme, la version du logiciel et la disponibilité.
show logging	Examiner les messages d'instabilité MAC et les événements de protocole associés.
show spanning-tree	Vérifiez le pont racine, les rôles de port, les états de port et les modifications de topologie.
show mac address-table address <adresse-mac> vlan <id-vlan>	Identifiez l'emplacement où l'adresse MAC est actuellement apprise.
show interfaces	L'inclusion est activée.
show etherchannel summary	Vérifiez l'état du port-channel et la cohérence des membres.
show cdp neighbors detail / show lldp neighbors detail	Identifiez le périphérique voisin connecté à une interface.

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.