Fehlerbehebung: Benachrichtigungsfehler bei MAC-Adressklappe

Inhalt

Benachrichtigung zu MAC-Adressmarkierung

ICSeverity

5 - Benachrichtigung

Auswirkungen

Diese Nachrichten können überprüft werden, um sicherzustellen, dass keine Weiterleitungsschleife vorhanden ist.

Beschreibung

Diese Benachrichtigungsmeldung wird vom Switch generiert, wenn ein Flapping-Ereignis bei einer MAC-Adresse im Netzwerk erkannt wird. Ein Flapping der MAC-Adresse wird erkannt, wenn ein Switch Pakete von derselben Quell-MAC-Adresse an zwei verschiedene Schnittstellen empfängt. Cisco Catalyst Switches benachrichtigen, wenn dieselbe MAC-Adresse an mehreren Switch-Ports erkannt wird, was dazu führt, dass der Switch den mit der MAC-Adresse verknüpften Port ständig ändert, und geben über dieses Syslog eine Warnung aus, das die MAC-Adresse des Hosts, des VLAN und der Ports enthält, zwischen denen die MAC-Adresse flattert. Da dieses Verhalten aus mehreren Gründen verursacht werden kann, ist die Identifizierung der zugrunde liegenden Ursache von Flapping-Ereignissen bei MAC-Adressen wichtig, um die Stabilität und Leistung des Netzwerks sicherzustellen.

SyslogMeldung

```
SW_MATM-4-MACFLAP_NOTIF
```

MessageSample

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

Produktfamilie

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

Regex

_

Empfehlung

Es gibt viele mögliche Ursachen für diesen Fehler, von denen einige auf ein ernstes Netzwerkproblem hinweisen können. Die drei häufigsten Nebenwirkungen werden im Folgenden ausführlich erläutert:

1. Wireless-Client-Bewegung (ohne Auswirkungen auf das Netzwerk).

2. Verschiebung virtueller Adressen aus redundanten Systemen oder duplizierten virtuellen Systemen (moderate Auswirkungen auf das Netzwerk).

3. Layer-2-Schleifen (hohe Auswirkungen auf das Netzwerk)

#1 Details: Eine Bewegung von Wireless-Clients wird häufig erwartet und kann in der Regel ignoriert werden, wenn keine Auswirkungen auf den Service beobachtet werden. Clients, die zwischen APs ohne CAPWAP zu einem Wireless-Controller wechseln oder zwischen APs

wechseln, die von zwei verschiedenen Wireless-Controllern gesteuert werden, erstellen dieses Protokoll wahrscheinlich. Die Zeit zwischen den Protokollen, die für dieselbe MAC-Adresse generiert werden, kann mehrere Sekunden oder Minuten voneinander entfernt sein. Wenn Sie feststellen, dass sich eine MAC-Adresse mehrmals pro Sekunde bewegt, kann dies auf ein ernsteres Problem hinweisen, für das ggf. eine zusätzliche Fehlerbehebung erforderlich ist.

#2 Details: Einige redundante Systeme oder Geräte, die im aktiven/Standby-Status betrieben werden, können eine gemeinsame virtuelle IP- und MAC-Adresse verwenden, wobei diese zu jedem Zeitpunkt nur vom aktiven Gerät verwendet wird. Wenn beide Geräte unerwartet aktiv werden und beide die virtuelle Adresse verwenden, ist dieser Fehler zu sehen. Mithilfe einer Kombination der im Protokoll genannten Schnittstellen und des Befehls show mac address-table address vlan wird der Pfad dieser MAC-Adresse durch das Netzwerk verfolgt, um festzustellen, wo und welche Geräte Datenverkehr von der freigegebenen MAC-Adresse generieren. Je nach Art der Geräte, die die Verschiebungen verursachen, kann eine zusätzliche Fehlerbehebung für deren Redundanzstatus erforderlich sein. #3 Details: L2-Schleifen erzeugen oft eine große Anzahl von MAC-Verschiebungsfehlern in sehr kurzer Zeit (mindestens eine pro Sekunde, oft mehr). Protokolle können in der Regel für eine einzelne oder eine kleine Anzahl von MAC-Adressen erstellt werden, und die Benutzer können Auswirkungen auf das Netzwerk haben. Routing und Layer-2-Protokolle können häufig fehlschlagen, was zu zusätzlichen Protokollen und allgemeiner Instabilität führen kann. Führen Sie den Befehl show int aus, um eine L2-Schleife zu behandeln. | in ist up|input rate und beachten Sie alle aktiven Schnittstellen, die ein extrem hohes Volumen an Eingangspaketen pro Sekunde zeigen (im Allgemeinen kann dies eine sehr große 6, 7 oder 8+ Ziffern sein, abhängig von der Geschwindigkeit der Schnittstelle). Wahrscheinlich gibt es nur 1 oder 2 Schnittstellen mit einer ungewöhnlich hohen Eingangsrate. Konzentrieren Sie sich nicht auf die Ausgaberaten und nicht auf Spanning-Tree-TCNs. Sobald die Schnittstelle für hohe Eingaben identifiziert wurde, melden Sie sich mit CDP, LLDP oder den Schnittstellenbeschreibungen/dem Netzwerkdiagramm bei dem benachbarten Gerät an, das mit diesem Port verbunden ist, und führen Sie show int aus. | in is up|input rate command again und wiederholen Sie den Vorgang der Rückverfolgung der Schnittstellen mit ungewöhnlichen Eingaberaten. Behalten Sie die Schnittstellen und Hostnamen im Auge, während Sie sie durch das Netzwerk verfolgen. Überprüfen Sie weiterhin die Nachbarn, und prüfen Sie die Eingangsraten, bis die Eingangsports zur Neige gehen und Sie keine Nachbarn mehr haben oder wieder auf dem bereits geprüften Gerät landen. Eines von zwei möglichen Ergebnissen kann während dieser Methode passieren: Wenn Sie am Ende einen Port haben, der kein CDP, LLDP oder einen bekannten Nachbarn, aber eine sehr hohe Eingangsrate hat, fahren Sie ihn administrativ herunter. Diese Schnittstelle ist wahrscheinlich die ultimative Quelle oder ein Beitrag zum Loop. Warten Sie 60 Sekunden, bis sich das Netzwerk stabilisiert hat. Wenn noch eine Schleifenbedingung auftritt, fahren Sie die Schnittstelle herunter und starten den Vorgang erneut, da es möglich ist, dass eine zweite Quelle im Netzwerk vorhanden ist. Wenn Sie auf einem Gerät landen, das Sie bereits überprüft haben, weist dies darauf hin, dass das verwendete Protokoll zur Vermeidung von Schleifen (Spanning-Tree ist das gängigste) irgendwo fehlgeschlagen ist. Bei Spanning-Tree-Netzwerken müssen Sie bestimmen, welcher Switch im Pfad, den Sie verfolgt haben, als Root-Switch erwartet wird, und von diesem Gerät aus rückwärts arbeiten, um zu bestimmen, welche Schnittstelle im Pfad, für den Sie nachverfolgt haben, blockiert werden kann. Beenden Sie die blockierende Schnittstelle administrativ, sobald diese gefunden wurde (sich aber im Weiterleitungsstatus befindet). Warten Sie 60 Sekunden, und überprüfen Sie die Netzwerkstabilität. Wenn die Schleife nicht unterbrochen

wird, fahren Sie die Schnittstelle herunter, und wiederholen Sie den Vorgang.

Befehle

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.