Fout bij melding van MAC-adresflap bij probleemoplossing

Inhoud

Melding van MAC-adresflap

- ICeverity
- Impact
- Beschrijving
- SyslogMessage
- Berichtvoorbeeld
- Productfamilie
- Regex
- Aanbeveling
- Opdrachten

Melding van MAC-adresflap

ICeverity

5 - Opmerking

Impact

Deze berichten kunnen worden onderzocht om ervoor te zorgen dat een het door:sturen lijn niet bestaat.

Beschrijving

Dit melding wordt gegenereerd door de switch wanneer deze een MAC-adresflapping op het netwerk detecteert. Een MAC-adresflapper wordt gedetecteerd wanneer een switch pakketten van hetzelfde Source MAC-adres in twee verschillende interfaces ontvangt. Cisco Catalyst switches melden wanneer hetzelfde MAC-adres wordt gedetecteerd op meerdere switch-poorten, waardoor de switch voortdurend de poort wijzigt die aan het MAC-adres is gekoppeld, en waarschuwen via deze syslog die het MAC-adres bevat van de host, VLAN en poorten waartussen het MAC-adres knippert. Gezien het feit dat dit gedrag kan worden veroorzaakt door meerdere redenen, is het identificeren van de onderliggende oorzaak van MAC-adresflapping belangrijk om de stabiliteit en prestaties van het netwerk te verzekeren.

SyslogMessage

```
SW_MATM-4-MACFLAP_NOTIF
```

Berichtvoorbeeld

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

Productfamilie

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

Regex

N.v.t.

Aanbeveling

Er zijn vele mogelijke oorzaken voor deze fout, waarvan sommige op een ernstig netwerkprobleem kunnen wijzen. De 3 meest voorkomende bijwerkingen worden hieronder in detail beschreven:

1. Draadloze clientverplaatsing (zonder gevolgen voor het netwerk).

2. Virtuele adresbeweging van redundante systemen of gedupliceerde virtuele machines (matige netwerkimpact).

3. Layer 2-lussen (groot netwerkeffect)

#1 Details: Draadloze cliëntbeweging wordt vaak verwacht, en kan gewoonlijk veilig worden genegeerd veronderstellend zijn er geen de dienstgevolgen waargenomen. Clients die zwerven tussen AP's die geen CAPWAP gebruiken terug naar een draadloze controller, of zwerven tussen AP's die worden bestuurd door twee verschillende draadloze controllers, zullen waarschijnlijk dit log genereren. De tijd tussen logbestanden die voor hetzelfde MAC-adres worden gegenereerd,

kan enkele seconden of enkele minuten uit elkaar liggen. Als u ziet één enkel MAC-adres meerdere keren per seconde verplaatst, kan dat een ernstiger probleem aangeven en kan er extra probleemoplossing nodig zijn.

#2 Details: Sommige redundante systemen of apparaten die in een actieve/stand-by staat werken, kunnen een gemeenschappelijk virtueel IP- en mac-adres delen, waarbij alleen het actieve apparaat het op elk moment gebruikt. Als beide apparaten onverwacht actief worden en beide beginnen met het gebruik van het virtuele adres, kan deze fout worden gezien. Gebruik makend van een combinatie van de interfaces vermeld in het logboek en de show mac adres-tabel adres VLAN opdracht traceren de weg van deze mac door het netwerk om te bepalen waar en welke apparaten verkeer genereren van de gedeelde mac. Afhankelijk van de aard van de apparaten die de bewegingen genereren, kan extra probleemoplossing van hun redundantiestatus vereist zijn.
#3 Details: L2-lussen genereren vaak een groot aantal mac-bewegingsfouten in een zeer korte periode (ten minste één per seconde, vaak meer). Logbestanden kunnen doorgaans worden gebruikt voor één of een klein aantal mac-adressen, en gebruikers kunnen een impact op het netwerk ervaren. Routing- en Layer 2-protocollen kunnen vaak mislukken, wat resulteert in extra logbestanden en algemene instabiliteit die worden gemaakt. Om een L2-lus op te lossen, voert u de opdracht show int | in is up|input rate en noteer alle actieve interfaces die een extreem hoog volume van invoerpakketten per seconde tonen (over het algemeen kan dit een zeer groot getal van 6, 7 of 8+ cijfers zijn, afhankelijk van de snelheid van de interface). Er zijn waarschijnlijk slechts 1 of 2 interfaces met een abnormaal hoge invoersnelheid. Richt u niet op uitvoersnelheden en richt u niet op overspannen-tree TCN's. Zodra de interface met hoge invoer is geïdentificeerd, gebruikt u CDP, LLDP of uw interfacebeschrijvingen/netwerkdiagram om in te loggen op het aangrenzende apparaat dat is aangesloten op die poort en voert u de show-inhoudsopgave uit | in is up|input rate commando en herhaal het proces van het overtrekken van de interfaces met abnormale invoersnelheden. Houd spoor van de interfaces en hostnames aangezien u hen door het netwerk vindt. Ga door met het controleren van buren en het bekijken van invoersnelheden tot je geen invoerpoorten meer hebt, en je geen buren meer hebt of weer terug komt op het apparaat dat je al hebt ingeschakeld. Een van de twee mogelijke uitkomsten kan gebeuren tijdens deze methodologie: Als je eindigt met een haven die geen CDP, LLDP, of bekende buur heeft, maar een zeer hoge invoersnelheid, sluit het administratief af. Deze interface is waarschijnlijk de ultieme bron, of levert een bijdrage aan de loop. Wacht 60 seconden op het netwerk om te stabiliseren en als er nog steeds een lusconditie wordt gezien, houd de interface shutdown en start het proces opnieuw, omdat er mogelijk een tweede bron op het netwerk is. Als u op een apparaat eindigt dat u al hebt gecontroleerd, geeft dit aan dat het luspreventieprotocol in gebruik (Spanning-tree is de meest voorkomende) ergens is mislukt. Voor overspannen-boomnetwerken, identificeer welke switch in de weg u overtrok wordt verwacht om wortel te zijn, en het werk achteruit van dat apparaat om te bepalen welke interface in een blokkerende staat binnen uw overgetrokken weg kan zijn. Zodra de interface die kan worden geblokkeerd (maar in staat van doorsturen is) gevonden is, sluit het administratief af. Wacht 60 seconden en controleer het netwerk op stabiliteit. Als de lijn voortduurt, houd de interfacestop en herhaal dit proces.

Opdrachten

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.