# Risoluzione dei problemi relativi alle notifiche di inversione degli indirizzi MAC

## Sommario



## Notifica Flap indirizzo MAC

### VeritàICS

5 - Avviso

### Conseguenze

È possibile esaminare questi messaggi per verificare che non esista un loop di inoltro.

### Descrizione

Questo messaggio di notifica viene generato dallo switch quando rileva un evento di flapping dell'indirizzo MAC sulla rete. L'evento di flapping dell'indirizzo MAC viene rilevato quando uno switch riceve pacchetti dallo stesso indirizzo MAC di origine in due interfacce diverse. Gli switch Cisco Catalyst notificano quando lo stesso indirizzo MAC viene rilevato su più porte dello switch, causando la modifica costante della porta associata all'indirizzo MAC, e avvisano tramite questo syslog che contiene l'indirizzo MAC dell'host, della VLAN e delle porte tra cui l'indirizzo MAC sta lampeggiando. Poiché questo comportamento può essere causato da più motivi, l'identificazione della causa sottostante del flapping dell'indirizzo MAC è importante per garantire la stabilità e le prestazioni della rete.

### MessaggioSyslog

```
SW_MATM-4-MACFLAP_NOTIF
```

## EsempioMessaggio

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

## Famiglia di prodotti

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

## Regex

N/D

## Suggerimento

Le cause possibili sono numerose, alcune delle quali possono indicare un problema di rete grave. I 3 più comuni sono spiegati in dettaglio qui di seguito:

1. Spostamento dei client wireless (nessun impatto sulla rete).

2. Spostamento dell'indirizzo virtuale da sistemi ridondanti o macchine virtuali duplicate (impatto moderato sulla rete).

3. Loop di livello 2 (impatto di rete elevato)

N. 1 Dettagli: lo spostamento dei client wireless è spesso previsto e può essere ignorato in modo sicuro presumendo che non si osservino impatti sui servizi. È probabile che i client in roaming tra punti di accesso che non utilizzano CAPWAP tornino a un controller wireless o che eseguano il roaming tra punti di accesso controllati da due diversi controller wireless generino questo registro. L'intervallo tra i registri generati per lo stesso indirizzo MAC può essere di diversi secondi o minuti. Se un singolo indirizzo MAC viene spostato più volte al secondo, ciò può indicare un problema più

grave ed è possibile richiedere ulteriori procedure di risoluzione dei problemi.

#2 Dettagli: Alcuni sistemi o dispositivi ridondanti che operano in stato attivo/standby possono condividere un indirizzo IP e MAC virtuale comune, ma solo il dispositivo attivo lo utilizza in un determinato momento. Se entrambi i dispositivi diventano inaspettatamente attivi ed entrambi iniziano a utilizzare l'indirizzo virtuale, è possibile visualizzare questo errore. Utilizzando una combinazione delle interfacce menzionate nel log e il comando show mac address-table address vlan, tracciare il percorso di questo mac attraverso la rete per determinare dove e quali dispositivi stanno generando il traffico dal mac condiviso. A seconda della natura dei dispositivi che generano gli spostamenti, può essere necessaria un'ulteriore risoluzione dei problemi relativi agli stati di ridondanza. N. 3 Dettagli: i loop L2 generano spesso un numero elevato di errori di spostamento mac in un periodo di tempo molto breve (almeno uno al secondo, spesso più). I registri possono in genere essere relativi a uno o a un numero ridotto di indirizzi mac e gli utenti possono riscontrare un impatto sulla rete. Il routing e i protocolli di livello 2 possono spesso avere esito negativo, determinando la creazione di log aggiuntivi e un'instabilità generale. Per risolvere i problemi relativi a un ciclo L2, eseguire il comando show int | in è up|velocità di input e notare tutte le interfacce attive che mostrano un volume estremamente elevato di pacchetti di input al secondo (generalmente parlando, questo può essere un numero molto grande 6, 7, o 8+ cifre a seconda della velocità dell'interfaccia). È probabile che vi siano solo 1 o 2 interfacce con una frequenza di ingresso insolitamente alta. Non concentrarsi sulle velocità di output e non sui TCN Spanning-Tree. Dopo aver identificato l'interfaccia a input elevato, utilizzare CDP, LLDP o le descrizioni dell'interfaccia/il diagramma di rete per accedere al dispositivo adiacente collegato a tale porta ed eseguire il comando show int | in è up|comando velocità di input e ripetere il processo di traccia delle interfacce con velocità di input anomale. Tenere traccia delle interfacce e dei nomi host mentre li si traccia attraverso la rete. Continuare a controllare i router adiacenti e le velocità di input fino a esaurimento delle porte di input e a esaurire le porte adiacenti oppure tornare al dispositivo già controllato. L'utilizzo di questa metodologia può produrre due possibili risultati: nel caso di una porta che non dispone di CDP, LLDP o unità adiacenti note, ma ha una velocità di input molto elevata, la porta viene chiusa manualmente. Questa interfaccia è probabilmente l'origine finale o contribuisce al ciclo. Attendere 60 secondi che la rete si stabilizzi e, se viene ancora rilevata una condizione di loop, mantenere l'interfaccia chiusa e riavviare il processo, poiché è possibile che esista una seconda origine nella rete. Se si finisce su un dispositivo già controllato, ciò indica che il protocollo di prevenzione dei loop in uso (Spanning-tree è il più comune) ha avuto un errore. Per le reti spanning-tree, identificare quale switch nel percorso tracciato deve essere root e lavorare all'indietro da quel dispositivo per determinare quale interfaccia può essere in stato di blocco all'interno del percorso tracciato. Una volta trovata l'interfaccia che può essere bloccata (ma che si trova nello stato di inoltro), chiuderla a livello amministrativo. Attendere 60 secondi e verificare la stabilità della rete. Se il loop persiste, mantenere l'interfaccia chiusa e ripetere il processo.

## Comandi

#show version

#show logging

#show spanning-tree

#show mac-address-table

#show mac address-table

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).