Risoluzione dei problemi di loop/flap MAC sugli switch Cisco Catalyst

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi ai link flap/loop MAC sugli switch Cisco Catalyst.

Prerequisiti

Requisiti

Cisco consiglia di avere una conoscenza fondamentale dei concetti base di switching e una conoscenza dello Spanning Tree Protocol (STP) e delle sue funzionalità sugli switch Cisco Catalyst.

Componenti usati

Per la stesura del documento, sono stati usati switch Cisco Catalyst di tutte le versioni (il documento non è limitato a versioni software o hardware specifiche).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento offre una guida per l'approccio sistematico alla risoluzione dei problemi di link o flap MAC sugli switch Cisco Catalyst. I link/loop MAC sono interruzioni in una rete causate da incoerenze nelle tabelle di indirizzi MAC degli switch. Questo documento non solo fornisce indicazioni per identificare e risolvere questi problemi, ma include anche esempi pratici per una migliore comprensione.

Cos'è il flapping degli indirizzi MAC?

Un link MAC si verifica quando uno switch riceve un frame con lo stesso indirizzo di origine MAC, ma da un'interfaccia diversa da quella da cui lo ha imparato inizialmente. In questo modo, lo switch esegue il flap tra le porte e aggiorna la tabella degli indirizzi MAC con la nuova interfaccia. Questa situazione può causare instabilità nella rete e causare problemi di prestazioni.

In uno switch Cisco, il flapping degli indirizzi MAC viene in genere registrato come messaggio simile al seguente:

```
"%SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan x is flapping between port (1) and port (2)"
```

Nell'esempio, l'indirizzo MAC`xxxx.xxxx.xxxx`è stato appreso per la prima volta sulla porta interfaccia (1), quindi visto sulla porta interfaccia (2), causando un link flap all'indirizzo MAC.

Il flapping degli indirizzi MAC è in genere causato da un loop sul layer 2 della rete, spesso causato da una configurazione errata di STP o da problemi con i collegamenti ridondanti. Altre cause possono essere guasti hardware, bug software o problemi di sicurezza come lo spoofing dei MAC.

La risoluzione dei problemi dei flap MAC spesso implica l'identificazione e la risoluzione di eventuali loop nella rete, la verifica delle configurazioni dei dispositivi o l'aggiornamento del firmware/software dei dispositivi.

Linee guida generali per la risoluzione dei problemi

- Identificazione del flapping degli indirizzi MAC: cercare nello switch i log che indicano il flapping degli indirizzi MAC. Ad esempio, in uno switch Cisco, il messaggio del log ha questo aspetto:

```
%SW_MATM-4-MACFLAP_NOTIF: Host [mac_address] in vlan [vlan_id] is flapping between port [port_id_
```

- Annotare l'indirizzo MAC e le interfacce: il messaggio di log fornisce l'indirizzo MAC che si sta flappando e le interfacce tra cui si sta flappando. Prendi nota di queste informazioni come supporto per la tua indagine.
- Esaminare le interfacce interessate: usare la CLI dello switch per esaminare le interfacce interessate. È possibile utilizzare comandi come`show interfaces`o`show mac address-table`per verificare quali dispositivi sono connessi alle interfacce e dove viene appreso l'indirizzo MAC.
- Traccia l'indirizzo MAC flapping: MAC sta imparando attraverso le porte X e Y. Una porta ci porta alla posizione in cui è collegato il MAC e l'altra ci porta al loop. Selezionare una porta e iniziare a eseguire il comando using`show mac address-table`su ciascuno switch di layer 2 nel percorso.
- Verifica loop fisici: esaminare la topologia di rete per verificare se sono presenti loop fisici. Questa condizione si può verificare se esistono più percorsi tra gli switch. Se viene rilevato un loop, è necessario riconfigurare la rete per rimuoverlo.
- Controllare STP: STP è stato progettato per impedire che nella rete si creino loop bloccando alcuni percorsi. Se STP non è configurato correttamente, non impedisce i loop come deve essere. Per controllare la configurazione STP, usare comandi come`show spanning-tree`. Verificare inoltre la presenza di notifiche di modifica della topologia (TCN) utilizzando il comando`show spanning-tree detail | include ieee|occur|from|is`.
- Verificare la presenza di indirizzi MAC duplicati: se due dispositivi della rete hanno lo stesso indirizzo MAC (principalmente nell'installazione ad alta disponibilità (HA) e più schede NIC (Network Interface Controller)), può causare lo sfarfallio degli indirizzi MAC. Usare il comando`show mac address-table`per cercare gli indirizzi MAC duplicati sulla rete.
- Verificare la presenza di hardware o cavi difettosi: cavi di rete o hardware difettosi possono causare l'invio di frame alle interfacce errate, con conseguente flapping dell'indirizzo MAC. Controllare le condizioni fisiche dei cavi e valutare se sostituire l'hardware per verificare se il problema persiste. Lo sfarfallio dell'interfaccia può causare lo sfarfallio dell'indirizzo MAC anche sugli switch.
- Controlla bug del software: a volte, il flapping dell'indirizzo MAC può essere causato da bug nel software dei dispositivi di rete. controllare lo strumento Bug Search.

Bug Search Tool: https://bst.cloudapps.cisco.com/bugsearch

Guida di Bug Search Tool: https://www.cisco.com/c/en/us/support/web/tools/bst/bsthelp/index.html#search

- Contatta il supporto TAC: se il problema persiste, potrebbe essere il momento di contattare il

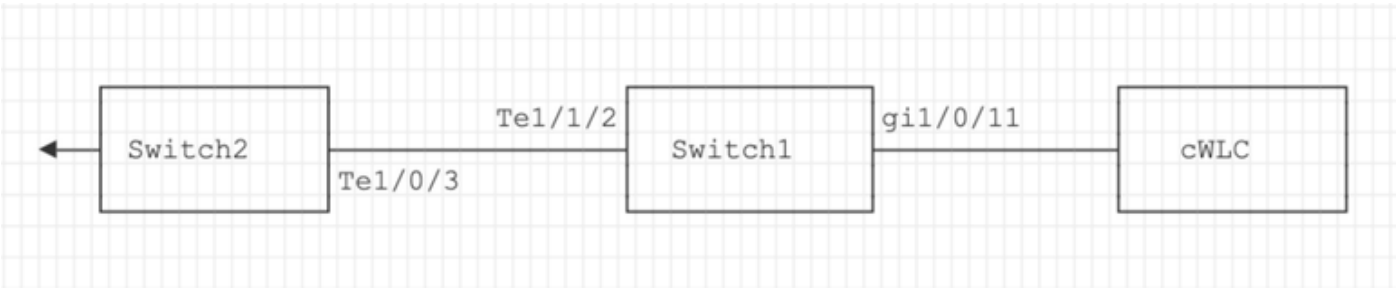
supporto TAC di Cisco. Possono fornire ulteriore assistenza.

Studio del caso 1

Descrizione del problema

Il controller WLC sta riscontrando una perdita di connettività al gateway e le perdite di pacchetti impediscono agli AP di unirsi al controller.

Topologia



Procedura di risoluzione dei problemi

Lo sfarfallio dell'indirizzo MAC è stato identificato sullo switch (switch 1) collegato al WLC.

```
*Aug  5 05:52:50.750: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:03.327: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
*Aug  5 05:53:21.466: %SW_MATM-4-MACFLAP_NOTIF: Host 0000.5e00.0101 in vlan 4 is flapping between port
```

Apprendimento MAC:

Immettere il comando`show mac address-table address`
per controllare l'indirizzo MAC appreso sulla porta.

<#root>

```
Switch1#show mac address-table address 0000.5e00.0101

          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    DYNAMIC     Gi1/0/11

   4    0000.5e00.0101    DYNAMIC     Te1/1/2
```

Configurazione delle porte Gi1/0/1 e Te1/1/2:

Immettere il comando`show running-config interface`
per controllare la configurazione dell'interfaccia.

<#root>

```
interface GigabitEthernet1/0/11


 switchport trunk native vlan 4
 switchport mode trunk
end


interface TenGigabitEthernet1/1/2


 switchport mode trunk
end
```

CDP Neighbors delle porte Gi1/0/1 e Te1/1/2:

Immettere il comando`show cdp neighbors`
per controllare i dettagli delle periferiche collegate.

<#root>

```
Switch1#show cdp neighbors gi1/0/11


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

eWLC            Gig 1/0/11        130              R T   C9115AXI- Gig 0 < ----- eWLC Controller



Switch1#show cdp neighbors gi1/1/2


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Switch2


                Ten 1/1/2         163            R S I  C9500-16X Ten 1/0/3 < ----- Uplink Switch
```

MAC Learning sullo switch 2 (switch uplink):

Immettere il comando`show mac address-table address`
per controllare l'indirizzo MAC appreso sulla porta.

<#root>

```
Switch2#show mac address-table address 0000.5E00.0101


          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   4    0000.5e00.0101    STATIC

Vl4 < ----- VRRP MAC of Vlan4


   4    0000.5e00.0101    DYNAMIC

Te1/0/13 < ----- Learning from Switch1 (eWLC connected Switch)
```

<#root>

```
Switch2#show vrrp  vlan 4


Vlan4 - Group 1

 - Address-Family IPv4
  State is MASTER
  State duration 5 days 4 hours 22 mins
  Virtual IP address is x.x.x.x

  Virtual MAC address is 0000.5E00.0101 < ------ VRRP MAC of Vlan4


  Advertisement interval is 1000 msec
```

Causa principale

È stato verificato che l'ID del protocollo VRRP (Virtual Router Redundancy Protocol) dello switch 2 e del WLC fossero gli stessi, con la conseguente generazione dello stesso MAC virtuale da parte del VRRP.

Risoluzione

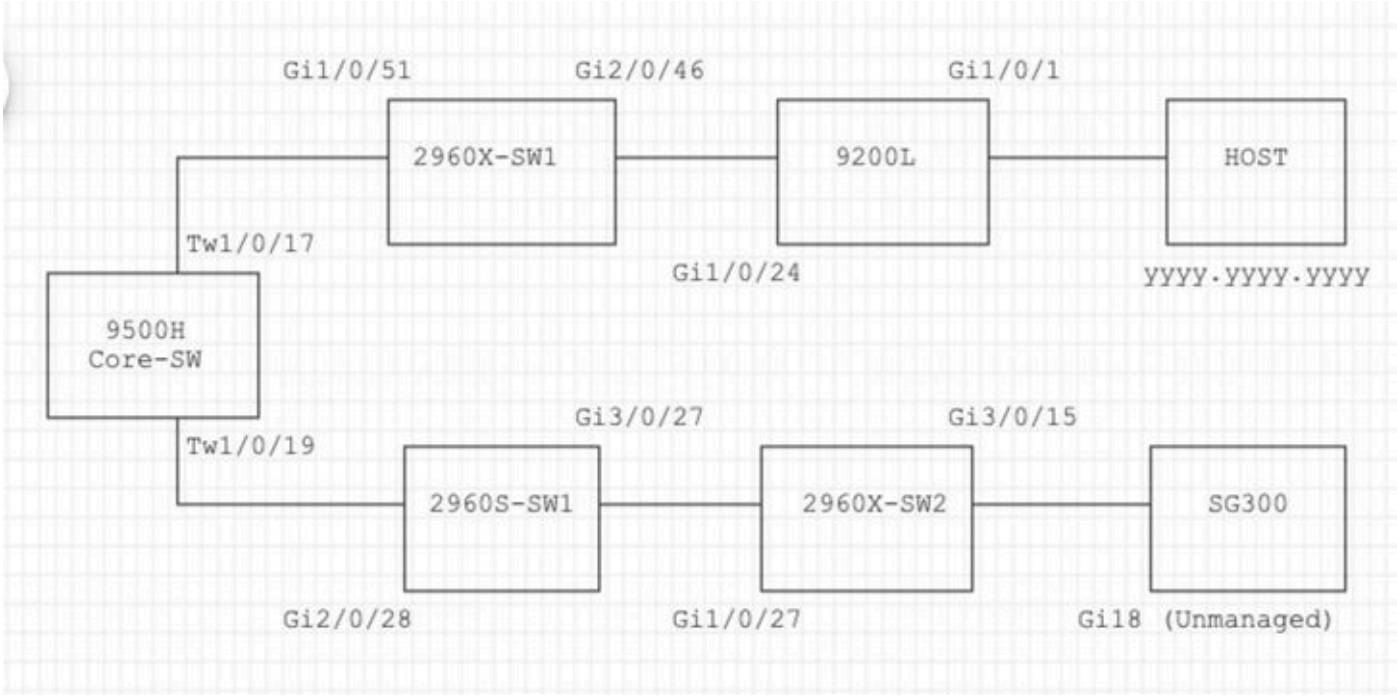
Il problema è stato risolto dopo la modifica dell'istanza VRRP sul WLC, che causava un MAC duplicato sullo switch con una perdita di connettività al gateway e perdite di pacchetti, impedendo agli AP di unirsi al controller.

Case study 2

Descrizione del problema

Alcuni dei server sono inaccessibili o hanno problemi di latenza/caduta significativi.

Topologia



Procedura di risoluzione dei problemi

1. Si è verificato un flapping dell'indirizzo MAC osservato sullo switch Core.

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port Tw
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port Tw
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port Po
```

2. Scelta dell'indirizzo MAC`yyyy.yyyy.yyyy`per il processo di risoluzione dei problemi.

Apprendimento MAC:

Immettere il comando`show mac address-table address`
per controllare l'indirizzo MAC appreso sulla porta.

<#root>

```
Core-SW#show mac address-table address yyyy.yyyy.yyyy
```

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Twe1/0/17
```

CDP Vicini delle porte Twe 1/0/17 e Twe 1/0/17:

Immettere il comando`show cdp neighbors`
per controllare i dettagli delle periferiche collegate.

<#root>

```
Core-SW#show cdp neighbors Twe 1/0/17


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960X-SW1


                 Twe 1/0/17        162              S I   WS-C2960X Gig 1/0/51



Core-SW#show cdp neighbors Twe 1/0/19


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

2960S-SW1


                 Twe 1/0/19        120              S I   WS-C2960S Gig 2/0/28
```

Registri da 2960X-SW1 collegati a Core-SW Twe1/0/17:

L'indirizzo MAC`yyyy.yyyy.yyyy`lampeggia tra le porte Gi1/0/51 e Gi2/0/46 (9200L).

<#root>

```
2960X-SW1#show mac address-table address yyyy.yyyy.yyyy


          Mac Address Table
-------------------------------------------
```

```
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy    DYNAMIC     Gi1/0/51
```

2960X-SW1#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi2/0/46
```

2960X-SW1#show run interface gi 1/0/51

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/51
switchport mode trunk
end
```

2960X-SW1#show run interface gi 2/0/46

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet2/0/46
switchport mode trunk
end
```

Registri da 9200L:

(Questa sembra essere la porta valida per questo indirizzo MAC).

<#root>

9200L#show mac address-table address yyyy.yyyy.yyyy

```
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    yyyy.yyyy.yyyy DYNAMIC     Gi1/0/1
```

9200L#show run interface gi 1/0/1

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet1/0/1
switchport mode access
end
```

2960S-SW1 Collegato al Core-SW Twe1/0/19:

(Sembra essere un percorso ciclico). La porta sul Core-SW è stata chiusa per ridurre il loop.

Tuttavia, i flap MAC erano ancora osservati sul Core-SW.

Registri da 2960S-SW1:

<#root>

```
Nov 14 08:36:34.637: %SW_MATM-4-MACFLAP_NOTIF: Host xxxx.xxxx.xxxx in vlan 1 is flapping between port G
Nov 14 08:36:34.838: %SW_MATM-4-MACFLAP_NOTIF: Host yyyy.yyyy.yyyy in vlan 1 is flapping between port G
Nov 14 08:36:34.882: %SW_MATM-4-MACFLAP_NOTIF: Host zzzz.zzzz.zzzz in vlan 1 is flapping between port G
```

2960S-SW1#show run interface gi 3/0/27

```
Building configuration...

Current configuration : 62 bytes
!
interface GigabitEthernet3/0/27
switchport mode trunk
end
```

2960S-SW1#show cdp neighbor gi 3/0/27

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

2960X-SW2

Gig 3/0/27 176 S I WS-C2960X Gig 1/0/27

Registri da 2960X-SW2:

<#root>

2960X-SW2#show run interface gi 3/0/15

```
Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet3/0/15
end
```

2960X-SW2#show cdp neighbor gi 3/0/15

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
```

SG300   Gig 3/0/15   157   S I   SG300-28P gi18

2960X-SW2#config terminal

2960X-SW2(config)#interface gi 3/0/15

2960X-SW2(config-if)#shutdown

Causa principale

Flash MAC rilevati a causa dello switch SG300 (non gestito) collegato alla rete.

Risoluzione

Il problema di flapping dell'indirizzo MAC è stato risolto chiudendo la porta collegata allo switch non gestito SG300.

Prevenzione

STP Portfast:

Con STP PortFast, una porta LAN di layer 2 entra immediatamente nello stato di inoltro, ignorando gli stati di ascolto e apprendimento. STP PortFast impedisce la generazione di TCN STP, non significativi per le porte che non ricevono BPDU (STP Bridge Protocol Data Unit). Configurare STP PortFast solo sulle porte connesse ai dispositivi host terminali di VLAN e dalle quali la porta non deve mai ricevere BPDU STP, quali workstation, server e porte sui router non configurati per supportare il bridging.

BPDU Guard:

STP BPDU Guard integra la funzionalità di STP PortFast. Sulle porte abilitate per STP PortFast, STP BPDU Guard protegge i loop di layer 2 che STP non può fornire quando STP PortFast è abilitato. STP BPDU Guard chiude le porte che ricevono BPDU.

Root Guard:

Root Guard impedisce che le porte diventino porte radice STP. Utilizzare STP Root Guard per evitare che porte non adatte diventino porte radice STP. Un esempio di porta non idonea è una porta che si collega a un dispositivo al di fuori del controllo amministrativo diretto della rete.

Loop Guard:

Loop Guard è un'ottimizzazione proprietaria di Cisco per STP. La protezione loop protegge le reti di layer 2 dai loop che si verificano quando qualcosa impedisce il normale inoltro di BPDU su collegamenti point-to-point (ad esempio, un malfunzionamento dell'interfaccia di rete o una CPU occupata). La funzionalità Loop Guard integra la protezione contro gli errori di collegamento unidirezionale fornita dal protocollo UDLD (Unidirectional Link Detection). La protezione loop isola gli errori e consente la convergenza di STP in una topologia stabile con il componente in errore escluso dalla topologia STP.

Filtro BPDU:

Il protocollo STP viene disattivato. I pacchetti BPDU non vengono inviati né elaborati al momento della ricezione. È comune ai provider di servizi, non necessariamente alle reti aziendali.

UDLD Aggressivo:

Il protocollo UDLD proprietario di Cisco controlla la configurazione fisica dei collegamenti tra i dispositivi e le porte che supportano UDLD. UDLD rileva l'esistenza di collegamenti unidirezionali. il protocollo UDLD può funzionare in modalità normale o aggressiva. Il protocollo UDLD in modalità normale classifica un collegamento come unidirezionale se i pacchetti UDLD ricevuti non contengono informazioni corrette per il dispositivo adiacente. Oltre alla funzionalità del protocollo UDLD in modalità normale, il protocollo UDLD in modalità aggressiva porta le porte in stato err-disabled se non è possibile ristabilire la relazione tra due router adiacenti sincronizzati in precedenza.

Controllo Storm:

Il controllo del Traffic Storm è implementato nell'hardware e non influisce sulle prestazioni complessive dello switch. In genere, le stazioni terminali come PC e server sono la fonte del traffico broadcast che può essere eliminato. Per evitare un'elaborazione non necessaria del traffico di trasmissione in eccesso, abilitare il controllo delle tempeste di traffico per il traffico di trasmissione sulle porte di accesso che si connettono a unità terminali e sulle porte che si connettono a nodi di rete chiave.

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).