Informazioni sull'apprendimento imprevisto dell'indirizzo MAC sugli switch Catalyst serie 9000

Sommario

Introduzione

In questo documento viene descritto uno scenario in cui uno switch di accesso Catalyst 9300 stava imparando un indirizzo MAC a monte su una porta a valle.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Switching per LAN
- Apprendimento indirizzo MAC
- Sessioni di autenticazione e comportamento correlato

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Switch Cisco Catalyst serie 9300
- Software versione 17.6.5

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

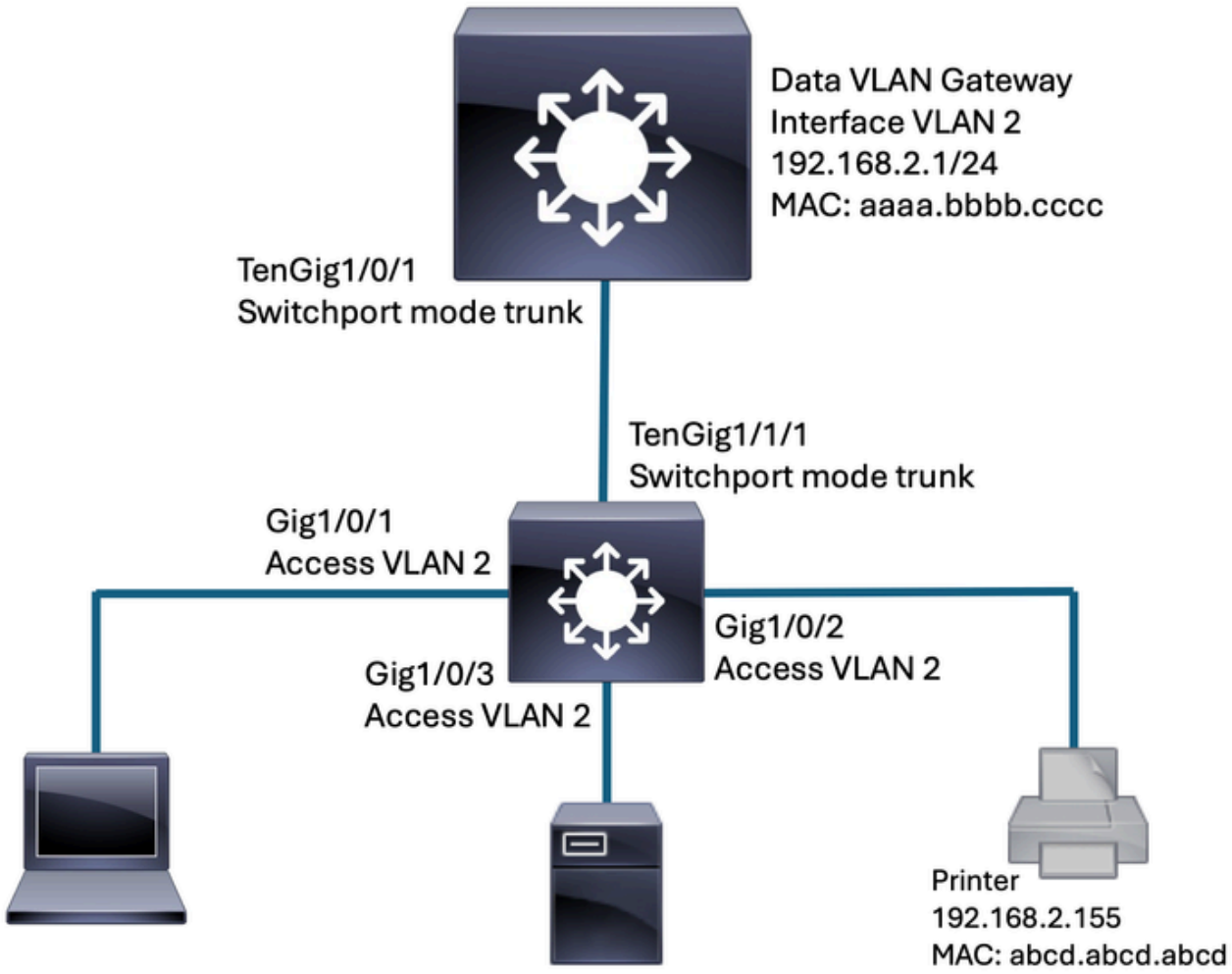
Gli switch Catalyst imparano gli indirizzi MAC sulle porte degli switch in base all'indirizzo MAC di origine (SMAC) di un frame in entrata. La tabella degli indirizzi MAC è in genere una fonte affidabile di informazioni che guida un tecnico di rete verso la posizione di un determinato indirizzo. Si verificano situazioni in cui il traffico proveniente da una particolare origine, un endpoint o persino il gateway della rete locale, entra in uno switch da una direzione imprevista. Questo

documento descrive una situazione specifica in cui l'indirizzo MAC del gateway upstream è stato appreso in modo imprevisto su interfacce di accesso casuale. I dettagli si basano sui casi TAC risolti dai tecnici TAC che lavorano in collaborazione con i team dei clienti.

Problema

In questo scenario, il client ha notato per primo il problema quando gli endpoint nella VLAN dati (VLAN 2 in questa dimostrazione) hanno perso la connettività con gli host all'esterno della subnet. Dopo un'ulteriore ispezione, hanno osservato che l'indirizzo MAC del gateway VLAN 2 è stato appreso su un'interfaccia utente anziché sull'interfaccia prevista.

Inizialmente, il problema si è verificato in modo casuale in una rete di grandi dimensioni composta da più campus. Viste le informazioni di cui disponiamo su come gli switch hanno appreso gli indirizzi MAC, abbiamo ipotizzato una sorta di riflessione dei pacchetti, ma la sfida è stata dimostrare che il problema era esterno allo switch. Dopo aver raccolto ulteriori dati su altre volte in cui si è verificato questo problema, è stato possibile identificare una tendenza con le porte utente coinvolte. In ogni occorrenza è stato coinvolto un modello specifico di endpoint.



Segmento della rete interessata

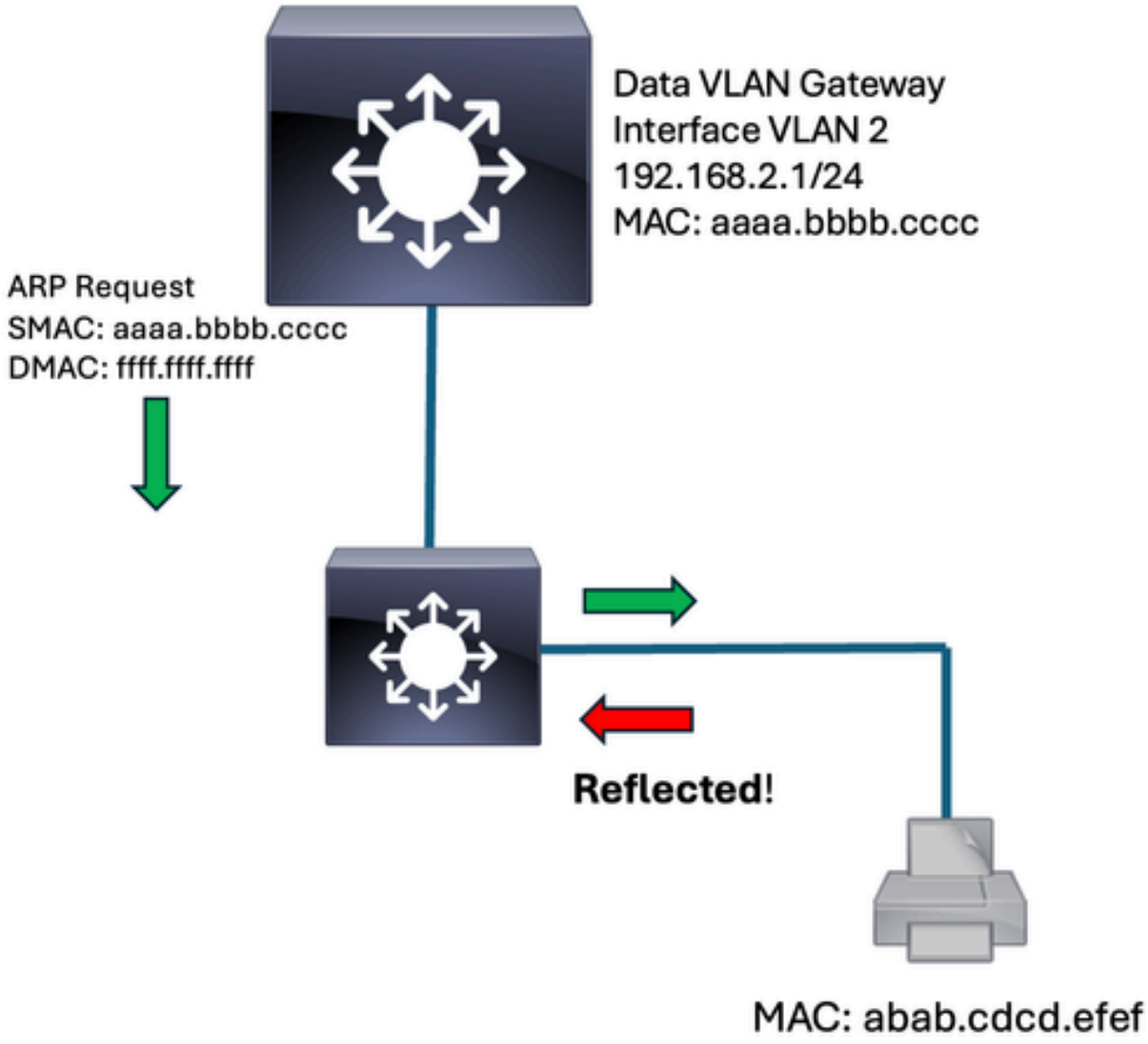
Il comando "show mac address-table <indirizzo>/<interfaccia>" viene usato per interrogare la tabella degli indirizzi MAC. Nello scenario operativo o normale, che l'indirizzo del gateway venga appreso nella modalità Ten1/1/1 dello switch a cui si connettono gli endpoint.

```
<#root>

ACCESS-SWITCH#

show mac address-table

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    DYNAMIC     Ten1/1/1 <-- Notice the "type" is DYNAMIC. This means the entry w
   2    abcd.abcd.abcd    STATIC      Gig1/0/2 <-- In contrast, this MAC is STATIC. This suggests a fea
```

Nello scenario interrotto, il MAC gateway è stato appreso su Gi1/0/2 e non su Te1/1/1.

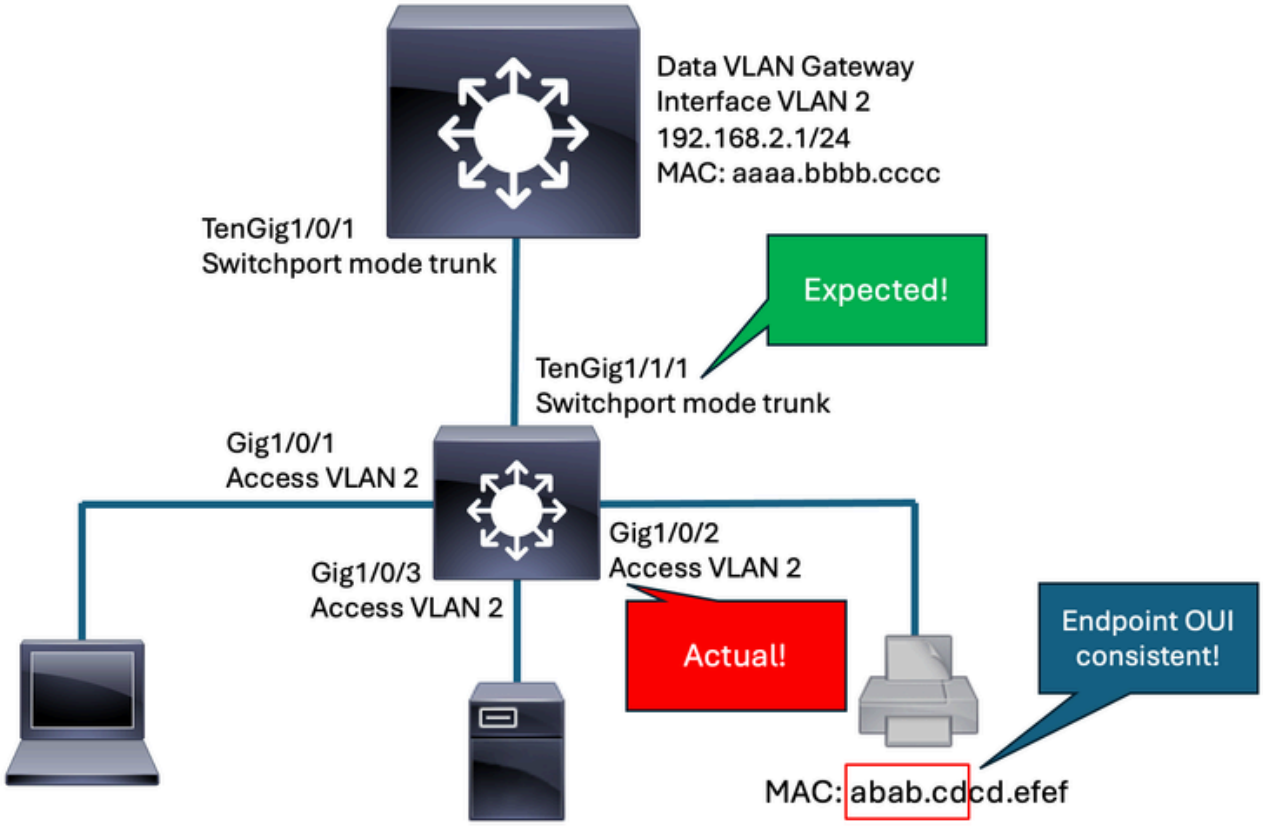
```
<#root>

ACCESS-SWITCH#

show mac address-table

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 <snip>
   2    aaaa.bbbb.cccc    STATIC      Gig1/0/2 <-- Notice that the type is now STATIC.
   2    abcd.abcd.abcd    STATIC      Gig1/0/2
```

In questo scenario, lo switch di accesso esegue 802.1x con fallback MAB (MAC Authentication Bypass) sulle relative interfacce di accesso. Queste funzionalità chiave hanno influito sull'impatto complessivo dei servizi. Una volta appreso l'indirizzo MAC del gateway su una porta di accesso, diventerebbe "statico" in funzione della funzione di sicurezza. La funzione di sicurezza ha inoltre impedito all'indirizzo MAC del gateway di tornare all'interfaccia corretta. Le informazioni su 802.1x, MAB e il concetto di 'mac-move' sono ulteriormente esplorate nella relativa guida alla configurazione.



Dimostrazione del traffico riflesso

Il riflesso del pacchetto porta all'apprendimento anomalo di MAC.



In questo diagramma viene evidenziata l'interfaccia prevista rispetto a quella effettiva che consente di apprendere l'indirizzo MAC GW.

Nell'esempio viene evidenziato l'identificatore univoco dell'organizzazione (OUI, Organizational Unique Identifier). Ciò ha consentito al team di identificare che l'endpoint è di un produttore comune.

Soluzione

Il problema è stato causato dal comportamento imprevisto dell'endpoint. Non ci si aspetta mai che un endpoint rifletta il traffico nella rete.

In questo caso, la conclusione principale è stata la tendenza con gli endpoint. È difficile risolvere un problema che si verifica in modo casuale in una rete di grandi dimensioni. Questo diede al team un sottoinsieme di porte utente da esaminare.

Notare anche che le funzionalità di sicurezza coinvolte, ovvero dot1x con fallback MAB, hanno giocato un ruolo nell'impatto del servizio. Senza queste funzionalità in grado di rispondere al traffico riflesso, l'impatto sul servizio probabilmente non sarebbe stato così significativo.

Gli strumenti di acquisizione dei pacchetti sono stati usati per identificare che il traffico era davvero riflesso dall'endpoint. Lo strumento di acquisizione dei pacchetti (EPC) incorporato disponibile sugli switch Catalyst può essere utilizzato per identificare i pacchetti in entrata.

<#root>

```
Switch#
monitor capture TAC interface gi1/0/2 in match mac host aaaa.bbbb.cccc any

Switch#
monitor capture TAC start


<wait for the MAC learning to occur>
Switch#
monitor capture TAC stop
Switch#
show monitor capture TAC buffer
```

Physical SPAN (analizzatore porte switch) è uno strumento affidabile di acquisizione dei pacchetti che può essere usato anche in questo scenario.

<#root>

```
Switch(config)#
monitor session 1 source gi1/0/2 rx

Switch(config)#
monitor session 1 filter mac access-group MACL
 <- Since we know the source MAC of the traffic we look for, the SPAN can be filtered.
Switch(config)#
monitor session 1 destination gig1/0/48
```

Il team è stato in grado di acquisire il traffico riflesso su una porta a cui era connesso un endpoint sospetto. In questo scenario, l'endpoint rifletterebbe i pacchetti ARP provenienti dall'indirizzo MAC del gateway e reintrodotti nella porta dello switch. La porta dello switch abilitata per il MAB tenterà di autenticare l'indirizzo MAC del gateway. L'implementazione della sicurezza della porta dello switch ha consentito all'indirizzo MAC del gateway di autorizzare la VLAN dati. Poiché l'indirizzo MAC è stato appreso insieme alla funzione di sicurezza, si "attacca" come indirizzo MAC STATICO sulla porta utente. Inoltre, poiché l'implementazione della sicurezza ha bloccato lo spostamento degli indirizzi MAC autorizzati, lo switch non ha potuto dimenticare l'indirizzo MAC sulla porta utente e non è riuscito a riapprenderlo sull'interfaccia prevista. La riflessione sui pacchetti, unita all'implementazione della sicurezza, ha portato a una situazione in cui il traffico è

stato influenzato per l'intera VLAN locale.

Sequenza di eventi:

1. Gli indirizzi MAC vengono appresi sulle interfacce previste. Si tratta dello stato normale della rete.

2. L'endpoint riflette il traffico inviato dal gateway alla porta che si connette allo switch.

3. A causa dell'implementazione della sicurezza della porta dello switch dell'endpoint, l'indirizzo MAC riflesso attiva una sessione di autenticazione. L'indirizzo MAC è programmato come voce STATIC.

4. Una volta che l'indirizzo MAC è scaduto dalla porta dello switch prevista, l'implementazione della sicurezza impedisce che venga riappreso sull'uplink.

5. Per eseguire il ripristino, è necessario chiudere o riattivare la porta.

Il rimedio definitivo per questa situazione è stato quello di risolvere il comportamento dell'endpoint. In questo scenario, il comportamento era già noto al fornitore dell'endpoint ed è stato corretto con un aggiornamento del firmware. L'hardware dello switch Catalyst, nonché il software e la configurazione si sono comportati correttamente come previsto.

Il concetto chiave di questo scenario è l'apprendimento MAC. Gli switch Catalyst imparano gli indirizzi MAC in entrata in base all'indirizzo MAC di origine del frame ricevuto. Se si apprende un indirizzo MAC su un'interfaccia imprevista, si può tranquillamente concludere che la porta dello switch ha ricevuto un frame in entrata con quell'indirizzo MAC nel campo MAC di origine.

In situazioni molto limitate, i pacchetti possono passare dall'interfaccia fisica all'ASIC di inoltro dello switch e viceversa, o essere trasmessi a causa di altri comportamenti errati interni. Se il problema persiste e non viene individuato alcun bug esistente, contattare TAC per assistenza nell'isolamento.

Informazioni correlate

- Configurazione dell'acquisizione del pacchetto - Catalyst 9300
- Configurazione di SPAN e RSPAN - Catalyst 9300
- Risoluzione dei problemi relativi a Mac Address Table Manager sugli switch Catalyst serie 9000
- Configurazione dell'autenticazione basata sulla porta IEEE 802.1x - Catalyst 9300
- Supporto tecnico Cisco e download

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).