瞭解Catalyst 9000系列交換器上的意外MAC學習

目錄

簡介

本檔案將說明Catalyst 9300存取交換器正在下游連線埠上學習上游MAC位址的情境。

必要條件

需求

思科建議您瞭解以下主題：

- LAN 交換
- MAC位址學習
- 驗證作業階段和相關行為

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 9300 系列交換器
- 軟體版本17.6.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

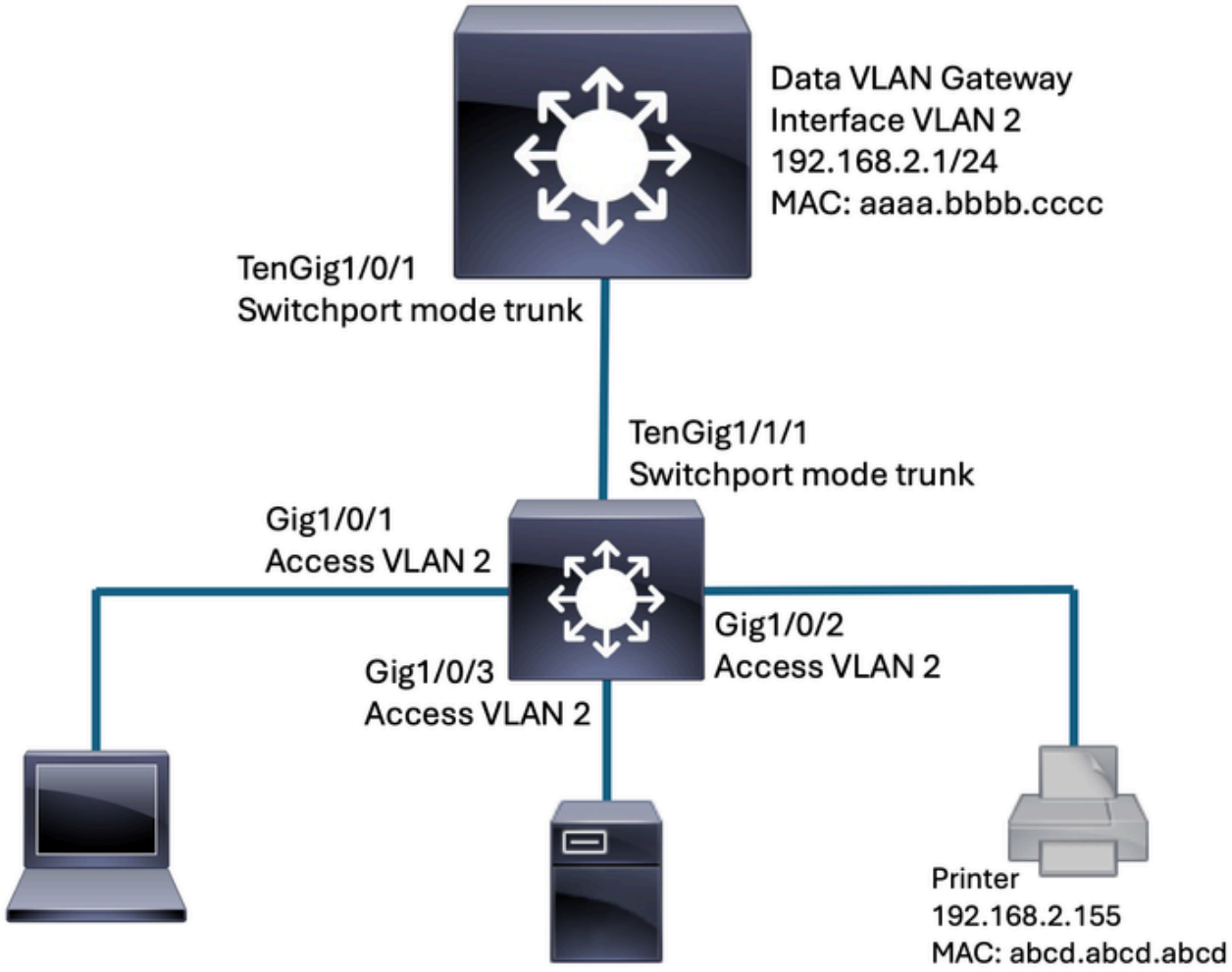
Catalyst交換器會根據傳入訊框的來源MAC位址(SMAC)，得知交換器連線埠上的MAC位址。MAC地址表通常是一個可信的資訊源，可引導網路工程師找到指定地址的位置。當來自特定來源（端點或甚至本地網路的閘道）的流量從意外方向進入交換器時，就會發生這種情況。本文描述在隨機訪問介面上意外獲知上游網關MAC地址的特定情況。詳細資訊基於與客戶團隊合作工作的TAC工程師解決的TAC案例。

問題

此案例中的客戶端首先發現了一個問題，即其資料VLAN（本演示中的VLAN 2）中的終端與其子網外主機的連線中斷。在進一步檢查後，他們發現VLAN 2網關的MAC地址是在使用者介面上獲知的，而不是在預期的介面上。

該問題最初似乎隨機發生在由多個校園組成的大型網路中。鑑於我們瞭解的交換機如何學習MAC地

址，我們假定採用某種資料包反射，但困難在於如何證明問題是交換機外部的問題。在收集有關此問題發生的其它時間的其他資料之後，我們能夠識別涉及使用者埠的趨勢。每次發生都涉及特定的端點模型。



受影響的網路段

命令「show mac address-table <address>/<interface>」用於查詢MAC地址表。在工作或正常情況下，會在終端連線的交換機的Ten1/1/1上學習網關地址。

<#root>

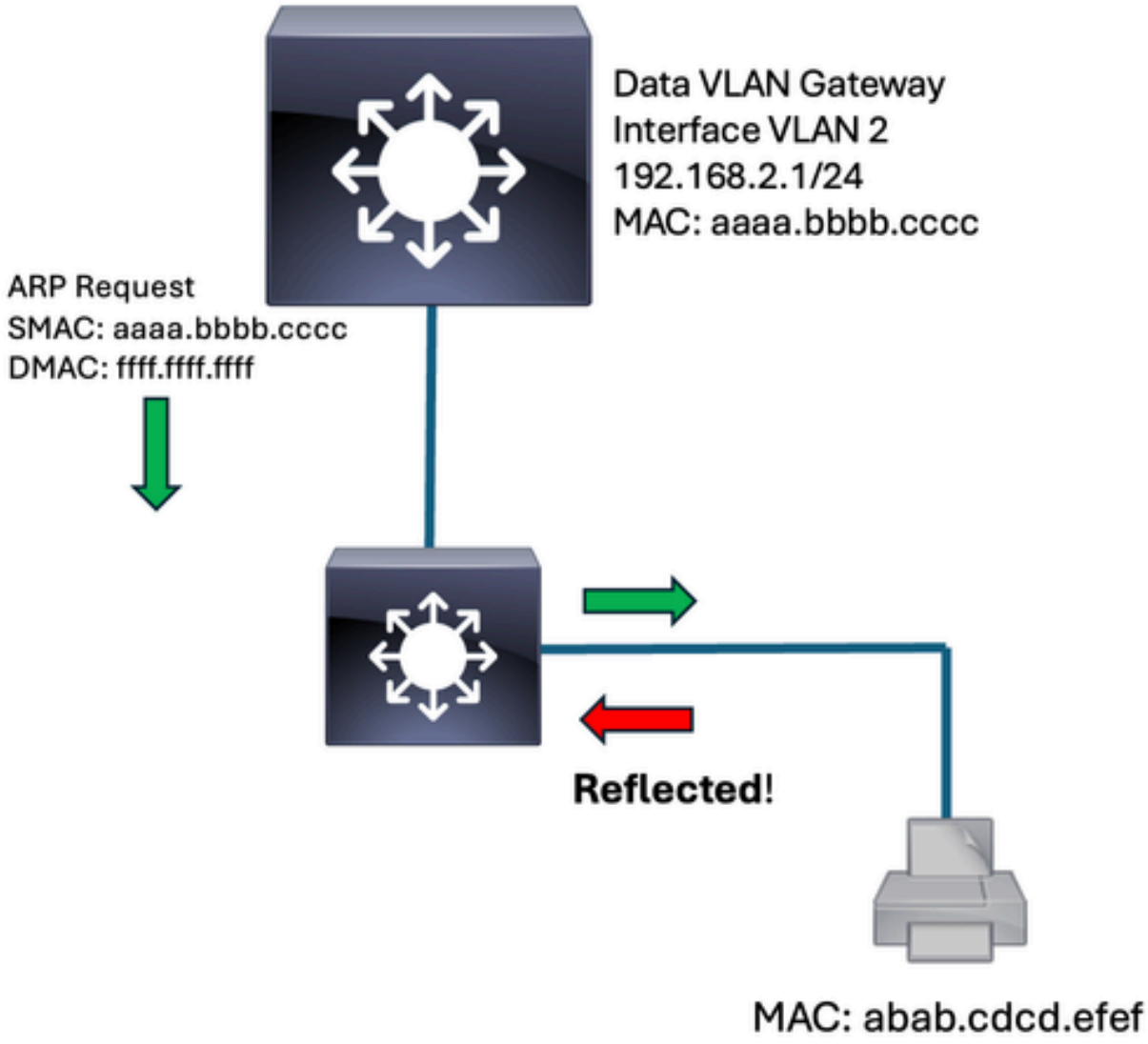
```
ACCESS-SWITCH#

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 wa
   2    abcd.abcd.abcd    STATIC      Gig1/0/2 <-- In contrast, this MAC is STATIC. This suggests a feat
```

在中斷的情況中，網關MAC是在Gi1/0/2上獲知的，而不是在Te1/1/1上。

<#root>

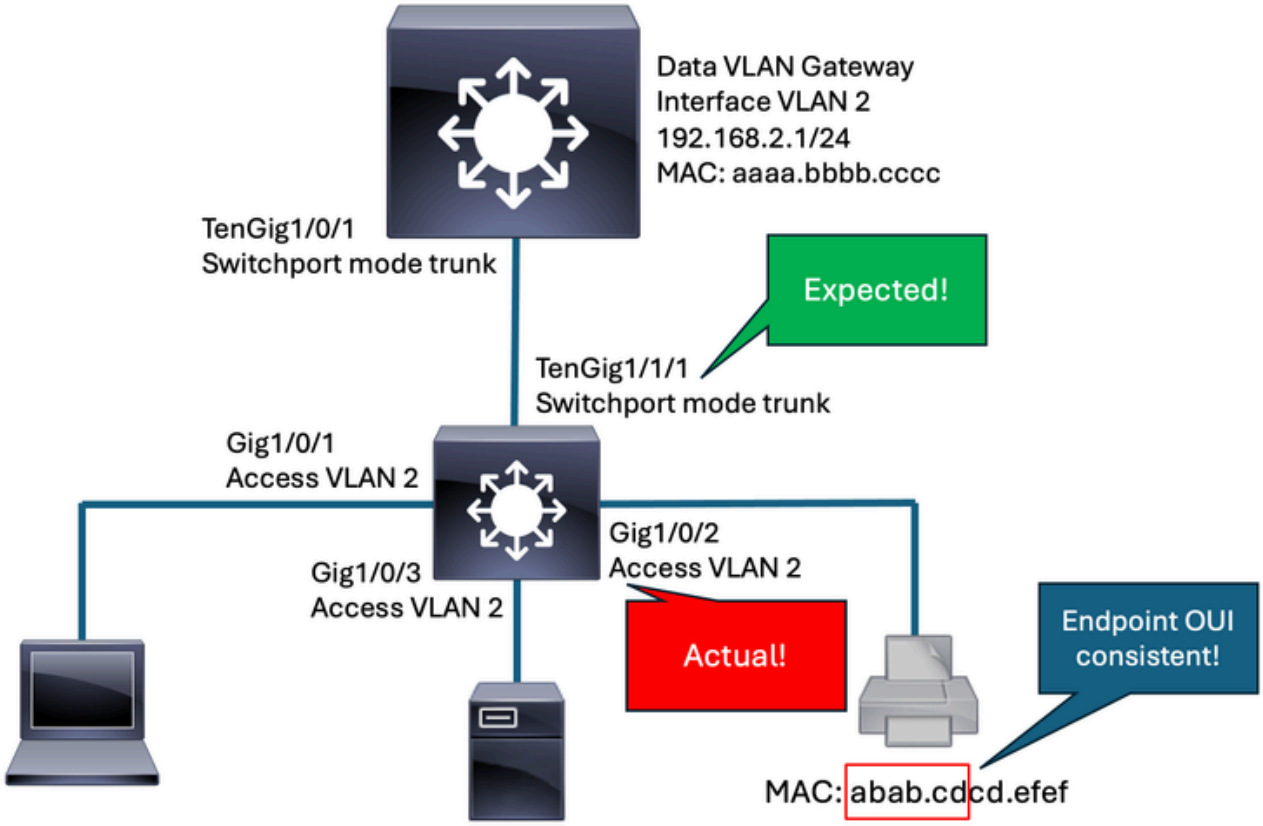
```
ACCESS-SWITCH#

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
```

此方案中的接入交換機在其接入介面上運行帶MAB（MAC身份驗證旁路）回退的802.1x。這些關鍵功能在整體服務影響中扮演了重要角色。一旦在接入埠上獲知網關MAC地址，它就會成為作為安全功能的「靜態」地址。 安全功能還阻止網關MAC地址移回正確的介面。有關802.1x、MAB和「mac-move」概念的資訊，將在相關配置指南中進一步探討。



反射流量的演示

封包反射導致異常MAC學習。



此圖突出顯示學習GW MAC的預期介面與實際介面。

該示例突出顯示組織唯一識別符號(OUI)。 這有助於團隊識別出該終端屬於一家公共製造商。

解決方案

此問題的核心是終結點的意外行為。我們從未期望端點將流量反映回網路。

此案例的關鍵發現是具有端點的趨勢。很難排除大型網路中隨機出現的問題。這給團隊提供了要仔細檢查的使用者埠子集。

另請注意，涉及的安全功能（即具有MAB回退的dot1x）在服務影響中發揮了作用。如果沒有這些功能對反映的流量做出響應，服務影響可能就不會那麼大。

利用資料包捕獲工具來識別流量確實被終端反映出來。 Catalyst交換器上可用的嵌入式封包擷取(EPC)工具可用於識別傳入封包。

<#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
```

實體SPAN（交換器連線埠分析器）是可靠的封包擷取工具，也可用於此情境。

<#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
```

該團隊能夠捕獲可疑終端連線的埠上的反射流量。 在此案例中，端點會將從閘道MAC位址獲得的ARP封包反射回交換器連線埠。啟用MAB的交換機埠將嘗試驗證網關MAC地址。交換機埠安全實施允許網關MAC在資料VLAN中進行授權。由於MAC地址是結合安全功能獲取的，因此它將「粘滯」為使用者埠上的靜態MAC。此外，由於安全實施阻止了授權MAC地址的MAC地址移動，因此交換機無法忘記使用者埠上的MAC，並且無法在預期的介面上重新學習該MAC。資料包反射加上安全實施導致整個本地VLAN的流量受到影響。

事件順序：

1.在預期介面上獲取MAC。這是網路的正常狀態。

2.端點將源自閘道的流量反射回連線到交換器的連線埠。

3.由於終端交換機埠安全實施，反映的MAC將觸發身份驗證會話。MAC被程式設計為STATIC條目。

4.一旦超出預期交換機埠的MAC老化，安全實施將阻止在上行鏈路上重新學習它。

5.埠需要關閉/取消關閉才能恢復。

此情況的最終修複方案是解決終端行為。 在此場景中，終端供應商已知道該行為，並且已使用韌體更新修復該行為。Catalyst交換機硬體以及軟體和配置都完全按照預期運行。

此場景的主要特點是MAC學習的概念。Catalyst交換機根據收到的幀的源MAC地址在入口獲取MAC地址。如果在意外的介面上獲知了MAC地址，可以安全推斷交換機埠在入口收到幀，該幀的MAC地址在源MAC欄位中。

在非常有限的情況下，資料包可能會在交換機的物理介面和轉發ASIC之間反映，或者通過某些其他內部錯誤行為反映。如果出現這種情況，且找不到可以說明問題的現有錯誤，請與TAC聯絡以協助隔離。

相關資訊

- 設定封包擷取 — Catalyst 9300
- 設定SPAN和RSPAN - Catalyst 9300
- Catalyst 9000系列交換器上的Mac位址表管理員疑難排解
- 配置IEEE 802.1x基於埠的身份驗證 — Catalyst 9300
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。