了解Catalyst 9000系列交换机上的意外MAC学习

目录

简介

本文档描述了Catalyst 9300接入交换机在下游端口上获取上游MAC地址的情况。

先决条件

要求

Cisco 建议您了解以下主题：

- LAN 交换
- MAC 地址学习
- 身份验证会话和相关行为

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 9300 系列交换机
- 软件版本17.6.5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

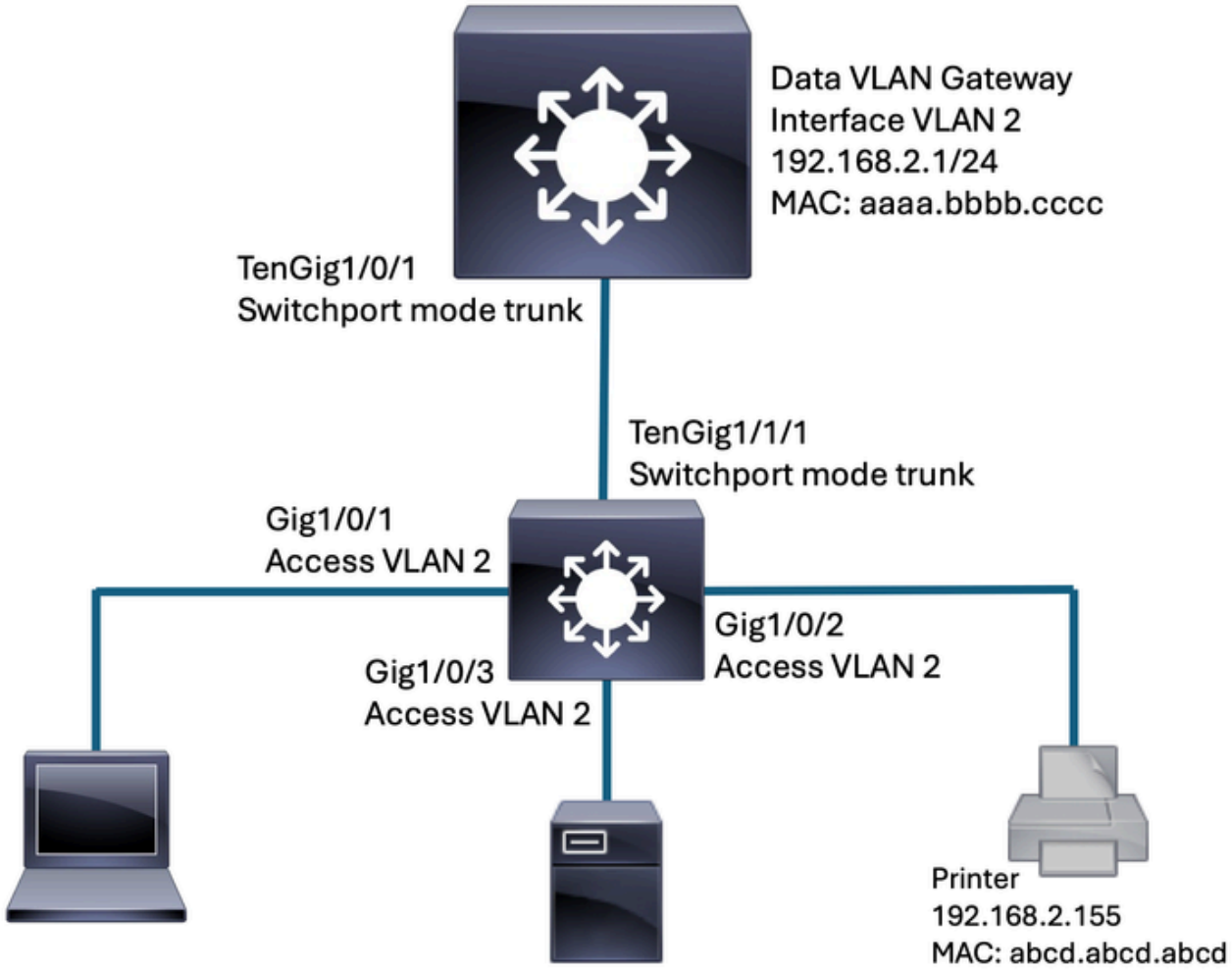
Catalyst交换机根据入站帧的源MAC地址(SMAC)学习交换机端口上的MAC地址。MAC地址表通常是一个可信的信息来源，可引导网络工程师找到指定地址的位置。当来自特定源（终端甚至本地网络的网关）的流量从意外方向进入交换机时，会出现这种情况。本文档描述一种特定情况，其中上游网关MAC地址在随机访问接口上意外获知。详细信息基于由与客户团队合作的TAC工程师解决的TAC案例。

问题

此场景中的客户端首先发现了一个问题，即其数据VLAN（本演示中的VLAN 2）中的终端与其子网外主机的连接断开。在进一步检查后，他们发现VLAN 2网关的MAC地址是在用户界面而非预期接口上获取的。

最初问题似乎随机发生在由多个园区组成的大型网络中。根据我们对交换机学习MAC地址的了解

，我们假设存在某种数据包反射，但困难在于如何证明问题是交换机外部的问题。在收集有关此问题发生的其它时间的其他数据后，我们能够识别出涉及用户端口的趋势。每次发生都涉及到特定的终端模型。



受影响的网络分段

命令“show mac address-table <address>/<interface>”用于查询MAC地址表。在工作或正常情况下，在终端连接的交换机的Ten1/1/1上获取网关地址。

<#root>

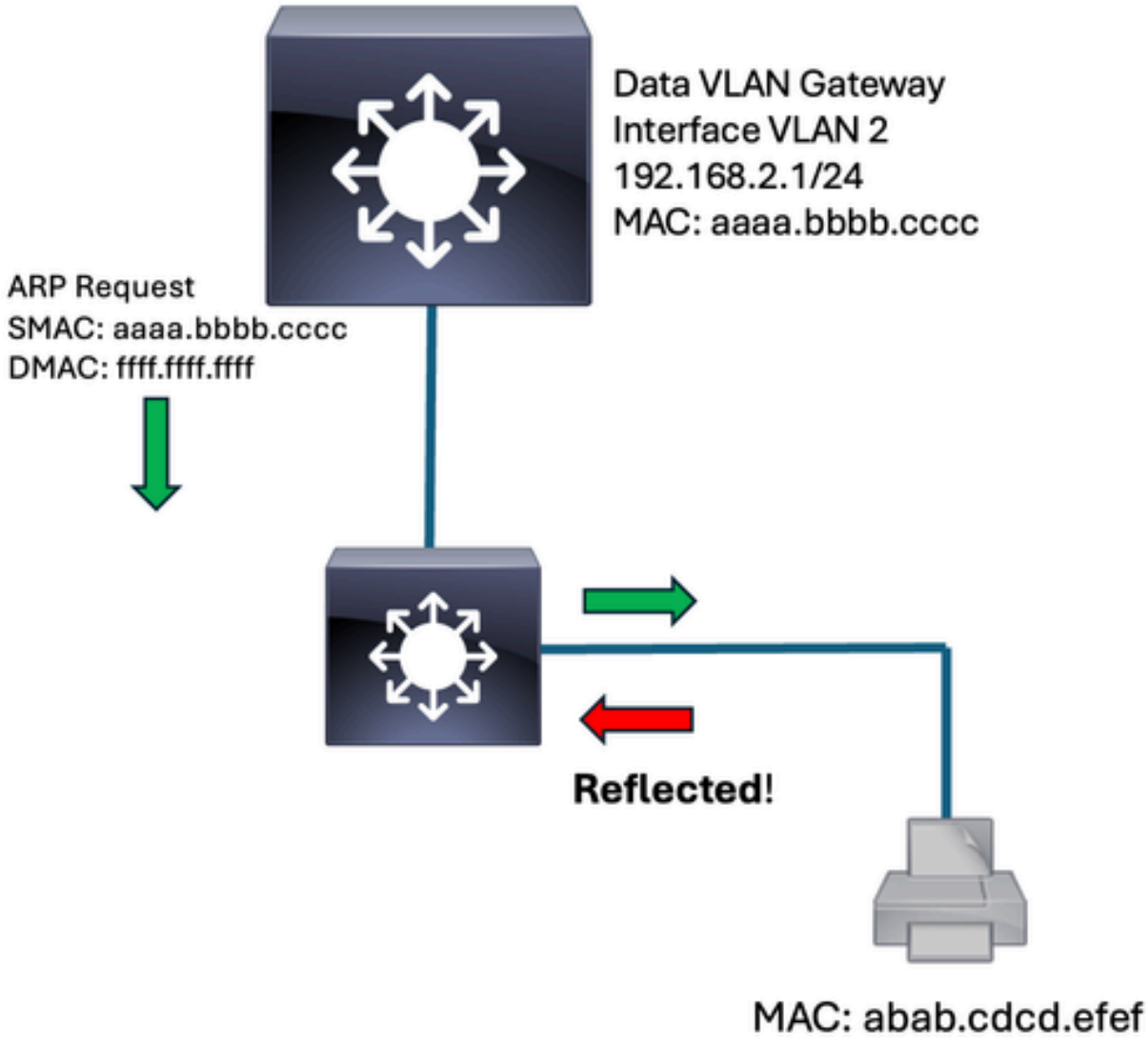
```
ACCESS-SWITCH#

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
```

在故障场景中，网关MAC是在Gi1/0/2上获知的，而不是在Te1/1/1上获知的。

<#root>

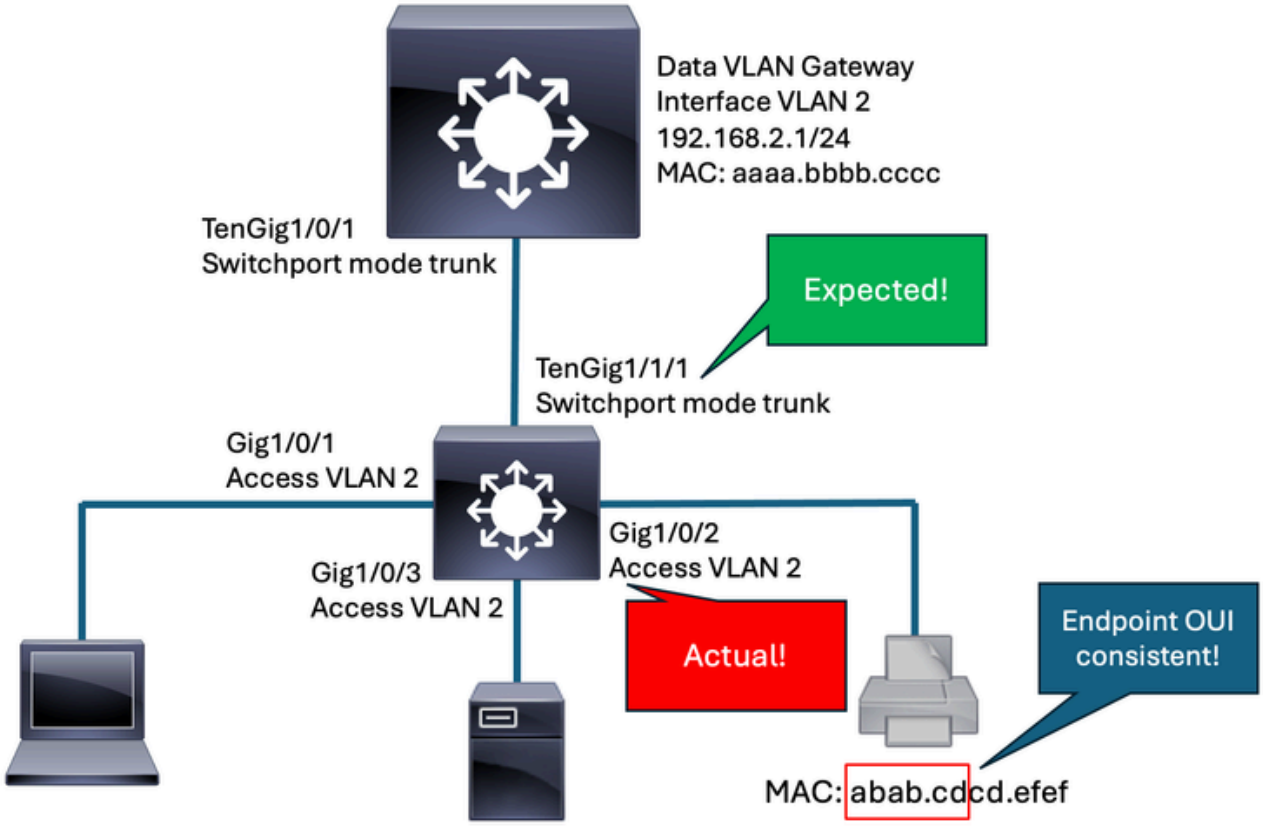
```
ACCESS-SWITCH#

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
```

此场景中的接入交换机在其接入接口上运行带MAB（MAC身份验证绕行）回退的802.1x。这些关键功能在整体服务影响中发挥了作用。一旦在接入端口上获知网关MAC地址，它就会成为安全功能的“静态”功能。 安全功能还阻止了网关MAC地址移回正确的接口。有关802.1x、MAB和“mac-move”概念的信息将在相关配置指南中进一步探讨。



反射流量的演示

数据包反射导致MAC学习异常。



下图突出显示学习GW MAC的预期接口与实际接口。

示例突出显示组织唯一标识符(OUI)。 这帮助团队确定该终端属于一家通用制造商。

解决方案

此问题的核心是终端的意外行为。我们从未期望终端将流量反映回网络。

此案例的关键发现是终端趋势。对大型网络中随机出现的问题很难进行故障排除。这为该团队提供了要仔细检查的用户端口子集。

另请注意，涉及的安全功能（即带MAB回退的dot1x）在服务影响中发挥了作用。如果没有这些功能对反映的流量做出响应，对服务的影响可能就不会那么大。

利用数据包捕获工具来识别流量是否真正被终端反映。 Catalyst交换机上提供的嵌入式数据包捕获(EPC)工具可用于识别入站数据包。

```
<#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
```

物理SPAN（交换机端口分析器）是一个可靠的数据包捕获工具，也可用于此场景。

```
<#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
```

该团队能够捕获可疑终端连接的端口上的反射流量。 在这种情况下，终端会将源自网关MAC地址的ARP数据包反射回交换机端口。启用MAB的交换机端口将尝试对网关MAC地址进行身份验证。交换机端口安全实施允许网关MAC在数据VLAN中进行授权。由于MAC地址是结合安全功能获取的，因此它将“粘滞”为用户端口上的静态MAC。此外，由于安全实施阻止了授权MAC地址的MAC地址移动，因此交换机无法忘记用户端口上的MAC，并且无法在预期接口上重新学习它。数据包反射与安全实施相加，导致整个本地VLAN的流量受到影响。

事件顺序：

1.在预期接口上获取MAC。这是网络的正常状态。

2.终端将来自网关的流量反映回连接到交换机的端口。

3.由于终端交换机端口安全实施，反映的MAC会触发身份验证会话。MAC被编程为STATIC条目。

4.一旦MAC老化超出预期的交换机端口，安全实施将阻止在上行链路上重新学习它。

5.端口需要关闭/取消关闭才能恢复。

此情况的最终修复方案是解决终端行为。 在此场景中，终端供应商已知道该行为，并且已使用固件更新修复该行为。Catalyst交换机硬件以及软件和配置都完全按照预期运行。

此场景的主要收获是MAC学习的概念。Catalyst交换机根据收到的帧的源MAC地址在入口获取MAC地址。如果在意外的接口上获知MAC地址，可以安全推断交换机端口在入口处收到一个帧，其中源MAC字段中包含该MAC地址。

在非常有限的情况下，数据包可能会在物理接口和交换机的转发ASIC之间反映 — 或通过某些其他内部错误行为反映。如果出现这种情况，并且找不到可以解释此问题的现有Bug，请联系TAC以帮助隔离。

相关信息

- 配置数据包捕获 — Catalyst 9300
- 配置SPAN和RSPAN - Catalyst 9300
- Catalyst 9000系列交换机上的Mac地址表管理器故障排除
- 配置IEEE 802.1x基于端口的身份验证 — Catalyst 9300
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。