Comprendre l'apprentissage MAC inattendu sur les commutateurs de la gamme Catalyst 9000

Table des matières

Introduction

Ce document décrit un scénario où un commutateur d'accès Catalyst 9300 apprenait une adresse MAC en amont sur un port en aval.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Commutation LAN
- Apprentissage des adresses MAC
- Sessions d'authentification et comportement associé

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs de la gamme Cisco Catalyst 9300
- Version logicielle 17.6.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

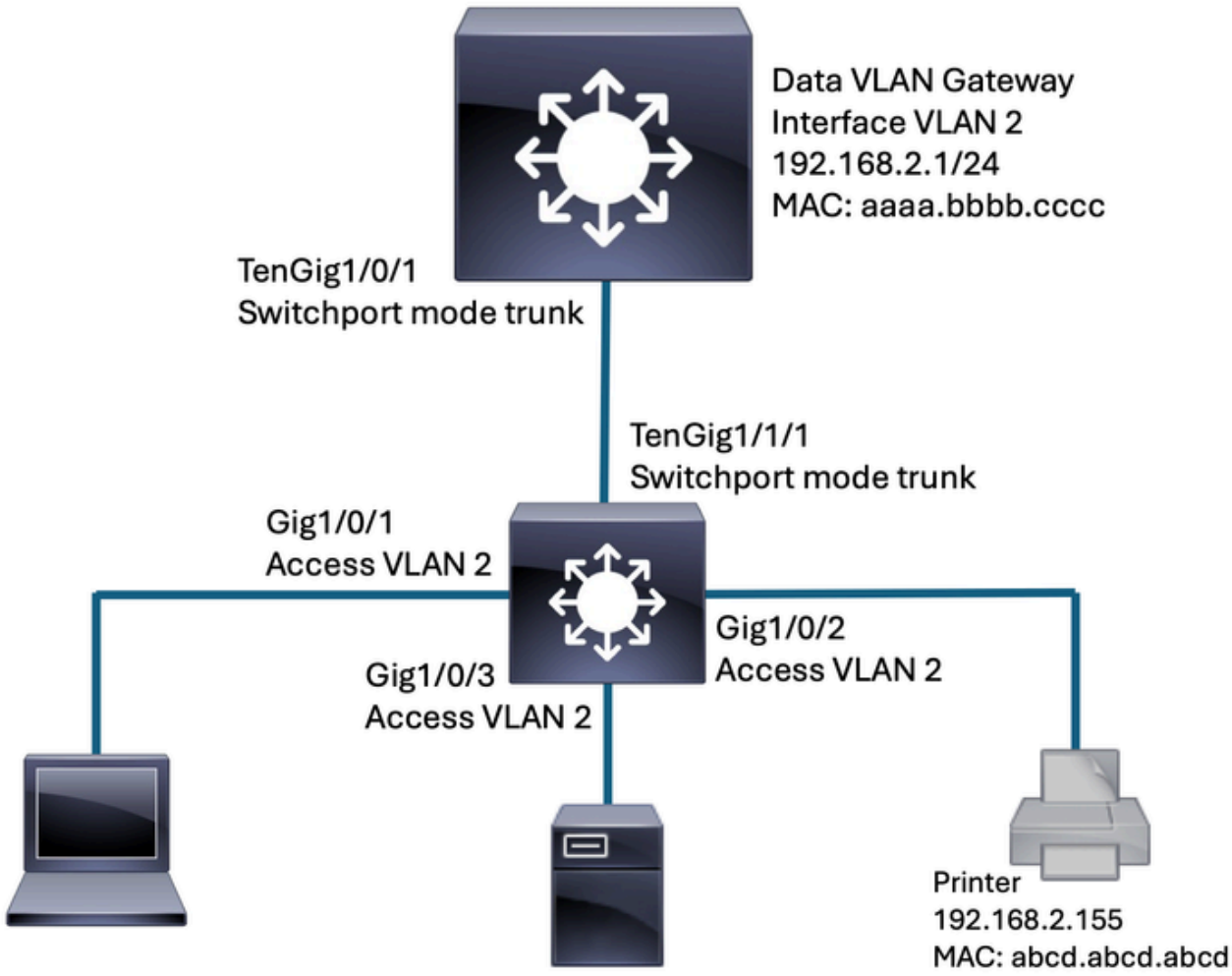
Les commutateurs Catalyst apprennent les adresses MAC sur les ports des commutateurs en fonction de l'adresse MAC source (SMAC) d'une trame entrante. La table d’adresses MAC est généralement une source d’informations fiable qui guide un ingénieur réseau vers l’emplacement d’une adresse donnée. Il arrive que le trafic provenant d’une source particulière (un point d’extrémité ou même la passerelle du réseau local) entre dans un commutateur à partir d’une direction inattendue. Ce document décrit une situation spécifique où l'adresse MAC de la passerelle en amont a été apprise de manière inattendue sur des interfaces d'accès aléatoire. Les détails sont basés sur des cas de TAC résolus par des ingénieurs du TAC travaillant en

partenariat avec des équipes de clients.

Problème

Dans ce scénario, le client a d'abord remarqué le problème lorsque les points d'extrémité de leur VLAN de données (VLAN 2 dans cette démonstration) ont perdu la connectivité avec les hôtes en dehors de leur sous-réseau. Après une inspection plus approfondie, ils ont observé que l'adresse MAC de la passerelle VLAN 2 a été apprise sur une interface utilisateur plutôt que sur l'interface attendue.

Au départ, le problème semblait se produire de manière aléatoire dans un grand réseau composé de plusieurs campus. Compte tenu de ce que nous savons sur la façon dont les commutateurs apprennent les adresses MAC, nous avons supposé une sorte de réflexion de paquets, mais le défi était de prouver que le problème était externe au commutateur. Après avoir collecté des données supplémentaires sur d'autres occurrences de ce problème, nous avons pu identifier une tendance avec les ports utilisateur concernés. Un modèle précis de critère d'effet a été utilisé dans chaque cas.



Segment du réseau affecté

La commande « show mac address-table <address>/<interface> » est utilisée pour interroger la table d'adresses MAC. Dans le scénario de fonctionnement normal, l'adresse de la passerelle est apprise sur Ten1/1/1 du commutateur auquel les points d'extrémité se connectent.

<#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
```

Dans le scénario interrompu, l'adresse MAC de la passerelle a été apprise sur Gi1/0/2 et non sur Te1/1/1.

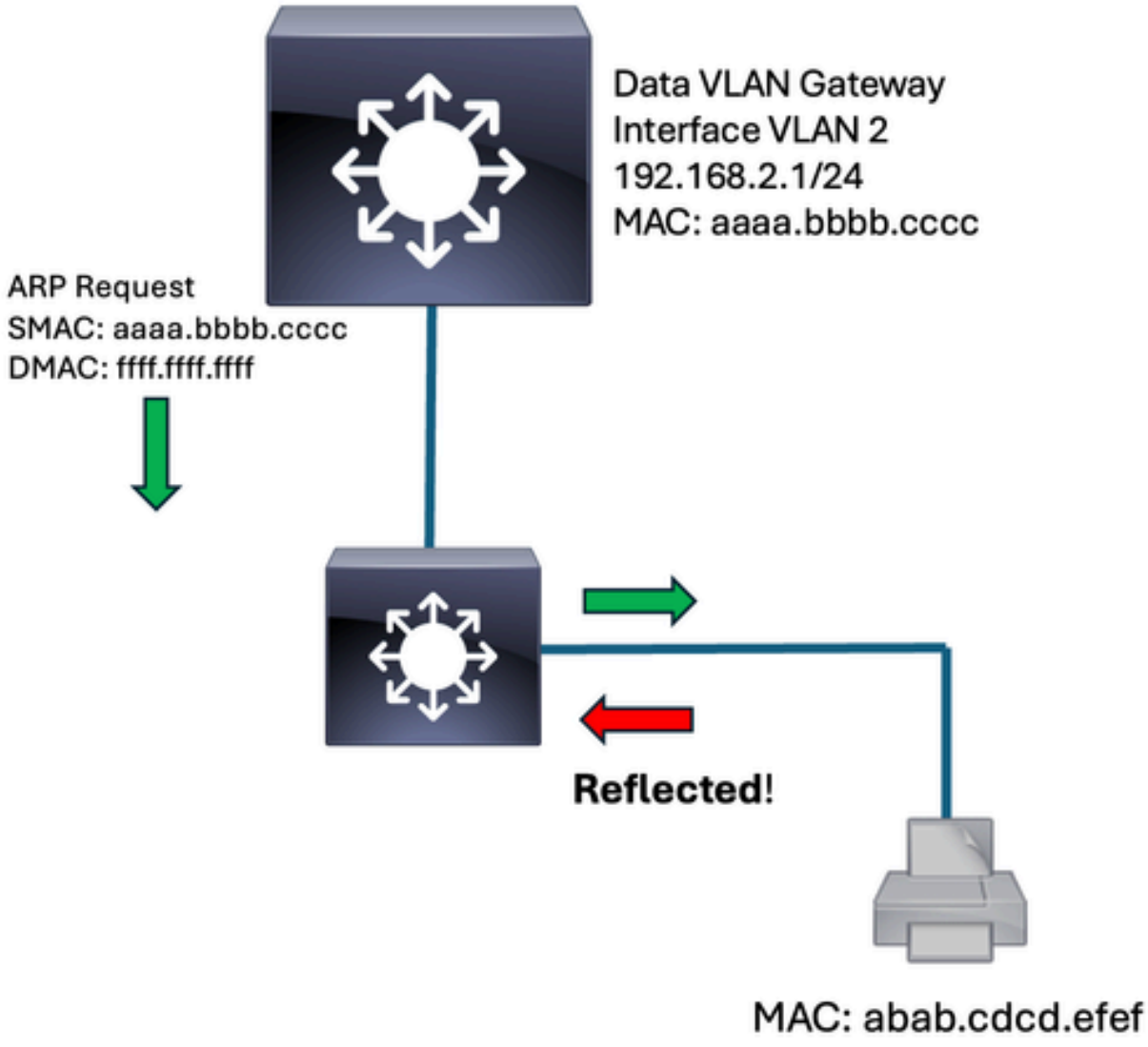
<#root>

```
ACCESS-SWITCH#
```

show mac address-table

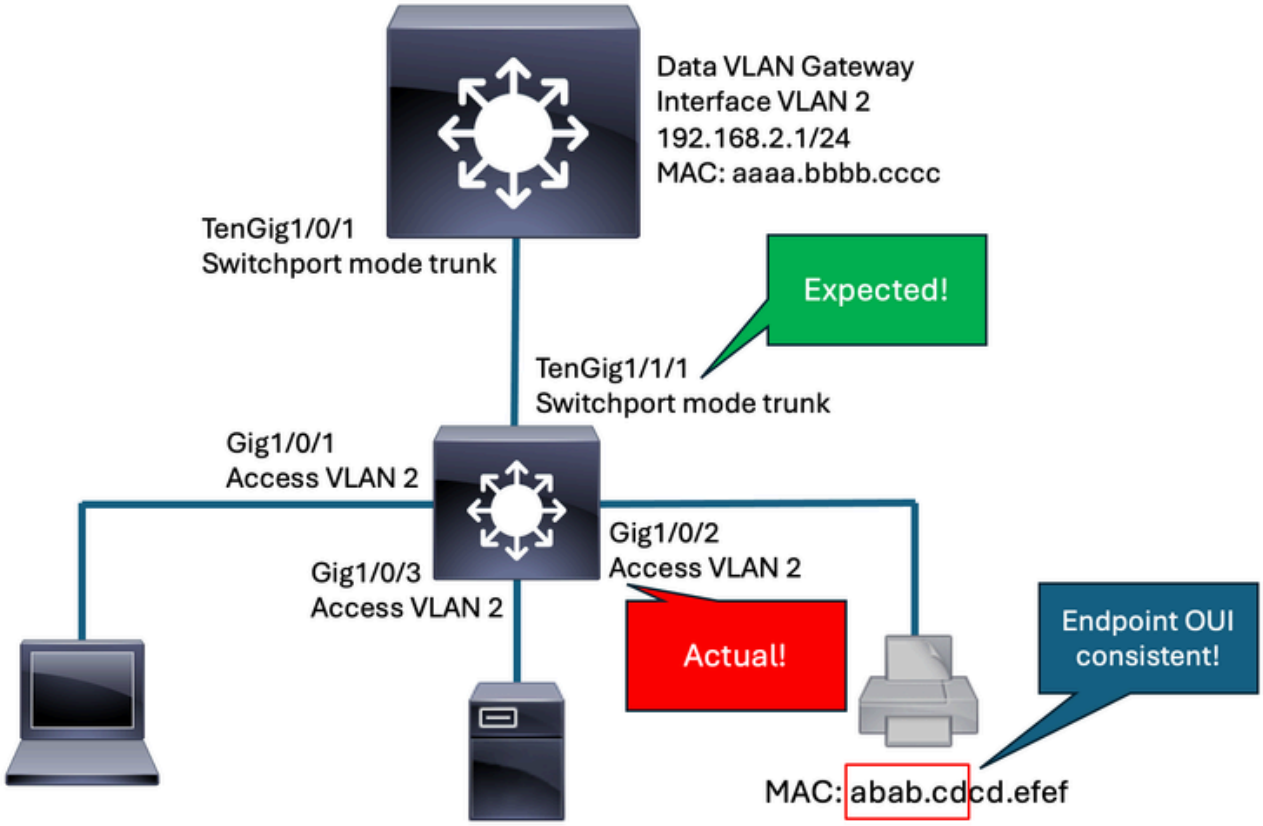
```
          Mac Address Table
-------------------------------------------

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
```

Dans ce scénario, le commutateur d'accès exécute la norme 802.1x avec le mode de secours MAB (MAC authentication bypass) sur ses interfaces d'accès. Ces fonctionnalités clés ont joué un rôle dans l'impact global du service. Une fois l'adresse MAC de la passerelle apprise sur un port d'accès, elle devient « statique » en fonction de la fonction de sécurité. La fonctionnalité de sécurité a également empêché l'adresse MAC de la passerelle de revenir à l'interface correcte. Des informations sur 802.1x, MAB et le concept de « mac-move » sont détaillées dans le guide de configuration approprié.



Démonstration du trafic réfléchi

La réflexion du paquet entraîne l'apprentissage MAC anormal.



Ce schéma met en évidence l'interface attendue par rapport à l'interface réelle qui apprend l'adresse MAC GW.

L'exemple met en évidence l'identifiant unique d'organisation (OUI). Cela a permis à l'équipe de déterminer que le terminal était d'un fabricant courant.

Solution

Le comportement inattendu du point d'extrémité est au coeur de ce problème. Nous ne nous attendons jamais à ce qu'un terminal reflète le trafic sur le réseau.

La principale conclusion dans ce cas était la tendance avec les terminaux. Il est difficile de résoudre un problème qui se produit de manière aléatoire sur un réseau de grande taille. Cela a permis à l'équipe d'obtenir un sous-ensemble de ports utilisateur à analyser.

Notez également que les fonctions de sécurité impliquées, à savoir dot1x avec MAB fallback, ont joué un rôle dans l'impact du service. Sans ces fonctionnalités répondant au trafic reflété, l'impact sur le service n'aurait probablement pas été aussi important.

Des outils de capture de paquets ont été utilisés pour identifier que le trafic était réellement reflété par le terminal. L'outil de capture de paquets intégré (EPC) disponible sur les commutateurs Catalyst peut être utilisé pour identifier les paquets entrants.

<#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
```

La fonctionnalité physique SPAN (Analyseur de port de commutateur) est un outil de capture de paquets fiable qui peut également être utilisé dans ce scénario.

<#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
```

L'équipe a pu capturer le trafic réfléchi sur un port auquel un point d'extrémité suspect était connecté. Dans ce scénario, le point d'extrémité refléterait les paquets ARP provenant de l'adresse MAC de la passerelle vers le port du commutateur. Le port de commutateur compatible MAB tente d'authentifier l'adresse MAC de la passerelle. La mise en oeuvre de la sécurité du port de commutateur a permis à l'adresse MAC de la passerelle d'autoriser dans le VLAN de données. Comme l'adresse MAC a été apprise en conjonction avec la fonction de sécurité, elle « reste » en tant qu'adresse MAC STATIQUE sur le port utilisateur. En outre, comme la mise en oeuvre de la sécurité bloquait le déplacement des adresses MAC autorisées, le commutateur n'a pas pu oublier l'adresse MAC sur le port utilisateur et n'a pas pu la réapprendre sur l'interface attendue. La réflexion des paquets associée à la mise en oeuvre de la sécurité a entraîné une situation où le trafic a été affecté pour l'ensemble du VLAN local.

Séquence des événements :

1. Les adresses MAC sont acquises sur les interfaces attendues. Il s’agit de l’état normal du réseau.

2. Le point d’extrémité reflète le trafic provenant de la passerelle vers le port qui se connecte au commutateur.

3. En raison de la mise en oeuvre de la sécurité du port de commutateur du point d’extrémité, l’adresse MAC reflétée déclenche une session d’authentification. L'adresse MAC est programmée en tant qu'entrée STATIC.

4. Une fois que l’adresse MAC a expiré sur le port de commutateur attendu, l’implémentation de la sécurité empêche qu’elle soit apprise à nouveau sur la liaison ascendante.

5. Le port doit être fermé/défermé pour pouvoir être restauré.

La solution ultime à cette situation était de traiter le comportement des terminaux. Dans ce scénario, le comportement était déjà connu du fournisseur du terminal et a été corrigé par une mise à jour du micrologiciel. Le matériel du commutateur Catalyst, ainsi que le logiciel et la configuration se comportaient entièrement comme prévu.

Le principal enseignement de ce scénario est le concept d’apprentissage MAC. Les commutateurs Catalyst apprennent les adresses MAC en entrée en fonction de l’adresse MAC source de la trame reçue. Si une adresse MAC est apprise sur une interface inattendue, il est raisonnable de conclure que le port du commutateur a reçu une trame en entrée avec cette adresse MAC dans le champ MAC source.

Dans des situations très limitées, les paquets peuvent être reflétés entre l'interface physique et l'ASIC de transfert du commutateur, ou par un autre comportement inapproprié interne. Si tel est le cas et qu'aucun bogue n'explique le problème, contactez le TAC pour vous aider à l'isoler.

Informations connexes

- Configuration de la capture de paquets - Catalyst 9300
- Configuration des fonctions SPAN et RSPAN - Catalyst 9300
- Dépannage du Gestionnaire de tables d'adresses Mac sur les commutateurs de la gamme Catalyst 9000
- Configuration de l'authentification basée sur les ports IEEE 802.1x - Catalyst 9300
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.