Erfahren Sie mehr über die unerwarteten Vorteile von MAC Learning auf Catalyst Switches der Serie 9000

Inhalt

Einleitung

In diesem Dokument wird ein Szenario beschrieben, in dem ein Catalyst 9300 Access Switch eine Upstream-MAC-Adresse an einem Downstream-Port lernte.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- LAN-Switching
- MAC-Adresslernen
- Authentifizierungssitzungen und zugehöriges Verhalten

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Switches der Cisco Catalyst 9300-Serie
- Softwareversion 17.6.5

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

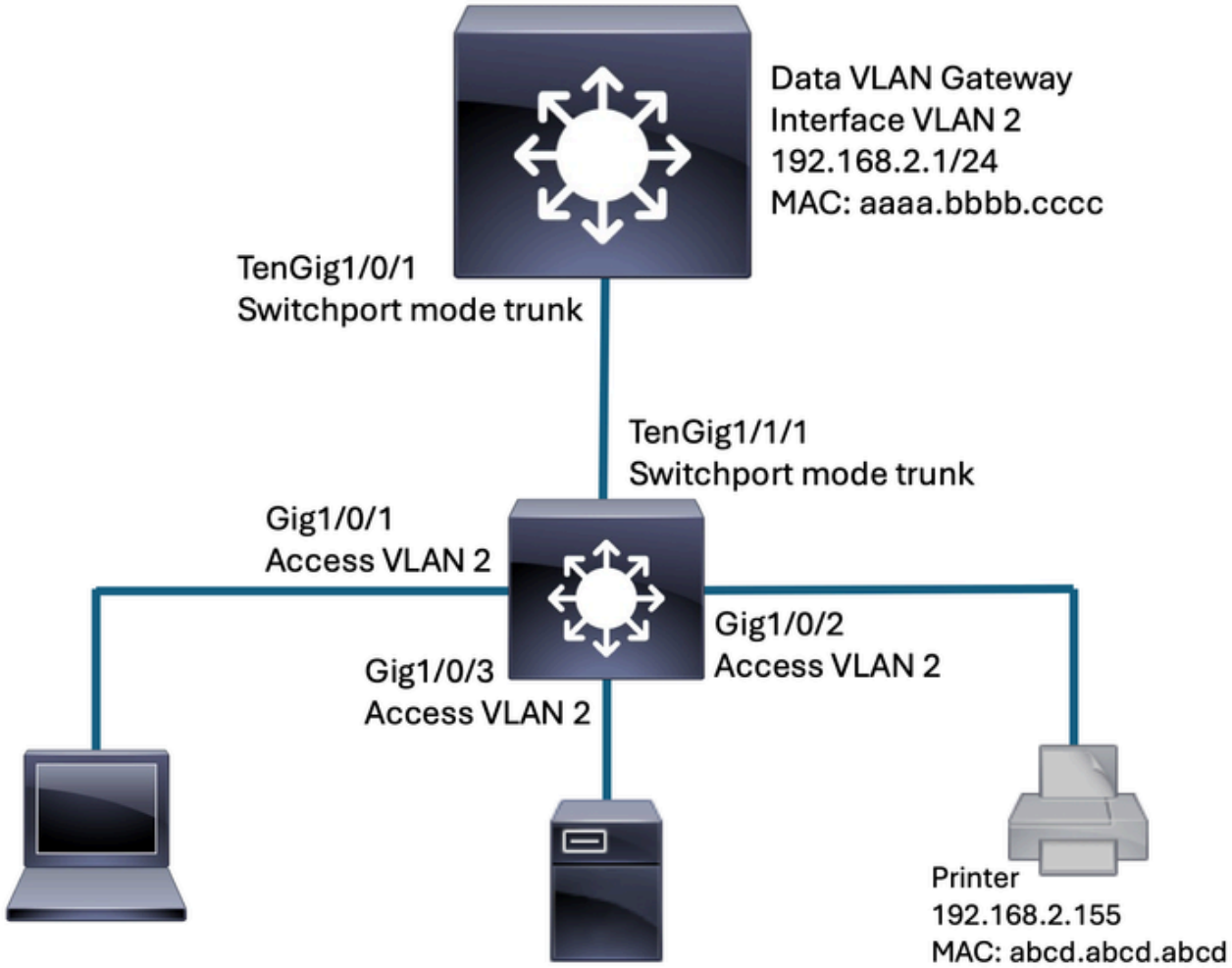
Catalyst Switches erfassen MAC-Adressen an Switch-Ports basierend auf der Quell-MAC-Adresse (SMAC) eines eingehenden Frames. Die MAC-Adresstabelle ist in der Regel eine vertrauenswürdige Informationsquelle, die einen Netzwerktechniker zum Standort einer bestimmten Adresse führt. Situationen entstehen, in denen Datenverkehr von einer bestimmten Quelle - einem Endpunkt oder sogar dem Gateway des lokalen Netzwerks - aus einer

unerwarteten Richtung in einen Switch gelangt. In diesem Dokument wird eine spezielle Situation beschrieben, in der die MAC-Adresse des Upstream-Gateways unerwartet an Schnittstellen mit wahlfreiem Zugriff erfasst wurde. Die Details basieren auf TAC-Fällen, die von TAC-Technikern in Zusammenarbeit mit Kundenteams gelöst wurden.

Problem

In diesem Szenario stellte der Client das Problem zuerst fest, als die Endpunkte in ihrem Daten-VLAN (in dieser Demonstration VLAN 2) die Verbindung zu Hosts außerhalb ihres Subnetzes verloren. Bei einer weiteren Überprüfung stellten sie fest, dass die MAC-Adresse des VLAN 2-Gateways nicht auf der erwarteten Schnittstelle, sondern auf einer Benutzeroberfläche erfasst wurde.

Das Problem schien zunächst nach dem Zufallsprinzip in einem großen Netzwerk mehrerer Campus zu passieren. Auf der Grundlage unseres Wissens über die Erfassung der MAC-Adressen durch die Switches gingen wir von einer Paketspiegelung aus. Die Herausforderung bestand jedoch darin, zu beweisen, dass sich das Problem nicht auf den Switch bezog. Nachdem wir zusätzliche Daten zu anderen Zeitpunkten gesammelt hatten, zu denen dieses Problem aufgetreten war, konnten wir einen Trend bei den beteiligten Benutzerports identifizieren. Bei jedem Vorfall wurde ein bestimmtes Endgerätemodell einbezogen.



Segment des betroffenen Netzwerks

Der Befehl "show mac address-table <Adresse>/<Schnittstelle>" wird zum Abfragen der MAC-Adresstabelle verwendet. Im funktionierenden oder normalen Szenario wird die Gateway-Adresse auf Ten1/1/1 des Switches gelernt, mit dem die Endpunkte eine Verbindung herstellen.

<#root>

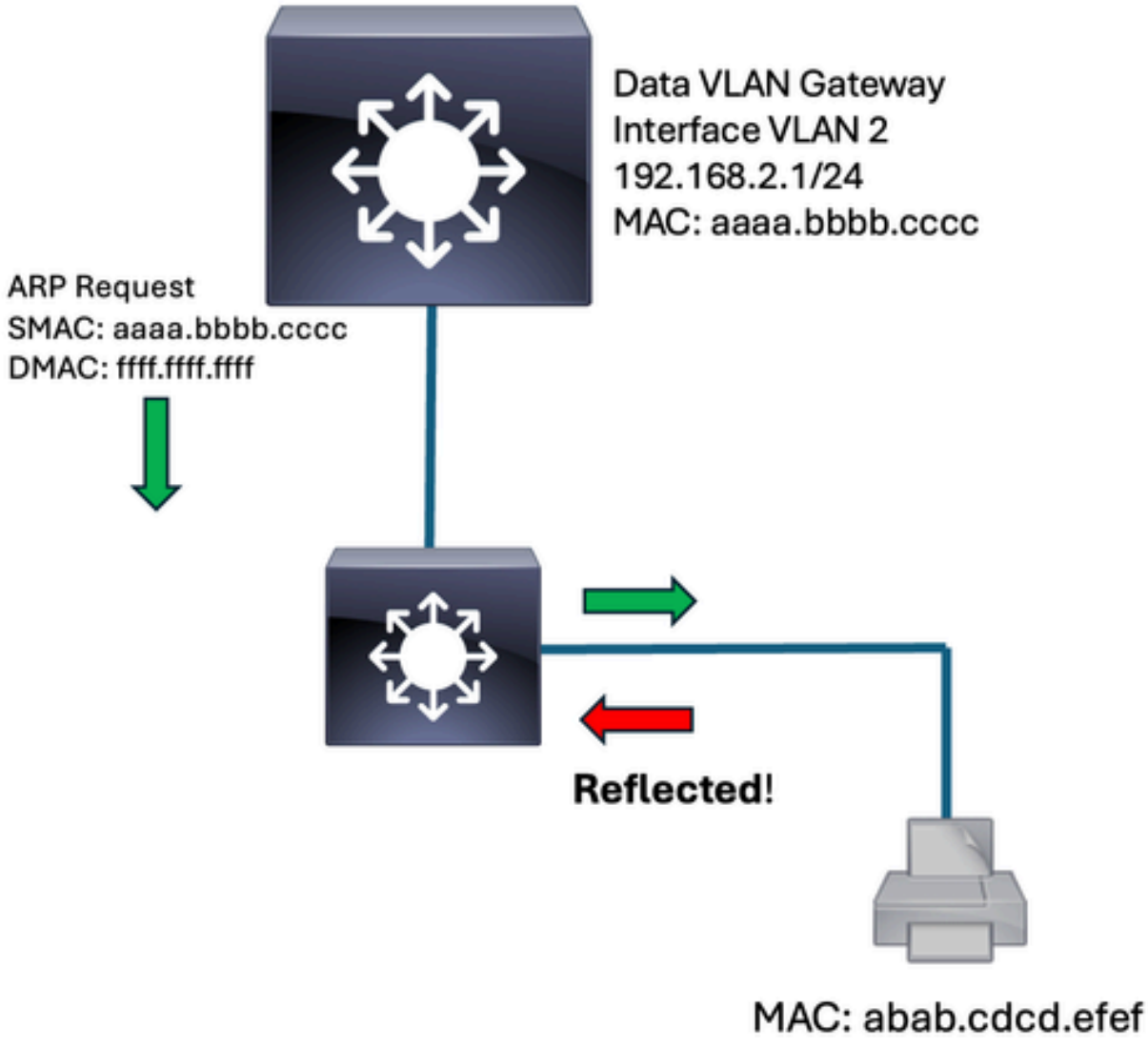
```
ACCESS-SWITCH#

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
```

Bei einem defekten Szenario wurde die Gateway-MAC auf Gi1/0/2 und nicht auf Te1/1/1 erfasst.

<#root>

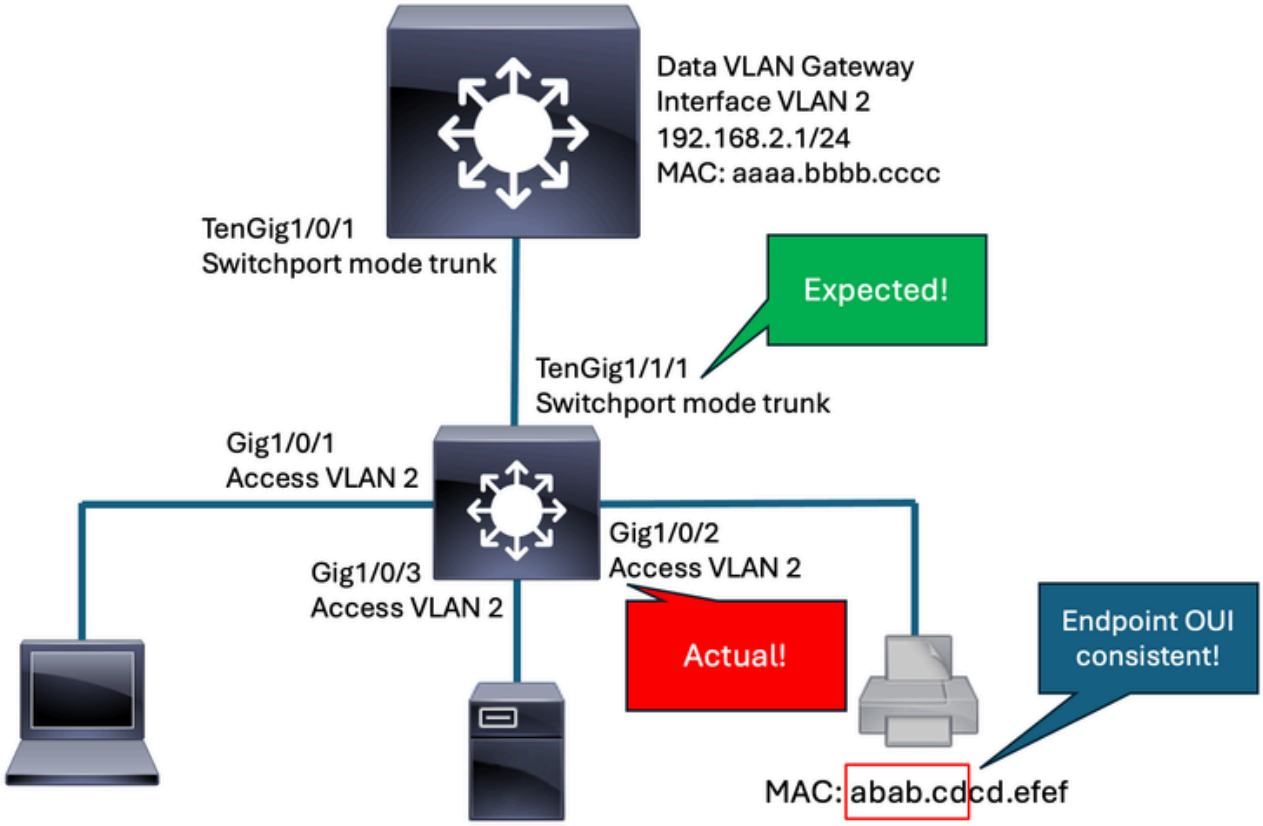
```
ACCESS-SWITCH#

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 diesem Szenario führt der Access Switch 802.1x mit MAB-Fallback (MAC Authentication Bypass) an seinen Zugriffsschnittstellen aus. Diese wichtigen Funktionen spielten bei den Auswirkungen auf den Service insgesamt eine Rolle. Sobald die Gateway-MAC-Adresse an einem Access-Port abgefragt wurde, wurde sie abhängig von der Sicherheitsfunktion statisch. Aufgrund der Sicherheitsfunktion konnte die Gateway-MAC-Adresse nicht zur richtigen Schnittstelle zurückverschoben werden. Weitere Informationen zu 802.1x, MAB und dem Konzept von "mac-move" finden Sie im entsprechenden Konfigurationsleitfaden.



Nachweis von reflektiertem Datenverkehr

Die Paketreflexion führt zu den abnormalen MAC-Lesevorgängen.



In diesem Diagramm wird die erwartete bzw. tatsächliche Schnittstelle hervorgehoben, die die GW-MAC-Adresse erfasst.

Im Beispiel wird der Organizational Unique Identifier (OUI) hervorgehoben. So konnte das Team feststellen, dass das Endgerät von einem gemeinsamen Hersteller stammte.

Lösung

Der Kern dieses Problems war das unerwartete Verhalten des Endpunkts. Wir erwarten niemals, dass ein Endgerät den Datenverkehr zurück in das Netzwerk reflektiert.

Die wichtigste Erkenntnis in diesem Fall war der Trend zu den Endgeräten. Es ist schwierig, ein Problem zu beheben, das in einem großen Netzwerk nach dem Zufallsprinzip auftritt. Das Team erhielt so eine Teilmenge der Benutzerports, die überprüft werden musste.

Beachten Sie außerdem, dass die beteiligten Sicherheitsfunktionen - dot1x mit MAB-Fallback - eine Rolle bei den Auswirkungen auf den Service spielten. Wenn diese Funktionen nicht auf den reflektierten Datenverkehr reagieren, wären die Auswirkungen auf den Service wahrscheinlich geringer ausgefallen.

Mithilfe von Paketerfassungstools wurde festgestellt, dass der Datenverkehr tatsächlich vom Endpunkt reflektiert wurde. Das Embedded Packet Capture (EPC)-Tool auf Catalyst Switches kann zur Identifizierung eingehender Pakete verwendet werden.

<#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 (Switch Port Analyzer) ist ein zuverlässiges Tool zur Paketerfassung, das ebenfalls in diesem Szenario verwendet werden kann.

<#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
```

Das Team war in der Lage, den reflektierten Datenverkehr an einem Port zu erfassen, an den ein verdächtiger Endpunkt angeschlossen war. In diesem Szenario spiegelt der Endpunkt ARP-Pakete wider, die von der Gateway-MAC-Adresse zurück an den Switch-Port gesendet wurden. Der MAB-fähige Switch-Port versucht, die Gateway-MAC-Adresse zu authentifizieren. Die Implementierung der Switch-Port-Sicherheit ermöglichte die Autorisierung der Gateway-MAC im Daten-VLAN. Da die MAC-Adresse in Verbindung mit der Sicherheitsfunktion ermittelt wurde, würde sie sich als STATIC MAC (statische MAC-Adresse) am Benutzerport "festhalten". Da die Sicherheitsimplementierung die Verschiebung von MAC-Adressen autorisierter MAC-Adressen blockierte, konnte der Switch die MAC-Adresse auf dem Benutzerport nicht vergessen und konnte sie nicht auf der erwarteten Schnittstelle neu lernen. Die Paketreflexion und die

Sicherheitsimplementierung führten zu einer Situation, in der der Datenverkehr für das gesamte lokale VLAN beeinträchtigt war.

Reihenfolge der Ereignisse:

1. MACs werden an den erwarteten Schnittstellen erfasst. Dies ist der Normalzustand des Netzwerks.

2. Der Endpunkt reflektiert den Datenverkehr vom Gateway zurück in den Port, der mit dem Switch verbunden ist.

3. Aufgrund der Sicherheitsimplementierung des Endpunkt-Switch-Ports löst die reflektierte MAC-Adresse eine Authentifizierungssitzung aus. Die MAC-Adresse ist als STATIC-Eintrag programmiert.

4. Wenn die MAC-Adresse außerhalb des erwarteten Switch-Ports liegt, verhindert die Sicherheitsimplementierung das erneute Erfassen der Adresse über den Uplink.

5. Der Port muss zum Wiederherstellen ausgeschaltet/wieder freigegeben werden.

Die endgültige Lösung für diese Situation war das Verhalten des Endgeräts. In diesem Szenario war das Verhalten dem Endgerätehersteller bereits bekannt und wurde mit einem Firmware-Update behoben. Sowohl die Hardware als auch die Software und Konfiguration der Catalyst Switches verhielten sich wie erwartet.

Die wichtigste Erkenntnis aus diesem Szenario ist das Konzept des MAC Learning. Catalyst Switches erfassen MAC-Adressen beim Eingang basierend auf der Quell-MAC-Adresse des empfangenen Frames. Wenn eine MAC-Adresse an einer unerwarteten Schnittstelle erkannt wird, kann mit Sicherheit der Schluss gezogen werden, dass der Switch-Port am Eingang ein Frame mit dieser MAC-Adresse im Quell-MAC-Feld empfangen hat.

In sehr eingeschränkten Situationen können Pakete zwischen der physischen Schnittstelle und dem weiterleitenden ASIC des Switches gespiegelt werden - oder durch ein anderes internes Fehlverhalten. Wenn dies der Fall zu sein scheint und kein vorhandener Fehler gefunden wird, der das Problem erklärt, wenden Sie sich an das TAC, um bei der Isolierung zu helfen.

Zugehörige Informationen

- Konfigurieren der Paketerfassung - Catalyst 9300
- Konfigurieren von SPAN und RSPAN - Catalyst 9300
- Fehlerbehebung bei MAC Address Table Manager auf Catalyst Switches der Serie 9000
- Konfigurieren der portbasierten IEEE 802.1x-Authentifizierung - Catalyst 9300
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.