Catalyst 9000 Series 스위치에서 예상치 못한 MAC 학습 이해

목차

소개

이 문서에서는 Catalyst 9300 액세스 스위치가 다운스트림 포트에서 업스트림 MAC 주소를 학습하는 시나리오를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LAN 스위칭
- MAC 주소 학습
- 인증 세션 및 관련 동작

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 9300 Series 스위치
- 소프트웨어 버전 17.6.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

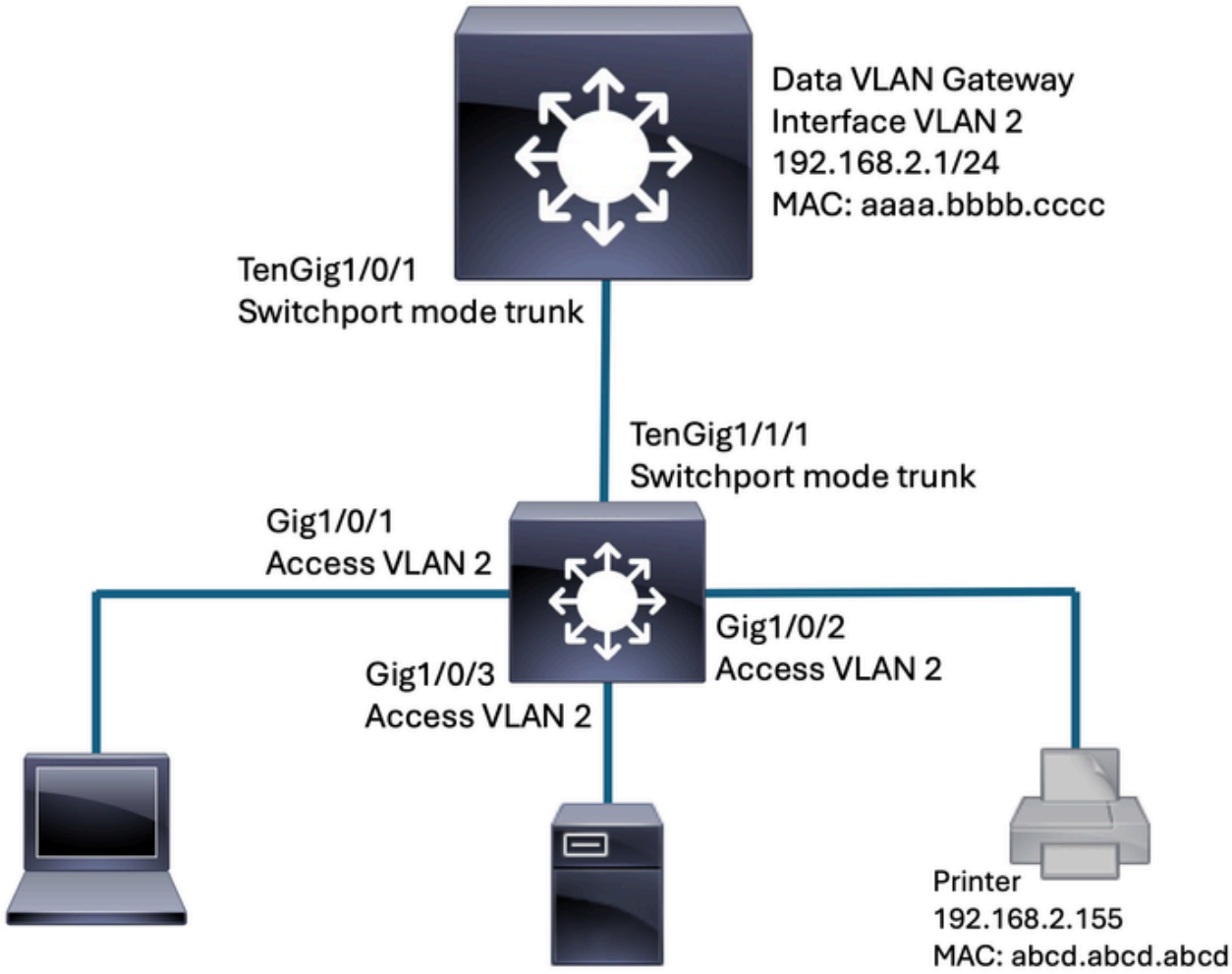
배경 정보

Catalyst 스위치는 인바운드 프레임의 소스 MAC 주소(SMAC)를 기반으로 스위치 포트에서 MAC 주소를 학습합니다. MAC 주소 테이블은 일반적으로 네트워크 엔지니어를 특정 주소의 위치로 안내하는 신뢰할 수 있는 정보 소스입니다. 특정 소스(엔드포인트 또는 로컬 네트워크의 게이트웨이)의 트래픽이 예기치 않은 방향에서 스위치를 가져오는 상황이 발생합니다. 이 문서에서는 업스트림 게이트웨이 MAC 주소가 임의 액세스 인터페이스에서 예기치 않게 학습된 특정 상황에 대해 설명합니다. 세부 정보는 고객 팀과 협력하는 TAC 엔지니어가 해결한 TAC 사례를 기반으로 합니다.

문제

이 시나리오의 클라이언트는 데이터 VLAN(이 데모의 VLAN 2)에 있는 엔드포인트가 서브넷 외부의 호스트에 대한 연결이 끊길 때 문제를 처음 발견했습니다. 추가 검사 결과, VLAN 2 게이트웨이의 MAC 주소가 예상 인터페이스가 아닌 사용자 인터페이스에서 학습된 것을 확인했습니다.

이 문제는 처음에 여러 캠퍼스로 구성된 대규모 네트워크에서 무작위로 발생한 것으로 나타났습니다. 스위치가 MAC 주소를 학습하는 방법에 대해 알고 있는 정보를 감안할 때, 패킷 반사를 가정했지만 문제는 스위치 외부에 문제가 있다는 것을 입증하는 것이었습니다. 이 문제가 발생한 다른 시간에 대한 추가 데이터를 수집한 후, 관련된 사용자 포트에 대한 추세를 파악할 수 있었습니다. 특정 엔드포인트 모델이 모든 상황에 포함되었습니다.



영향을 받는 네트워크의 세그먼트

"show mac address-table <address>/<interface>" 명령은 MAC 주소 테이블을 쿼리하는 데 사용됩니다. 정상 작동 시나리오에서는 엔드포인트가 연결되는 스위치의 10/1/1에 게이트웨이 주소가 학습됩니다.

<#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
```

깨진 시나리오에서 게이트웨이 MAC는 Te1/1/1이 아니라 Gi1/0/2에서 학습되었습니다.

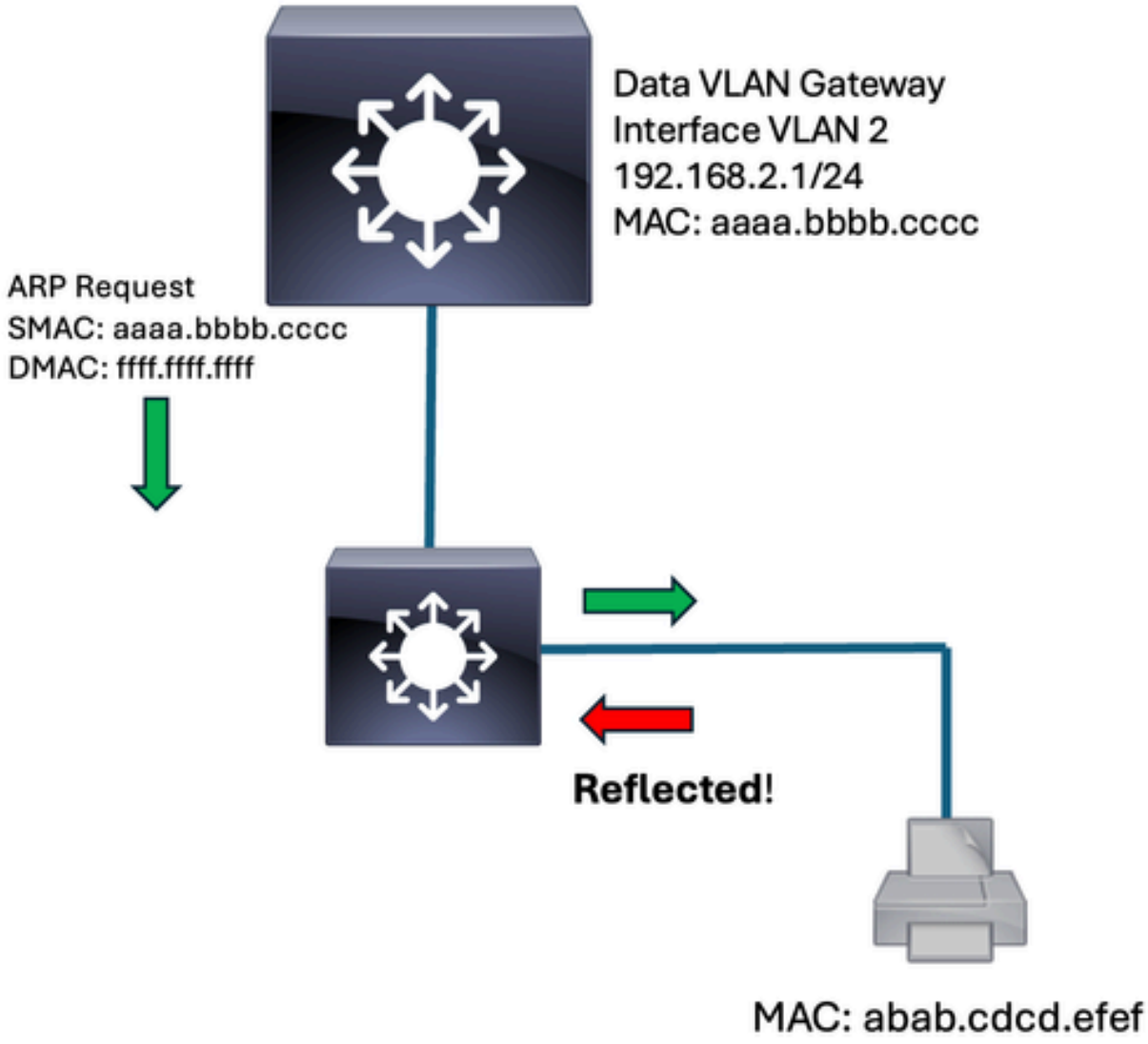
<#root>

ACCESS-SWITCH#

show mac address-table

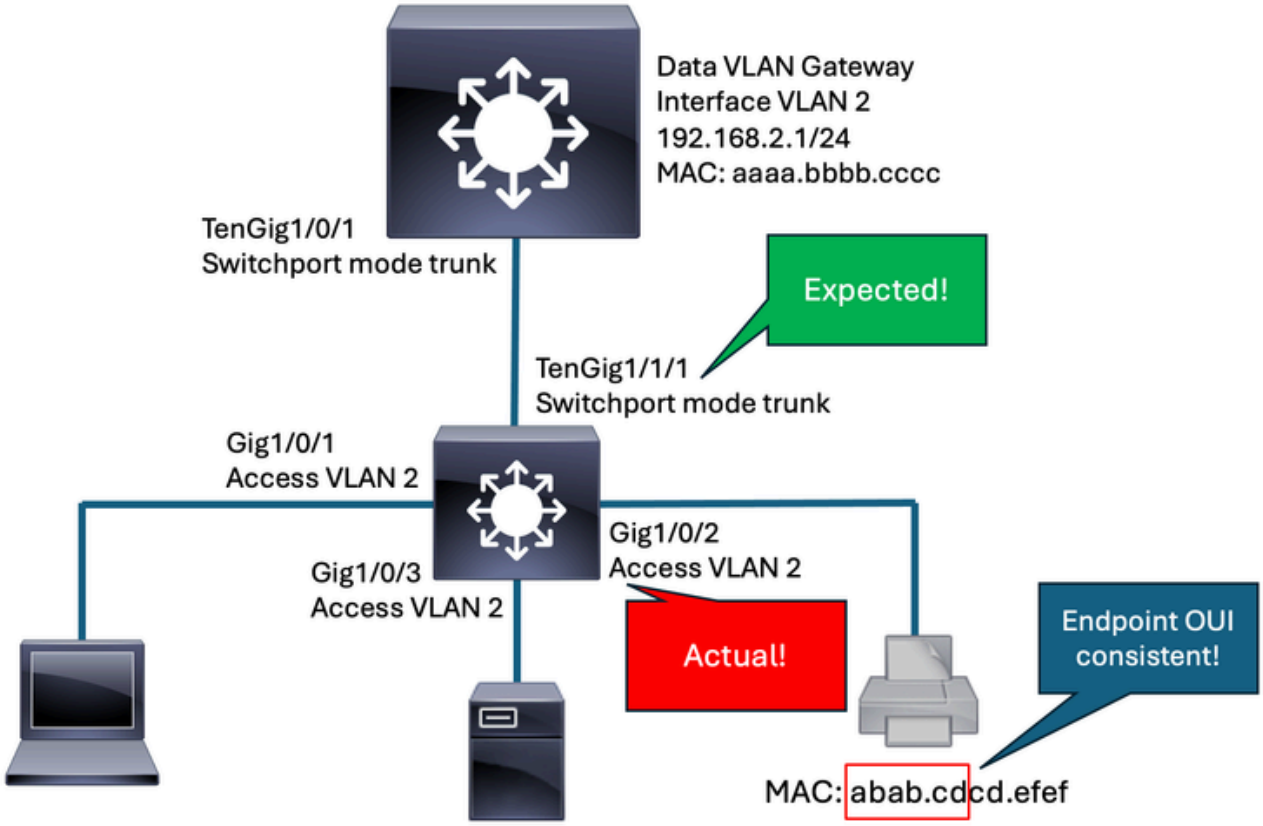
```
          Mac Address Table
-------------------------------------------

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
```

이 시나리오의 액세스 스위치는 액세스 인터페이스에서 MAB(MAC 인증 우회) 폴백으로 802.1x를 실행합니다. 이러한 주요 기능은 전반적인 서비스 영향에서 한 몫을 했습니다. 게이트웨이 MAC 주소가 액세스 포트에서 학습되면 보안 기능의 기능으로 '고정'이 됩니다. 또한 보안 기능으로 인해 게이트웨이 MAC 주소가 올바른 인터페이스로 다시 이동하지 못했습니다. 802.1x, MAB 및 'mac-move'의 개념에 대한 정보는 관련 컨피그레이션 가이드에서 자세히 살펴봅니다.



반영된 트래픽 데모

패킷 반영은 비정상적인 MAC 학습으로 이어집니다.



이 다이어그램은 GW MAC를 학습하는 예상 인터페이스와 실제 인터페이스를 보여줍니다.

이 예에서는 OUI(Organizational Unique Identifier)를 강조 표시합니다. 이를 통해 팀은 엔드포인트가 일반 제조업체의 엔드포인트임을 확인할 수 있었습니다.

솔루션

이 문제의 핵심은 엔드포인트에 의한 예기치 않은 동작이었습니다. 엔드포인트에서 트래픽을 다시 네트워크에 반영할 가능성은 전혀 없습니다.

이 사례에서 가장 중요한 결과는 엔드포인트의 동향이었습니다. 대규모 네트워크에서 무작위로 발생하는 문제를 해결하기 어렵습니다. 따라서 팀은 검토할 사용자 포트의 하위 집합을 보유하게 되었습니다.

또한 관련 보안 기능(예: dot1x with MAB fallback)이 서비스 영향에서 역할을 했습니다. 이러한 기능이 반영된 트래픽에 응답하지 않았다면 서비스 영향은 그리 크지 않았을 것입니다.

패킷 캡처 툴을 활용하여 트래픽이 엔드포인트에 제대로 반영되었음을 확인했습니다. Catalyst 스위치에서 사용 가능한 내장형 EPC(Packet Capture) 툴을 사용하여 인바운드 패킷을 식별할 수 있습니다.

<#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
```

물리적 SPAN(스위치 포트 분석기)은 이 시나리오에서도 사용할 수 있는 신뢰할 수 있는 패킷 캡처 툴입니다.

```
<#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
```

팀은 의심스러운 엔드포인트가 연결된 포트에서 반영된 트래픽을 캡처할 수 있었습니다. 이 시나리오에서 엔드포인트는 게이트웨이 MAC 주소에서 소싱된 ARP 패킷을 스위치 포트에 다시 반영합니다. MAB 지원 스위치 포트는 게이트웨이 MAC 주소 인증을 시도합니다. 스위치 포트 보안 구현에서는 게이트웨이 MAC에서 데이터 VLAN에 권한을 부여할 수 있었습니다. MAC 주소는 보안 기능과 함께 학습되었으므로 사용자 포트에서 고정 MAC으로 "고정"됩니다. 또한 보안 구현으로 인해 인증된 MAC 주소의 MAC 주소 이동이 차단되었기 때문에 스위치에서 사용자 포트의 MAC을 잊어버릴 수 없었고 예상 인터페이스에서 MAC을 다시 학습할 수 없었습니다. 패킷 반영과 보안 구현이 겹쳐 전체 로컬 VLAN에 대해 트래픽이 영향을 받는 상황이 발생했습니다.

이벤트 순서:

1. MAC은 예상 인터페이스에서 학습됩니다. 네트워크의 정상 상태입니다.

2. 엔드포인트는 게이트웨이에서 시작된 트래픽을 스위치에 연결된 포트에 다시 반영합니다.

3. 엔드포인트 스위치 포트 보안 구현으로 인해 반영된 MAC에서 인증 세션이 트리거됩니다. MAC은 STATIC 엔트리로 프로그래밍됩니다.

4. MAC가 예상 스위치 포트에서 노후화되면 보안 구현으로 인해 업링크에서 MAC를 다시 학습할 수 없습니다.

5. 복구하려면 포트를 닫거나 닫지 않아야 합니다.

이러한 상황을 궁극적으로 해결하는 방법은 엔드포인트 동작을 해결하는 것이었습니다. 이 시나리오에서 동작은 엔드포인트 벤더에 이미 알려져 있으며 펌웨어 업데이트로 수정되었습니다. Catalyst 스위치 하드웨어, 소프트웨어 및 구성은 모두 예상대로 작동했습니다.

이 시나리오의 핵심 교훈은 MAC 학습의 개념입니다. Catalyst 스위치는 수신된 프레임의 소스 MAC 주소를 기반으로 인그레스(ingress)에서 MAC 주소를 학습합니다. MAC 주소가 예기치 않은 인터페이스에서 학습된 경우, 스위치 포트가 소스 MAC 필드의 해당 MAC 주소를 사용하여 인그레스(ingress)에서 프레임을 수신했다고 결론을 내리는 것이 안전합니다.

매우 제한적인 상황에서는 물리적 인터페이스와 스위치의 포워딩 ASIC 간에 또는 기타 내부 오동작을 통해 패킷이 반영될 수 있습니다. 이 경우 문제를 설명하는 기존 버그가 발견되지 않으면 TAC에 문의하여 격리를 지원하십시오.

관련 정보

- 패킷 캡처 구성 - Catalyst 9300
- SPAN 및 RSPAN 구성 - Catalyst 9300
- Catalyst 9000 Series 스위치의 Mac Address Table Manager 문제 해결
- IEEE 802.1x 포트 기반 인증 구성 - Catalyst 9300
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.