# Catalyst 6500/6000 스위치 ARP 또는 CAM 테이블 문제 해결

## 목차



## 소개

이 문서에서는 Catalyst 6500/6000 스위치의 ARP(Address Resolution Protocol) 또는 CAM(Content Addressable Memory) 테이블 관련 문제를 해결하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

# 배경 정보

Catalyst 스위치는 레이어 2 스위칭 또는 MLS(Multilayer Switching)에 맞게 조정된 여러 유형의 테이블을 유지 관리하며 프레임 또는 패킷 내의 많은 필드를 병렬로 비교할 수 있도록 매우 빠른 메모리에 보관됩니다.

- **ARP** - 레이어 2 브로드캐스트 도메인 내에서 IP 통신을 제공하기 위해 IP 주소를 MAC 주소에 매핑합니다.예를 들어, 호스트 B는 호스트 A에 정보를 보내려고 하지만 ARP 캐시에 호스트 A의 MAC 주소가 없습니다.호스트 B는 호스트 A의 IP 주소와 연결된 MAC 주소를 얻기 위해 브로드캐스트 도메인 내의 모든 호스트에 대한 브로드캐스트 메시지를 생성합니다.브로드캐스트 도메인 내의 모든 호스트는 ARP 요청을 수신하며, 호스트 A만 MAC 주소로 응답합니다.
- **CAM**—모든 Catalyst 스위치 모델은 레이어 2 스위칭을 위해 CAM 테이블을 사용합니다.프레임이 스위치 포트에 도착하면 소스 MAC 주소를 학습하고 CAM 테이블에 기록됩니다.도착 포트 및 VLAN은 타임스탬프와 함께 테이블에 기록됩니다.한 스위치 포트에서 학습한 MAC 주소가 다른 포트로 이동한 경우 가장 최근의 도착 포트에 대해 MAC 주소와 타임스탬프가 기록됩니다.그런 다음 이전 항목이 삭제됩니다.올바른 도착 포트에 대해 테이블에 MAC 주소가 이미 있는 경우 해당 타임스탬프만 업데이트됩니다.
- **TCAM(Ternary Content Addressable Memory)**—멀티레이어 스위치에서 ACL(Access Control List)이 제공하는 모든 프로세스는 매칭, 필터링, 특정 트래픽 제어 등 기존 라우팅에서 하드웨어에서 구현됩니다.TCAM을 사용하면 단일 테이블 조회에서 전체 액세스 목록에 대해 패킷을 평가할 수 있습니다.대부분의 스위치에는 여러 개의 TCAM이 있으므로 인바운드 및 아웃바운드 보안, QoS ACL을 동시에 또는 레이어 2 또는 레이어 3 포워딩 결정과 완전히 병렬로 평가할 수 있습니다.

# ARP 또는 CAM 관련 문제 해결

## 분산형 스위칭으로 동적 MAC 주소 손실

분산 스위칭에서는 각 DFC(Distributed Feature Card)가 각 CAM 테이블을 유지 관리하는 역할을 합니다.즉, 각 DFC는 MAC 주소를 학습하고 에이징합니다. 이는 CAM 에이징 및 해당 항목과 일치하는 트래픽에 따라 달라집니다.분산형 스위칭에서는 수퍼바이저 엔진이 특정 MAC 주소에 대한 트래픽을 한동안 볼 수 없는 것이 정상이므로 항목이 만료될 수 있습니다.DFC(라인 모듈에 있음)와 PFC(Policy Feature Card)(수퍼바이저 모듈에 있음)와 같은 서로 다른 엔진 간에 CAM 테이블을 일관되게 유지하기 위해 현재 두 가지 메커니즘을 사용할 수 있습니다.

- 패브릭 플러드(FF)
- MAC 알림(MN)

MAC 주소 항목이 PFC에서 에이징되면 **show mac-address *<MAC_Address>* all** 명령은 이 MAC 주소를 포함하는 DFC 또는 PFC를 표시합니다.

DFC 또는 PFC의 항목 밖으로 에이징을 방지하려면 해당 MAC 주소에 대한 트래픽이 없더라도 MAC 주소 동기화를 활성화합니다.동기화를 활성화하려면 다음 명령을 실행합니다.

```
!--- This is a global configuration command and is used to enable the synchronization. Cat6K-
IOS(config)#mac-address-table synchronize
```

```
!--- This is a privileged EXEC command and is used to clear dynamic MAC addresses. Cat6K-
IOS#clear mac-address-table dynamic
```

mac-**address-table synchronize** 명령은 Cisco IOS® Software Releases 12.2(18)SXE4 이상에서 사용할 수 있습니다.활성화한 후에도 PFC 또는 DFC에 없는 항목을 계속 볼 수 있습니다.그러나 이 모듈은 EOBC(Ethernet Out of Band Channel)를 사용하는 다른 사용자로부터 학습할 수 있는 방법을 제공합니다.

**주의: mac-address-table synchronize** 명령은 라우티드 MAC 엔티티를 삭제합니다.이를 방지하려면 **mac-address-table aging-time** ***0 routed*****-mac 전역 컨피그레이션** 명령을 사용하여 라우티드 MAC 비우기를 비활성화합니다.

## CEF가 정기적으로 패킷을 삭제

Cisco CEF(Express Forwarding)는 다른 스위칭 기술, 특히 동적 트래픽 패턴이 있는 네트워크에 비해 뛰어난 성능을 제공하는 레이어 3 IP 스위칭 기술입니다.CEF는 FIB(Forwarding Information Base) 및 인접성 테이블이라는 데이터 구조를 유지 관리합니다.FIB 테이블은 라우팅 테이블의 정보를 미러링하며 전달 결정을 내리는 데 사용됩니다.인접성 테이블에는 next hop 디바이스에 대한 사전 계산된 링크 레이어 헤더가 포함됩니다.다음 hop 인터페이스에 따라 FIB 테이블의 항목은 인접성 테이블의 엔트리에 매핑됩니다.인접성 테이블이 필수 정보로 채워지지 않으면 디바이스는 CEF 스위치 패킷을 수행할 수 없습니다.

CEF가 정상적인 작업 기간별로 간격을 두고 정기적으로 패킷을 삭제하는 경우 인접성 테이블이 주기적으로 지워지기 때문일 수 있습니다.이는 ARP 항목의 에이징 때문입니다.패킷은 인접성 테이블이 필수 next hop 정보로 다시 채워지는 기간 동안 CEF가 전환되지 않습니다.ARP 항목은 기본적으로 4시간마다 새로 고쳐지는 반면, 매우 작은 ARP 시간 초과 값을 구성하면 CEF 작업이 중단됩니다.

ARP 캐시에 항목이 남아 있는 시간을 변경하려면 인터페이스 컨피그레이션 모드에서 arp timeout 명령을 실행합니다.

이 취약성에 대한 자세한 내용은 Cisco 버그 ID CSCeb53542(등록된 고객만 해당)를 참조하십시오.CEF 인접성에 대한 자세한 내용은 CEF를 사용한 불완전한 인접성 문제 해결을 참조하십시오.

## CAM 테이블에서 All-Zero MAC 주소 전환 필터

소스 MAC 주소가 00-00-00-00-00-00인 스위치 필터 프레임은 CAM 테이블에서 유효하지 않은 소스 MAC입니다.이 경우 syslog 오류 출력의 예는 다음과 같습니다.

```
%SYS-4-P2_WARN: 1/Filtering MAC address 00-00-00-00-00-00 on port 2/48 from host table
```

이러한 메시지는 정보 제공용이므로 소스 MAC 주소가 00-00-00-00-00-00인 프레임이 발견되고 스위치가 CAM 테이블에 이 메시지를 추가하지 않음을 알려줍니다.그러나 스위치는 영(0) MAC 주소가 아닌 모든 MAC 주소에서 제공된 트래픽을 전달합니다.

해결 방법은 영(all-zero) 소스 MAC 주소로 프레임을 생성하는 엔드 스테이션을 식별하는 것입니다.일반적으로 다음 디바이스 중 하나가 이러한 프레임을 전송합니다.

- 트래픽 생성기(예: Spient SmartBits)

- IBM WebSphere 서버 로드 밸런싱 등 특정 유형의 서버
- all-zeros 브로드캐스트를 전송하는 디바이스와 같이 잘못 구성된 라우터 또는 엔드 스테이션
- 결함이 있는 NIC

## 5분마다 네트워크의 유니캐스트 플러딩

LAN 스위치는 레이어 2 및 CAM 테이블과 같은 포워딩 테이블을 사용하여 프레임의 VLAN 번호 및 대상 MAC 주소를 기반으로 특정 포트로 트래픽을 전송합니다.수신 VLAN에 있는 프레임의 대상 MAC 주소에 해당하는 항목이 없으면 (유니캐스트) 프레임이 해당 VLAN 내의 모든 포워딩 포트로 전송됩니다.이것은 홍수를 유발한다.패킷의 대상 MAC 주소가 스위치의 레이어 2 포워딩 테이블에 없는 것이 플러딩의 원인입니다.이 경우 패킷은 수신된 포트를 제외하고 VLAN의 모든 포워딩 포트에서 플러딩됩니다.

기본 ARP 테이블 에이징 시간은 4시간이고 CAM은 항목을 5분 동안만 보관합니다.대상 MAC 주소가 CAM 테이블에서 에이징될 때 스위치는 각 VLAN 내의 모든 포워딩 포트로 프레임을 전송합니다.유니캐스트 플러딩을 방지하려면 ARP 시간 초과보다 크거나 같은 CAM 에이징 타이머가 필요합니다.해결 방법으로, ARP 에이징 시간을 매칭하기 위해 문제가 있는 VLAN의 CAM 에이징 타이머를 늘리려면 다음 명령 중 하나를 실행할 수 있습니다.

- CatOS의 경우 set cam agingtime 명령을 실행합니다.
- Cisco IOS 소프트웨어의 경우 mac-address-table aging-time 명령을 실행합니다.

**참고:** HSRP(Hot Standby Router Protocol)를 실행하는 Catalyst 환경에서는 CAM 및 ARP 타이머가 동기화되도록 하는 것이 좋습니다.

스위치드 네트워크에서 유니캐스트 패킷 플러딩의 가능한 원인과 영향에 대한 자세한 내용은 스위치드 캠퍼스 네트워크의 유니캐스트 플러딩을 참조하십시오.

## 하이브리드 CatOS의 ARP 문제

하이브리드 모드에서 수퍼바이저 엔진은 CatOS를 실행하고 MSFC(Multilayer Switch Feature Card)는 Cisco IOS를 실행합니다.CatOS는 레이어 2에서 작동하며 VLAN, MAC 주소 및 포트 번호 정보를 저장할 CAM 주소 테이블을 구성합니다.MSFC의 Cisco IOS는 레이어 3에서 작동하며 IP 주소를 MAC 주소 확인에 보관할 ARP 테이블을 구성합니다.프린터 또는 서버와 같은 디바이스의 IP 주소를 변경할 경우 해당 새 IP 주소를 ping하지 못할 수 있습니다.그러나 동일한 VLAN에서 새 IP 주소를 ping할 수 있습니다.이는 MSFC의 ARP 문제일 수 있습니다.

이 해결 방법을 사용하면 문제를 격리하고 해결할 수 있습니다.

1. MSFC에서 ARP 테이블을 지웁니다.
   ```
   MSFC2#clear arp int vlan 40
   ```

2. ARP 시간 초과 값을 확인합니다.기본값은 4시간입니다.VLAN의 ARP 시간 제한이 높으면 시간 초과 값을 기본값 또는 최적 값으로 다시 설정할 수 있습니다.
   ```
   MSFC2#show int vlan 40
   Vlan40 is up, line protocol is up
     Hardware is Cat6k RP Virtual Ethernet, address is 00d0.0050.33fc (bia 00d0.005
   0.33fc)
     Internet address is 40.40.40.3/24
     MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
        reliability 255/255, txload 1/255, rxload 1/255
     Encapsulation ARPA, loopback not set
     Keepalive not supported
     ARP type: ARPA, ARP Timeout 04:00:00
   ```

```
  Last input 00:00:00, output 00:01:44, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

MSFC2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
MSFC2(config)#int vlan 40
MSFC2(config-if)#arp timeout ?
  <0-2147483>  Seconds

MSFC2(config-if)#arp timeout 240
```

3. MSFC를 다시 로드합니다.

```
MSFC2#write memory
Building configuration...
[OK]
MSFC2#reload
Proceed with reload? [confirm]
Supervisor> (enable)
```

## CAM 테이블 조회 중 EARL-2-EARL4LOOKUPRAMROR 오류

이 문제가 있는 경우 syslog 오류 출력의 예입니다.

```
%EARL-2-EARL4LOOKUPRAMERROR:Address eac6, data 0-0-8000-0, count 8
```

이는 CAM 테이블 조회를 수행할 때 나타납니다.이는 메모리에 액세스할 때 패리티 오류로 인해 발생합니다.이 오류는 일반적으로 show cam 명령을 실행하여 CAM 테이블에 액세스할 때 발생합니다.경우에 따라 스위치가 **show cam** 명령을 실행하면 재설정됩니다.

```
%EARL-2-EARLLOOKUPRAMERROR: Address [hex], data [hex]-[hex]-[hex]-[hex], count [dec]
```

이 오류 메시지는 조회 RAM 패리티 오류가 감지되었음을 나타냅니다.주소 [hex] 필드는 오류가 탐지된 전달 테이블의 주소입니다.data [hex]-[hex]-[hex]-[hex]-[hex] 필드는 패리티 오류를 생성한 RAM 데이터의 word0, word1, word2 및 word3입니다.count [dec] 필드는 패리티 오류의 총 수입니다.

이 메시지는 심각한 상황이 아니며, 격리된 항목만 있는 경우 중단 상황이 발생하지 않을 수 있습니다.이 메시지가 계속 표시되면 스위치가 CAM 테이블에 새 항목을 추가할 때 잘못된 DRAM 섹터에 쓰려고 함을 나타냅니다.그런 다음 DRAM 또는 수퍼바이저 자체를 교체해야 합니다.

## 수퍼바이저 전환 후 고정 CAM 항목이 손실됨

활성 수퍼바이저 엔진에 구성된 고정 CAM 항목은 빠른 전환 후 손실됩니다.이 문제를 해결하려면 빠른 전환 후 CAM 항목을 재구성해야 합니다.

이 취약성에 대한 자세한 내용은 Cisco 버그 ID CSCed87627(등록된 고객만) 및 CSCee27955(등록된 고객만 해당)를 참조하십시오.

## %ACL-5-TCAMFULL:acl 엔진 TCAM 테이블이 가득 찼습니다.

TCAM이 꽉 차서 새 ACL 또는 ACE(Access Control Entry)를 존재하는 ACL에 추가하려고 하면 커밋 또는 맵 프로세스가 실패합니다.이전 컨피그레이션은 그대로 적용됩니다.RACL(Router Access Control Lists)의 경우 ACL은 MSFC(Multilayer Switch Feature Card)의 소프트웨어에서 해당 성능

페널티를 적용합니다.

하이브리드 소프트웨어를 실행하는 스위치에서 TCAM의 패턴 또는 마스크 용량을 초과하는 VACL(Virtual Local Area Network Access Control List) 또는 QoS ACL ACE를 구성하는 경우 다음과 유사한 syslog 메시지가 콘솔에 출력됩니다.

```
%ACL-5-TCAMFULL: acl engine TCAM table is full
```

Supervisor IOS 시스템 또는 하이브리드 시스템의 MSFC에서 TCAM의 용량을 초과하는 RACL ACE를 구성하는 경우 다음과 유사한 syslog 메시지가 콘솔에 출력됩니다.

```
%FM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

Supervisor IOS 시스템 또는 하이브리드 시스템의 MSFC에서 **show fm summary** 명령을 실행하여 하드웨어(ACTIVE)에서 ACL을 적용하고 소프트웨어(INACTIVE)에서 ACL을 적용하는 인터페이스를 확인합니다.

이 문제를 해결하려면 스위치 컨피그레이션에서 사용하지 않는 ACL 또는 QoS를 제거합니다.자세한 내용은 Catalyst 6500 Series 스위치의 ACL 이해를 참조하십시오.

## Ping 문제는 MSFC가 Catalyst 6500 Series 스위치의 ARP 요청에 응답하지 않을 때 발생합니다.

VLAN 인터페이스를 ping할 때 해당 VLAN의 소스 IP가 있는 ARP 요청이 기본 라우터(MSFC)로 전송되지만 라우터는 ARP 요청에 응답하지 않으며 디버그 ARP는 다음 오류 메시지를 표시합니다.

```
IP ARP req filtered src [ip-address] [mac-address] dst [ip-address]
[mac-address] wrong cable, interface-id
```

각 ARP 데이터그램에 대해 대상 IP 주소가 로컬 호스트 주소와 일치하지 않으면 ARP 회신이 삭제됩니다.소스 IP 주소가 동일한 서브넷에 없는 경우 ARP 요청이 삭제됩니다.동일한 케이블에 둘 이상의 서브넷이 공존할 수 있는 드문 경우를 지원하려면 컨피그레이션 매개변수로 이 테스트를 재정의하는 것이 좋습니다.

ARP 응답은 라우팅 알고리즘에 의해 결정된 대로 로컬 호스트에서 대상 프로토콜 IP 주소에 연결할 수 있고 다음 홉이 동일한 인터페이스를 통해 연결되지 않은 경우에만 생성됩니다.로컬 호스트가 게이트웨이로 작동하는 경우 동일한 서브넷에 없는 대상에 대해 ARP 응답이 발생할 수 있습니다.이는 ARP 요청을 삭제하는 것이 정당하다는 것을 보여줍니다.

ARP 요청의 소스 IP 주소가 ARP의 대상 IP 주소와 다른 서브넷에 있기 때문에 Catalyst 6500이 모든 ARP 요청에 응답하지 않도록 함으로써 이 문제를 해결할 수 있습니다.따라서 MSFC/라우터는 ARP가 동일한 레이어 2 도메인에 유지되지 않고 잘못된 케이블 유형을 표시한다고 결론을 내립니다.즉, ARP 소스와 대상이 동일한 레이어 2 도메인에 속하지 않을 때 잘못된 케이블 디버그 메시지가 생성됩니다.이 시나리오에서 ARP가 작동하도록 하려면 고정 경로를 사용하여 대상 프로토콜 IP에 연결할 수 있어야 합니다.

## MAC 주소 테이블의 여러 항목

MAC 주소 테이블의 MAC 주소에 대해 두 개의 항목이 표시됩니다.

```
Cat6K#show mac-address-table int gi 6/11
```

```
Displaying entries from Line card 6:

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+---------------+--------+-----+----------+--------------------------
[FE 1]:
*  100  0011.857c.4d10   dynamic  Yes          0   Gi6/11
[FE 2]:
*  100  0011.857c.4d10   dynamic  Yes         95   Gi6/11


Cat6K#show module 6
Mod Ports Card Type                              Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  6   48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6748-GE-TX     SADxxxxxxxx

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ---------------------------------- ------ ------------ ------------ -------
  6  001d.45fd.xx4a to 001d.45fd.xx79   2.6   12.2(14r)S5  12.2(18)SXF8 Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  6  Distributed Forwarding Card WS-F6700-DFC3B     SALxxxxxxxx  4.6    Ok

Mod  Online Diag Status
---- -------------------
  6  Pass
```

2개의 레이어 2 포워딩 조회 엔진이 DFC 환경에 존재합니다.dCEF 환경에서는 FE1 및 FE2가 CEF720/dCEF720 아키텍처 라인 카드의 동일한 포트에서 동일한 MAC 주소를 학습하는 것이 일반적입니다.

## Microsoft 로드 밸런싱에서 사용하는 가상 IP 주소에 연결할 수 없습니다.

Cisco 라우터에는 모든 가상 IP 주소에 대해 ARP(Address Resolution Protocol) 항목이 필요합니다.네트워크 로드 밸런싱은 패킷 전달에 레벨 2 멀티캐스트를 사용합니다.Cisco의 RFC 구현에서 멀티캐스트는 IP 멀티캐스트에만 사용됩니다.따라서 라우터에 멀티캐스트 IP 주소가 표시되지 않으면 ARP 항목이 자동으로 생성되지 않으며 라우터에 수동으로 추가해야 합니다.

일반적으로 Cisco 디바이스는 유니캐스트 IP 주소(클러스터의 가상 주소)를 통해 해결된 경우 멀티캐스트 MAC 주소(클러스터 가상 MAC 주소)를 ARP 테이블에 두지 않습니다. 이 문제를 해결하려면 유니캐스트 가상 IP 주소를 멀티캐스트 MAC 주소에 정적 매핑해야 합니다.

자세한 내용은 *Catalyst* Switches for Microsoft Network Load Balancing Configuration Example(*Microsoft 네트워크 로드 밸런싱 컨피그레이션*의 *Multicast Mode) 섹션을* 참조하십시오.

# 관련 정보

- CEF를 사용한 불완전한 인접성 트러블슈팅
- 스위치드 캠퍼스 네트워크의 유니캐스트 플러딩
- LAN 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems