

Supervisor Engine 2 및 Running CatOS System Software를 사용하여 Catalyst 6500/6000 Series 스위치에서 CEF를 포함하는 유니캐스트 IP 라우팅 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[CEF 개요](#)

[포워딩 정보 베이스\(FIB\)](#)

[인접성 테이블](#)

[PFC2에서 FIB 및 인접성 테이블을 읽는 방법](#)

[문제 해결 방법](#)

[사례 연구 1: 직접 연결된 네트워크의 호스트에 연결](#)

[문제 해결 단계](#)

[발언 및 결론](#)

[사례 연구 2: 원격 네트워크에 연결](#)

[문제 해결 단계](#)

[발언 및 결론](#)

[사례 연구 3: 여러 개의 다음 홉으로 로드 밸런싱](#)

[사례 연구 4: 기본 라우팅](#)

[MSFC2 라우팅 테이블에 기본 경로가 있음](#)

[라우팅 테이블에 기본 경로 없음](#)

[기타 문제 해결 팁 및 알려진 문제](#)

[show mls cef mac 명령 실행](#)

[새도우 TCAM](#)

[기본 라우팅 끝값](#)

[관련 정보](#)

소개

이 문서는 Supervisor Engine 2, PFC2(Policy Feature Card 2), MSFC2(Multilayer Switch Feature Card 2)를 사용하는 Catalyst 6500/6000 스위치에서 유니캐스트 IP 라우팅 문제를 해결하는 가이드로 사용해야 합니다. Supervisor Engine 2의 유니캐스트 라우팅은 Cisco CEF(Express Forwarding)를 사용하여 수행됩니다. 이 문서는 Supervisor Engine 2, PFC2, MSFC2가 장착된 Catalyst 6500/6000 시리즈의 IP 라우팅에 대해서만 다룹니다. 이 문서는 Supervisor Engine 1(또는

1A)이 있는 Catalyst 6500/600 또는 MSM(Multilayer Switch Module)에 대해 유효하지 않습니다. 이 문서는 Supervisor Engine에서 Catalyst OS(CatOS) 시스템 소프트웨어를 실행하는 스위치에만 유효하며 Cisco IOS® 시스템 소프트웨어에는 적용되지 않습니다.

[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 규칙](#)을 참조하십시오.

[CEF 개요](#)

CEF는 원래 패킷을 더 빨리 라우팅하도록 설계된 Cisco IOS Software 스위칭 기술입니다. CEF는 고속 스위칭보다 훨씬 확장성이 뛰어납니다. (첫 번째 패킷을 전송하여 스위칭을 처리할 필요가 없습니다.) Supervisor Engine 2가 포함된 Catalyst 6500은 PFC2에 구현된 하드웨어 기반 CEF 포워딩 메커니즘을 사용합니다. CEF는 주로 두 개의 테이블을 사용하여 라우팅에 필요한 정보를 저장합니다. FIB(Forwarding Information Base) 및 인접성 테이블

[포워딩 정보 베이스\(FIB\)](#)

CEF는 FIB를 사용하여 IP 대상 접두사 기반 스위칭 결정을 합니다(가장 긴 일치 우선). FIB는 라우팅 테이블 또는 정보 베이스와 개념적으로 비슷합니다. IP 라우팅 테이블에 포함된 전달 정보의 미러 이미지를 유지 관리합니다. 네트워크에서 라우팅 또는 토폴로지 변경이 발생하면 IP 라우팅 테이블이 업데이트되고 이러한 변경 사항이 FIB에 반영됩니다. FIB는 IP 라우팅 테이블의 정보를 기반으로 다음 hop 주소 정보를 유지 관리합니다. FIB 항목과 라우팅 테이블 항목 간의 일대일 상관관계 때문에 FIB는 모든 알려진 경로를 포함하며 빠른 스위칭 및 최적 스위칭 같은 스위칭 경로와 연결된 경로 캐시 유지 관리가 필요하지 않습니다. FIB에는 항상 기본 또는 와일드카드 중 하나가 일치합니다.

[인접성 테이블](#)

연결 레이어를 통해 단일 홉으로 서로 연결할 수 있는 경우 네트워크의 노드는 인접해 있다고 합니다. CEF는 FIB 외에도 인접성 테이블을 사용하여 L2(Layer 2) 주소 지정 정보를 추가합니다. 인접성 테이블에는 모든 FIB 항목에 대한 L2 next hop 주소가 유지됩니다. 즉, 전체 FIB 항목에는 최종 IP 대상에 도달하기 위해 다음 홉에 대한 L2 재작성 정보가 들어 있는 인접성 테이블의 위치에 대한 포인터가 포함됩니다. 하드웨어 CEF가 Catalyst 6500/Supervisor Engine 2 시스템에서 작동하려면 MSFC2에서 IP CEF를 실행해야 합니다.

[PFC2에서 FIB 및 인접성 테이블을 읽는 방법](#)

PFC2의 FIB 테이블은 MSFC2의 FIB 테이블과 정확히 같아야 합니다. PFC2에서 FIB의 모든 IP 접두사는 TCAM(ternary content addressable memory)에 저장되고 가장 긴 마스크부터 마스크 길이가 정렬됩니다. 즉, 먼저 마스크가 32(호스트 항목)인 모든 항목을 찾습니다. 그런 다음 마스크 길이가 31인 모든 항목을 찾습니다. 이렇게 하면 마스크 길이가 0인 항목이 됩니다. 이것이 기본 항목입니다. FIB는 순차적으로 읽히고 첫 번째 적중은 일치로 사용됩니다. PFC2의 다음 샘플 FIB 테이블을 고려하십시오.

```
Cat6k> (enable) show mls entry cef
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 receive 0.0.0.0 255.255.255.255
!--- This is the first entry with mask length 32. 15 receive 255.255.255.255 255.255.255.255
15 receive 192.168.254.254 255.255.255.255 15 receive 10.48.72.237 255.255.255.255 15
receive 10.48.72.0 255.255.255.255 15 receive 10.48.72.255 255.255.255.255 15
receive 192.168.222.7 255.255.255.255 15 receive 192.168.100.254 255.255.255.255 15
receive 192.168.10.254 255.255.255.255 15 resolved 192.168.199.3 255.255.255.255
192.168.199.3 1 15 resolved 192.168.222.2 255.255.255.255 192.168.222.2 1 15
resolved 192.168.199.2 255.255.255.255 192.168.199.2 1 15 resolved 192.168.254.252
255.255.255.255 192.168.199.3 1 !--- This is the last entry with mask length 32. 15
connected 192.168.222.0 255.255.255.252 !--- This is the only entry with mask length 30. 15
receive 224.0.0.0 255.255.255.0 !--- This is the first entry with mask length 24. 15
connected 10.48.72.0 255.255.255.0 15 connected 192.168.10.0 255.255.255.0 15 connected
192.168.11.0 255.255.255.0 15 connected 192.168.100.0 255.255.255.0 15 connected
192.168.101.0 255.255.255.0 15 connected 192.168.199.0 255.255.255.0 !--- This is the last
entry with mask length 24. 15 connected 127.0.0.0 255.0.0.0 0 !--- This is the entry with
mask length 8. 15 wildcard 0.0.0.0 0.0.0.0 0 !--- This is the entry with mask length 0.
```

각 항목은 다음 필드로 구성됩니다.

- Mod(수정) - 항목을 설치하는 MSFC2는 지정된 MSFC2에 따라 15 또는 16입니다.
- FIB-Type - 이 특정 항목과 연결된 유형입니다. 가능한 FIB 은 다음과 같습니다.receive - MSFC 인터페이스와 연결된 접두사입니다. 여기에는 MSFC 인터페이스의 IP 주소와 브로드캐스트 서브넷의 IP 주소에 해당하는 32의 마스크가 포함된 접두사가 포함됩니다.resolved—유효한 next hop 주소와 연결된 접두사입니다. 여기에는 다음 홉에 대해 해결된 인접성이 있는 접두사가 모두 포함됩니다.connected—연결된 네트워크와 연결된 접두사입니다. - 모든 항목(drop 또는 MSFC 리디렉션)과 일치합니다. 이 항목은 기본 항목이 없고 마스크 길이가 0인 경우에만 표시 됩니다.default - 기본 경로입니다. 와일드카드 항목은 모든 서브넷과 일치하며 마스크 길이가 0인 상태로 표시됩니다. 다음 홉을 가리킵니다. 이 기본 CEF 항목은 라우팅 테이블에 기본 경로가 있는 경우에만 존재합니다.drop - 드롭이 있는 항목과 일치하는 모든 패킷이 삭제됩니다.
- Destination-IP - 대상 IP 주소 또는 관련 IP 서브넷입니다.
- Destination-Mask - 항목과 연결된 마스크입니다. 위의 예에서 볼 수 있듯이 FIB는 가장 긴 마스크(255.255.255.255)로 시작하고 가능한 가장 짧은 마스크(0.0.0.0)로 끝납니다.
- Next-Hop IP - 다음 hop IP(있는 경우)를 표시합니다.

다음 명령을 입력하여 전체 인접성 테이블을 볼 수 있습니다.

```
Cat6k> (enable) show mls entry cef adjacency
Mod:15
Destination-IP : 192.168.98.2 Destination-Mask : 255.255.255.255
FIB-Type :resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp Tx-Packets Tx-Octets
-----
connect 192.168.98.2 00-90-21-41-c5-57 98 ARPA 0 0
```

참고: 이 출력에는 FIB의 확인된(또는 기본) CEF 항목 각각에 대해 위의 샘플 FIB 테이블에 있는 항목과 유사한 항목이 포함됩니다.

문제 해결 방법

트러블슈팅에 대한 몇 가지 예와 세부 정보를 제공하기 전에 이 섹션에서는 특정 IP 주소에 대한 연결성 또는 연결성 문제를 해결하는 데 따르는 방법을 요약합니다. PFC2의 CEF 테이블은 MSFC2의 CEF 테이블을 미러링한다는 점에 유의하십시오. 따라서 MSFC2에서 알고 있는 정보가 올바르면 PFC2는 IP 주소에 도달하기 위한 올바른 정보만 보관합니다. 따라서 항상 아래 정보를 확인해야 합니다.

MSFC2에서

다음 단계를 완료하십시오.

1. **show ip route** 명령(또는 **show ip route x.x.x.x** 명령을 실행하여 전체 라우팅 테이블을 검색하지 않도록) MSFC2 테이블의 IP 라우팅에 있는 정보가 올바른지 확인한 다음 출력에 예상 다음 홉이 포함되어 있는지 확인합니다. 그렇지 않은 경우, 실행 중인 라우팅 프로토콜과 관련된 라우팅 프로토콜, 컨피그레이션, 라우팅 프로토콜 네이버 및 기타 트러블슈팅을 확인해야 합니다.
2. **show ip arp next_hop_ip_address** 명령을 실행한 다음 ARP가 확인되고 올바른 MAC 주소가 포함되어 있는지 확인하여 다음 홉이나 연결된 네트워크에 대한 최종 목적지가 MSFC2에 올바른 ARP(Address Resolution Protocol) 항목을 가지고 있는지 확인합니다. MAC 주소가 올바르지 않으면 다른 장치가 해당 IP 주소를 소유하고 있는지 확인해야 합니다. 결국 해당 MAC 주소를 소유하는 디바이스를 연결하는 포트에서 스위치 레벨을 추적해야 합니다. ARP 항목이 불완전하면 해당 호스트에서 어떤 회신도 수신하지 않았음을 의미합니다. 호스트가 실행 중인지 확인해야 합니다. 호스트에서 스니퍼를 사용하여 ARP 회신을 수신하는지, 올바르게 응답하는지 확인할 수 있습니다.
3. 다음 단계를 수행하여 MSFC2의 CEF 테이블에 올바른 정보가 포함되어 있고 인접성이 해결되었는지 확인합니다. **show ip cef destination_network** 명령을 실행하여 CEF 테이블의 다음 홉이 IP 라우팅 테이블의 다음 홉과 일치하는지 확인합니다(위의 1단계). **show adjacency detail**을 실행하여 인접성이 올바른지 확인합니다. | **next_hop_ip_address** 명령을 시작합니다. 위의 2단계에서 볼 수 있는 ARP의 동일한 MAC 주소를 포함해야 합니다.

위의 1단계와 2단계에서 올바른 결과를 제공하지만 3a 또는 3b단계가 실패하면 Catalyst 6500/6000과 관련이 없는 Cisco IOS Software CEF 문제가 발생합니다. ARP 테이블 및 IP 라우팅 테이블을 지워야 합니다.

PFC2에서

다음 단계를 완료하십시오.

1. PFC2에 저장된 FIB 정보가 올바르고 MSFC2의 CEF 테이블에 저장된 정보(위의 3단계에서 표시됨)와 일치하는지 확인한 다음 **show mls entry cef ip destination_ip_network/destination_subnet_mask** 명령을 실행한 다음 다음 다음 hop IP 주소가 예상하는 주소인지 확인합니다. 위의 3단계에서 얻은 결과와 일치하지 않는 정보는 MSFC2와 PFC2 간의 통신 문제(Catalyst 6500/6000 내부)를 가리킵니다. 실행 중인 MSFC2의 CatOS 또는 Cisco IOS 소프트웨어의 알려진 버그가 없는지 확인합니다. MSFC2에서 **clear ip route** 명령을 실행하여 올바른 항목을 복원할 수 있습니다.
2. **show mls entry cef ip next_hop_ip_address/32 adjacency** 명령을 실행하여 PFC2의 인접성 테이블을 확인한 다음 [위 MSFC2 섹션에서](#) 단계 2 및 3b에 표시된 것과 동일한 MAC 주소를 포함하는지 확인합니다. PFC2의 인접성이 3b단계에서 다음 홉의 인접성과 일치하지 않으면

MSFC2와 PFC2 간의 내부 통신 문제가 발생할 수 있습니다. 인접성을 지워 올바른 정보를 복원할 수 있습니다.

사례 연구 1: 직접 연결된 네트워크의 호스트에 연결

이 간단한 사례에서는 다음 사이의 연결에 대해 설명합니다.

- IP 주소가 192.168.10.10인 VLAN 10의 호스트 1
- IP 주소가 192.168.199.3인 VLAN 199의 호스트 2

다음은 MSFC2 구성 출력의 예입니다.

```
interface VLAN 10
description Server VLAN
ip address 192.168.10.1 255.255.255.0
no ip redirects
!
interface VLAN 199
ip address 192.168.199.1 255.255.255.0
```

참고: Catalyst 6500/6000(Supervisor Engine 2 및 MSFC2 포함)은 하드웨어에서 CEF를 사용하여 라우팅을 수행하고 있습니다. 구성할 항목이 없습니다. MSFC2에서는 CEF를 비활성화할 수 없습니다.

문제 해결 단계

IP 주소 192.168.199.3에 도달할 경로를 확인하려면 이 문서의 [Troubleshooting Method](#) 섹션에서 강조 표시된 절차를 수행합니다.

1. 다음 명령 중 하나를 실행하여 IP 라우팅 테이블을 확인합니다.

```
Cat6k-MSFC2# show ip route 192.168.199.3
Routing entry for 192.168.199.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via VLAN 199
Route metric is 0, traffic share count is 1
```

또는

```
Cat6k-MSFC2# show ip route | include 192.168.199.0
C 192.168.199.0/24 is directly connected, VLAN 199
```

이러한 명령 출력에서 대상이 직접 연결된 서브넷에 있음을 확인할 수 있습니다. 따라서 목적지에는 다음 hops가 없습니다.

2. MSFC2에서 ARP 항목을 확인합니다. 이 경우 다음 명령을 실행하여 대상 IP 주소에 대한 ARP 항목이 있는지 확인합니다.

```
Cat6k-MSFC2# show ip arp 192.168.199.3
Protocol Address      Age (min) Hardware      Addr Type Interface
Internet 192.168.199.3 176          0030.7150.6800 ARPA VLAN 199
```

3. MSFC2에서 CEF 및 인접성 테이블을 확인합니다. 다음 명령을 실행하여 CEF 테이블을 확인합니다.

```
Cat6k-MSFC2# show ip cef 192.168.199.3
192.168.199.3/32, version 281, connected, cached adjacency 192.168.199.3
0 packets, 0 bytes
via 192.168.199.3, VLAN 199, 0 dependencies
next-hop 192.168.199.3, VLAN 199
valid cached adjacency
```

마스크 길이가 32이고 유효한 캐시 인접성이 있는 유효한 CEF 항목이 있음을 확인할 수 있습니다.

니다. 다음 명령을 실행하여 인접성 테이블을 확인합니다.

```
Cat6k-MSFC2# show adjacency detail | begin 192.168.199.3
IP VLAN 199192.168.199.3(7)
0 packets, 0 bytes
003071506800
```

```
!--- This is the destination MAC address. 00D0003F8BFC0800 ARP00:58:35
```

위 출력에서 볼 수 있듯이 인접성이 있습니다. 인접성의 대상 MAC 주소는 위의 2단계 ARP 테이블에 있는 MAC 주소와 동일한 정보를 표시합니다. 패킷이 하드웨어에서 L3(Layer 3)로 전환되므로 3b단계의 카운터는 거의 항상 0입니다. 따라서 MSFC2에 도달하지 않으며 MSFC2 CEF 카운터에 포함되지 않습니다. 지정된 대상으로 전달된 패킷에 대한 통계를 볼 수 있는 유일한 방법은 5단계에서 PFC2에 있는 인접성의 통계를 확인하는 것입니다.

4. Supervisor Engine POV에서 올바른 CEF/FIB 항목이 있는지 확인합니다. FIB에는 다음과 같은 두 가지 흥미로운 항목이 있습니다. 다음과 같이 대상 IP 주소에 대한 항목입니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.199.3/32
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 resolved 192.168.199.3 255.255.255.255 192.168.199.3 1
```

이 항목은 이미 알려진 next hop(이 경우 대상 자체)이 있는 호스트 항목입니다. 다음과 같이 대상 네트워크에 해당하는 항목입니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.199.0/24
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 connected 192.168.199.0 255.255.255.0
```

이 항목은 연결된 FIB 항목입니다. 즉, 이 항목을 적중하는 모든 패킷이 추가 처리를 위해 MSFC2로 리디렉션됩니다(주로 ARP를 전송하고 ARP 확인을 기다리는 중). FIB는 가장 긴 마스크 길이로 시작하여 순차적으로 탐색됩니다. 따라서 위의 4단계에 나열된 항목이 모두 있는 경우 마스크 32(호스트 항목)가 있는 첫 번째 항목을 누르면 FIB 테이블이 더 아래로 내려가지 않습니다. /32 항목이 없는 경우 네트워크 항목인 두 번째 항목을 누릅니다. 연결된 항목이므로 추가 처리를 위해 패킷을 MSFC2로 리디렉션합니다. MSFC2에서 대상 마스크에 대한 ARP 요청을 보낼 수 있습니다. ARP 회신이 수신되면 MSFC2의 해당 호스트에 대해 ARP 테이블 및 인접성 테이블이 완료됩니다.

5. 마스크 길이가 32인 올바른 FIB 항목이 있으면 다음 명령을 실행하여 해당 호스트에 대해 인접성이 올바르게 입력되었는지 확인합니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.199.3/32 adjacency
Mod:15
Destination-IP : 192.168.199.3 Destination-Mask : 255.255.255.255
FIB-Type : resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect 192.168.199.3 00-30-71-50-68-00 199 ARPA 0 0
```

참고: 인접성이 채워지고 NextHop-Mac 필드에 호스트 2의 유효한 MAC 주소가 포함됩니다(단계 2 및 3b 참조). 이 시점에서는 이 인접성에 대해 전송된 패킷 수가 여전히 0이지만 모든 출력이 정확합니다. 다음 예에서는 호스트 1에서 호스트 2로 100바이트의 ping 10개를 전송하고 인접성을 다시 확인합니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.199.3/32 adjacency
Mod:15
Destination-IP : 192.168.199.3 Destination-Mask : 255.255.255.255
FIB-Type : resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect 192.168.199.3 00-30-71-50-68-00 199 ARPA 10 1000
```

이제 TX-Packets 수가 10이며, 전송된 트래픽과 일치합니다.

발언 및 결론

위의 문제 해결 [단계](#) 4단계에서 언급한 것처럼, 아래 설명과 같이 일치하는 FIB 항목이 두 개 있습니다.

- network entry(이 경우, 192.168.199.0/24) - 이 항목은 항상 표시되며 MSFC의 라우팅 및 CEF 테이블에서 직접 가져옵니다. 이 네트워크는 항상 라우팅 테이블에 직접 연결됩니다.
- destination host entry(이 경우 192.168.199.3/32) - 이 항목이 반드시 존재하지 않을 수도 있습니다. 그렇지 않으면 네트워크 항목을 클릭하면 다음 항목이 발생합니다.패킷이 MSFC2로 전달됩니다.그런 다음 마스크 길이가 32인 호스트 항목이 PFC의 FIB 테이블에 생성됩니다. 그러나 아직 완전한 인접성이 없으므로 형식이 frc drop인 인접성이 (즉, 강제 삭제).해당 대상에 대한 후속 패킷은 /32의 항목에 도달하고 패킷이 삭제됩니다.동시에 MSFC2로 전송된 원래 패킷은 MSFC2를 트리거하여 ARP 요청을 보냅니다.ARP가 확인되면 ARP 항목이 완료됩니다. MSFC2에서 인접성이 완료되고 인접성 업데이트가 Supervisor Engine에 전송되어 기존 FC를 완료합니다.Supervisor Engine은 재작성 MAC 주소를 반영하여 호스트 인접성을 변경하고 인접성 유형이 연결되도록 변경됩니다.ARP가 해결될 때까지 기다리는 동안 fec drop 을 설치하는 이 메커니즘을 ARP 스로틀이라고 합니다. ARP 스로틀은 모든 패킷이 MSFC2에 전달되고 여러 ARP 요청을 생성하지 않도록 하는 데 유용합니다. 처음 몇 개의 패킷만 MSFC2로 전송되고, 나머지는 인접성이 완료될 때까지 PFC2에서 삭제됩니다.또한 직접 연결된 네트워크의 존재하지 않거나 응답하지 않는 호스트로 향하는 트래픽을 삭제할 수 있습니다.

서로 다른 두 VLAN에 있는 두 사용자 간의 연결을 트러블슈팅할 때 다음 사항을 고려해야 한다는 점을 항상 염두에 두어야 합니다.

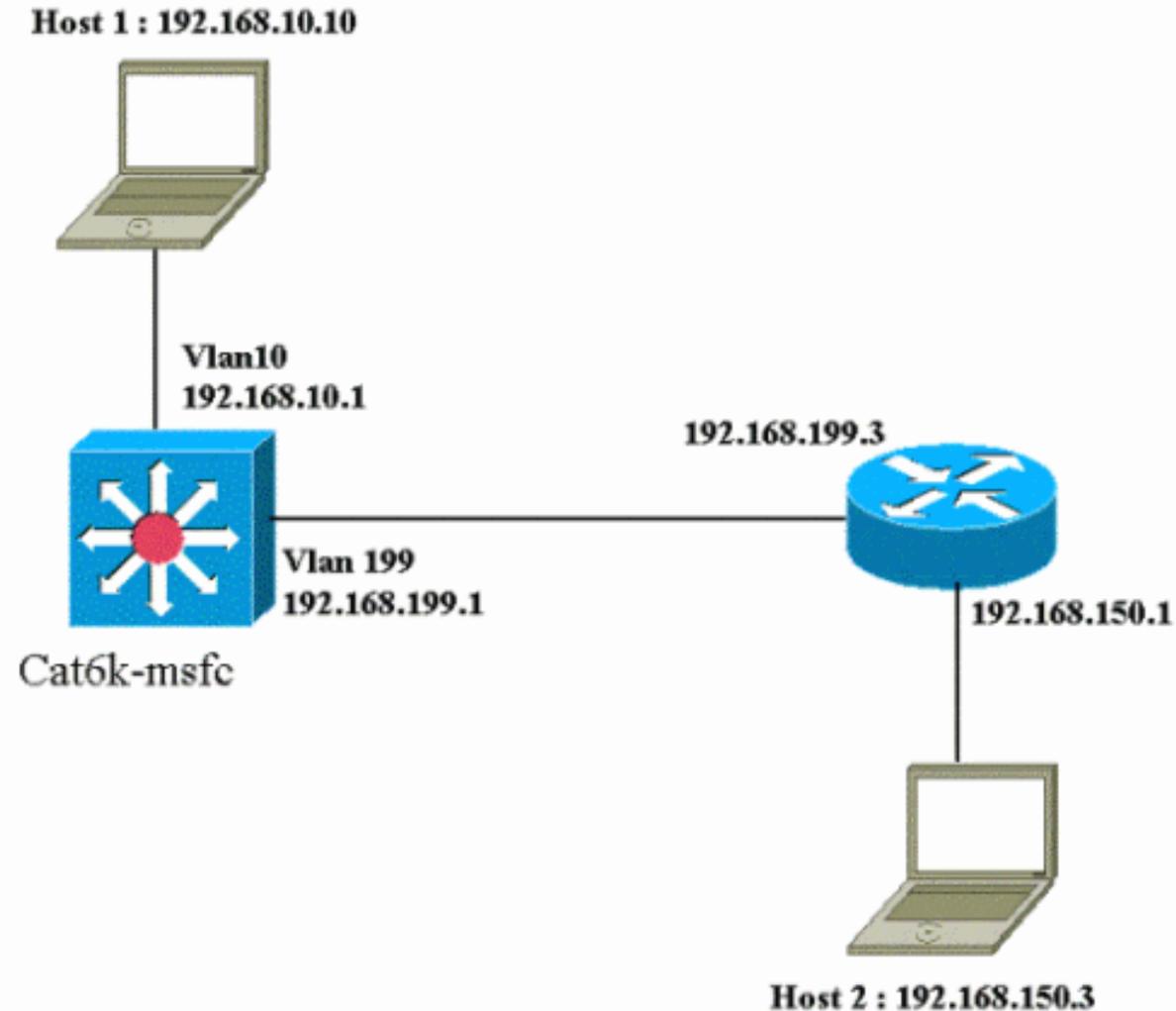
- 위의 Troubleshooting [Method](#)(문제 해결 방법)를 사용하여 호스트 1에서 호스트 2로 이동하는 트래픽(대상 IP 주소 호스트 2)
- 동일한 방법을 사용하여 호스트 2에서 호스트 1로 이동하는 트래픽이지만 이번에는 목적지가 호스트 1인 경우

또한 출력은 소스의 기본 게이트웨이에서 가져와야 합니다. 이 경우 호스트 1에서 호스트 2로 이동하는 트래픽과 호스트 2에서 호스트 1로 이동하는 트래픽이 반드시 동일하지는 않습니다.

참고: 하드웨어에서 L3로 패킷이 스위칭되므로 위 문제 해결 [단계](#)의 3b단계의 카운터가 거의 항상 0입니다. 따라서 MSFC2에 도달하지 않으며 MSFC2 CEF 카운터에 포함되지 않습니다. 지정된 대상으로 전달된 패킷에 대한 통계를 볼 수 있는 유일한 방법은 위의 Troubleshooting Steps(문제 해결 단계)의 5단계에서 PFC2에 있는 인접성 [의](#) 통계를 확인하는 것입니다.

[사례 연구 2: 원격 네트워크에 연결](#)

IP 주소가 192.168.150.3인 192.168.10.10 ping 호스트 2인 호스트 1을 사용하는 다음 다이어그램을 고려하십시오. 그러나 이번에는 호스트 2가 Catalyst 6500/6000-MSFC2에 직접 연결되는 대신 라우팅된 두 홉에 있습니다. 동일한 방법을 사용하여 Catalyst 6500/6000-MSFC2에서 CEF 라우팅 경로를 따릅니다.



문제 해결 단계

다음 단계를 완료하십시오.

1. 다음 명령을 실행하여 MSFC2의 라우팅 테이블을 확인합니다.

```
Cat6k-MSFC2# show ip route 192.168.150.3
Routing entry for 192.168.150.0/24
Known via "ospf 222", distance 110, metric 2, type intra area
Last update from 192.168.199.3 on VLAN 199, 00:12:43 ago
Routing Descriptor Blocks:
* 192.168.199.3, from 192.168.254.252, 00:12:43 ago, via VLAN 199
Route metric is 2, traffic share count is 1
```

```
Cat6k-MSFC2#sh ip route | include 192.168.150.0
O 192.168.150.0/24 [110/2] via 192.168.199.3, 00:13:00, VLAN 199
```

위 출력에서 IP 주소 192.168.150.3을 사용하여 호스트 2에 도달하기 위해 OSPF(Open Shortest Path First) 경로가 있음을 확인할 수 있습니다. VLAN 199의 IP 주소 192.168.199.3을 다음 홉으로 사용하여 연결해야 합니다.

2. 아래 명령을 실행하여 MSFC2의 ARP 테이블을 확인합니다.참고: 최종 대상이 아닌 다음 홉의 ARP 항목을 확인합니다.

```
Cat6k-MSFC2# show ip arp 192.168.199.3
Protocol Address      Age (min) Hardware      Addr Type  Interface
Internet 192.168.199.3    217          0030.7150.6800 ARPA     VLAN 199
```

3. 다음 명령을 실행하여 MSFC2의 CEF 테이블 및 인접성 테이블을 확인합니다.

```
Cat6k-MSFC2# show ip cef 192.168.150.0
192.168.150.0/24, version 298, cached adjacency 192.168.199.3
0 packets, 0 bytes
```

```
via 192.168.199.3, VLAN 199, 0 dependencies
next-hop 192.168.199.3, VLAN 199
valid cached adjacency
```

대상 네트워크에 대한 CEF 항목이 있으며, 다음 hop 결과는 라우팅 테이블의 1단계에서 얻은 것과 일치합니다.

4. 다음 명령을 실행하여 다음 홉의 인접성 테이블을 확인합니다.

```
Cat6k-MSFC2# show adjacency detail | begin 192.168.199.3
IP VLAN 199 192.168.199.3(9)
0 packets, 0 bytes
003071506800
00D0003F8BFC0800
ARP 00:17:48
```

다음 홉에 유효한 인접성이 있으며, 대상 MAC 주소는 위의 2단계에서 찾은 ARP 항목과 일치합니다.

5. 다음 명령을 실행하여 PFC2(Supervisor Engine)의 FIB 테이블을 확인합니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.150.0/24
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 resolved 192.168.150.0 255.255.255.0 192.168.199.3 1
```

FIB는 3단계에서 찾은 것과 동일한 정보를 반영하며, 다음 홉도 동일합니다.

6. 다음 명령을 실행하여 PFC2(Supervisor Engine)에서 인접성을 확인합니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.150.0/24 adjacency
Mod:15
Destination-IP : 192.168.150.0 Destination-Mask : 255.255.255.0
FIB-Type : resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect 192.168.199.3 00-30-71-50-68-00 199 ARPA 0 0
```

위의 2단계와 4단계에서 찾은 것과 동일한 MAC 주소를 반영하는 연결 인접성이 있는지 확인할 수도 있습니다.

참고: PFC2에서 인접성을 확인할 때 최종 대상의 인접성을 확인할 수 있습니다. MSFC2의 Cisco IOS Software에서는 인접성을 확인할 수 없으며, 다음 홉의 인접성을 확인해야 합니다. 최종 대상에 대한 PFC2의 인접성 테이블에는 다음 홉의 다음 홉과 인접성(해결된 경우)이 모두 하나의 명령 출력으로 표시됩니다. MSFC2에서 CEF 항목을 별도로 확인하여 다음 홉을 찾은 다음 다음 홉의 인접성 자체를 확인해야 합니다.

발언 및 결론

이 예에서는 원격 네트워크에 연결하기 위해 Catalyst 6500/6000-MSFC2에서 연결을 확인하는 데 사용되는 문제 해결 단계가 [사례 연구 1](#)의 이전 예와 비슷함을 확인할 수 있습니다. [직접 연결된 네트워크의 호스트에 대한 연결](#). 그러나 몇 가지 차이점이 있습니다.

- IP 라우팅 테이블, CEF 테이블 및 FIB에서 최종 대상을 확인합니다(단계 1, 3, 5).
- ARP 테이블 및 인접성 테이블에서 다음 hop 정보를 확인합니다(2단계 및 4단계).
- 6단계에서는 최종 대상에 대한 인접성을 직접 확인할 수 있습니다. 결과는 FIB의 다음 홉과 인접성 테이블의 인접성 재작성 정보를 모두 표시합니다.

이 경우 아래 그림과 같이 최종 대상에 대한 FIB에 항목이 없습니다. 마스크 길이가 24인 네트워크 항목만 있습니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.150.3/32 adjacency
Cat6k> (enable)
```

[사례 연구 3: 여러 개의 다음 홉으로 로드 밸런싱](#)

이 사례 연구에서는 동일한 목적지 네트워크에 연결하기 위해 몇 개의 다음 홉과 여러 경로를 사용할 수 있는 경우에 발생하는 상황을 설명합니다.

1. 아래 라우팅 테이블의 샘플 섹션에서는 동일한 목적지 IP 주소인 192.168.254.253에 도달할 수 있는 세 가지 경로와 세 가지 다른 다음 홉이 있음을 확인할 수 있습니다.
 O 192.168.254.253 [110/2] via 192.168.222.6, 00:42:45, POS8/2
 [110/2] via 192.168.222.2, 00:42:45, VLAN 222
 [110/2] via 192.168.199.2, 00:42:45, VLAN 199
2. 다음 3개의 다음 홉의 각 ARP 항목을 다음 단계에 따라 확인합니다. 대상에 대한 CEF 테이블을 확인합니다. 대상이 MSFC2의 CEF 테이블에 세 개의 서로 다른 항목을 표시한다는 점에 유의하십시오. Cisco IOS Software CEF는 서로 다른 경로 간에 로드 공유를 수행할 수 있습니다

```
cat6k-MSFC2# show ip cef 192.168.254.253
192.168.254.253/32, version 64, per-destination sharing
0 packets, 0 bytes
via 192.168.222.6, POS8/2, 0 dependencies
traffic share 1
next-hop 192.168.222.6, POS8/2
valid adjacency
via 192.168.222.2, VLAN 222, 0 dependencies
traffic share 1
next-hop 192.168.222.2, VLAN 222
valid adjacency
via 192.168.199.2, VLAN 199, 0 dependencies
traffic share 1
next-hop 192.168.199.2, VLAN 199
valid adjacency
0 packets, 0 bytes switched through the prefix
```

MSFC2 인접성 테이블에서 세 개의 인접성을 확인합니다. 위의 2단계에서 ARP 항목과 일치해야 합니다.

3. 동일한 대상에 대해 세 개의 서로 다른 FIB 항목이 설치되어 있습니다. PFC2의 하드웨어 CEF는 동일한 대상에 대해 최대 6개의 다른 경로를 공유할 수 있습니다. 가중치 필드에서 각 다음 홉에 사용된 가중치를 확인할 수 있습니다. PFC2에서 사용하는 로드 공유는 흐름별 로드 공유일 뿐입니다. 패킷별 로드 공유를 활성화하지 않습니다.

```
Cat6k> (enable) show mls entry cef ip 192.168.254.253/32
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
---
15 resolved 192.168.254.253 255.255.255.255 point2point 1
192.168.222.2 1
192.168.199.2 1
```

4. 다음 명령을 실행하여 해당 대상 항목의 인접성을 확인합니다.

```
cat6k> (enable) show mls entry cef ip 192.168.254.253/32 adjacency
Mod : 15
Destination-IP : 192.168.254.253 Destination-Mask : 255.255.255.255
FIB-Type : resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect point2point 00-00-08-00-04-00 1025 ARPA 0 0
connect 192.168.222.2 00-90-21-41-c4-07 222 ARPA 0 0
connect 192.168.199.2 00-90-21-41-c4-17 199 ARPA 0 0
```

사례 연구 4: 기본 라우팅

라우팅 테이블이 어떤 모양이든지 Supervisor Engine 2에는 다른 이전 항목과 일치하지 않는 패킷을 전달하는 FIB 항목이 항상 있습니다. 다음 명령을 실행하여 이 항목을 볼 수 있습니다.

```
Cat6k> (enable) show mls entry cef ip 0.0.0.0/0
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 default 0.0.0.0 0.0.0.0 192.168.98.2 1
```

보시다시피 이 항목은 마스크 길이가 0인 유일한 항목입니다. 이 기본값은 MSFC2 라우팅 테이블의 기본 경로가 있고 라우팅 테이블의 기본 경로가 없는 섹션에서 설명한 대로 두 가지 유형으로 구성 될 수 있습니다.

MSFC2 라우팅 테이블에 기본 경로가 있음

먼저 MSFC2 라우팅 테이블에 기본 경로가 있는지 확인하는 방법을 결정합니다. 목적지가 0.0.0.0인 경로를 찾거나 라우팅 테이블을 볼 수 있습니다. 기본 경로는 별표(*)로 표시됩니다. 여기서 굵은 글꼴도 표시됩니다.

```
Cat6k-MSFC2# show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "rip", distance 120, metric 1, candidate default path
Redistributing via rip
Last update from 192.168.98.2 on VLAN 98, 00:00:14 ago
Routing Descriptor Blocks:
* 192.168.98.2, from 192.168.98.2, 00:00:14 ago, via VLAN 98
Route metric is 1, traffic share count is 1
Cat6k-MSFC2#sh ip ro | include 0.0.0.0
R* 0.0.0.0/0 [120/1] via 192.168.98.2, 00:00:22, VLAN 98
```

이 경우 기본 경로가 MSFC2 라우팅 테이블에 있으며 RIP(Routing Information Protocol)를 통해 학습됩니다. 그러나 CEF 동작은 이 기본 경로를 학습하는 방식(고정, OSPF, RIP 등)에 관계없이 동일합니다.

이 경우 기본 경로가 있는 경우 항상 마스크 길이가 0이고 다른 접두사와 일치하지 않는 모든 트래픽을 전달하는 데 사용되는 의 FIB-Type이 있는 CEF 항목이 있습니다.

```
Cat6k> (enable) show mls entry cef ip 0.0.0.0/0
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 default 0.0.0.0 0.0.0.0 192.168.98.2 1
Cat6k< (enable) show mls entry cef ip 0.0.0.0/0 adjacency
Mod : 15
Destination-IP : 0.0.0.0 Destination-Mask : 0.0.0.0
FIB-Type : default
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect 192.168.98.2 00-90-21-41-c5-57 98 ARPA 10433743 3052325803
```

FIB는 각 패킷에 대해 순차적으로 검색되므로 가장 긴 일치 첫 번째 항목으로 시작하면 이 기본 FIB는 다른 일치 항목이 없는 패킷에 대해서만 사용됩니다.

라우팅 테이블에 기본 경로 없음

```
Cat6k-MSFC2# show ip route 0.0.0.0
% Network not in table
```

라우팅 테이블에 기본 경로가 없는 경우 Supervisor Engine 2에는 마스크 길이가 0인 FIB 항목이 여전히 있습니다. 그러나 이제 이 항목에는 의 FIB 이 있습니다. 이 와일드카드 FIB는 FIB에 있는 모든 패킷을 삭제하고 FIB의 다른 항목과 일치하지 않는 패킷과 일치시킵니다. 기본 경로가 없으므로 이

러한 패킷을 삭제하는 것이 좋습니다. 이러한 패킷을 MSFC2로 전달할 필요가 없습니다. MSFC2는 이를 삭제합니다. 이 와일드카드 FIB를 사용하면 하드웨어에서 이러한 불필요한 패킷의 삭제를 보장할 수 있습니다.

```
Cat6k> (enable) show mls entry cef ip 0.0.0.0/0
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 wildcard 0.0.0.0 0.0.0.0
```

참고: FIB 테이블이 가득 찬 드문 경우 와일드카드 항목은 여전히 존재하지만 일치하는 패킷을 삭제하는 대신 MSFC2로 전달됩니다. FIB에 256K 접두사가 있고 FIB에 전체 라우팅 테이블 및 ARP 인접성을 저장할 수 없는 경우에만 발생합니다. 그런 다음 MSFC2에 FIB에 없는 라우팅 항목이 있을 수 있으므로 MSFC2로 기본 메커니즘을 전송해야 합니다.

[기타 문제 해결 팁 및 알려진 문제](#)

[show mls cef mac 명령 실행](#)

Supervisor Engine 2에서 패킷을 가져오는 경우 패킷의 대상 MAC 주소가 MSFC2 MAC 주소 중 하나와 동일한 경우에만 잠재적 L3 패킷으로 간주합니다. 다음 명령을 실행하여 이러한 주소가 Supervisor Engine 2의 POV인지 확인할 수 있습니다.

```
Cat6k> (enable) show mls cef mac
Module 15 : Physical MAC-Address 00-d0-00-3f-8b-fc
VLAN Virtual MAC-Address(es)
-----
10 00-00-0c-07-ac-0a
100 00-00-0c-07-ac-64
Module 15 is the designated MSFC for installing CEF entries
```

MSFC2의 물리적 MAC 주소를 볼 수 있습니다. MSFC2의 모든 인터페이스는 동일한 MAC 주소를 사용합니다. 서로 다른 두 인터페이스에서 서로 다른 MAC 주소를 구성할 수 없습니다.) 이 MAC 주소는 MSFC2의 주소와 동일해야 합니다.

```
Cat6k-MSFC2# show interface
VLAN1 is up, line protocol is up
Hardware is Cat6k RP Virtual Ethernet, address is 00d0.003f.8bfc (bia 00d0.003f.8bfc)
?..
```

show mls cef mac 명령은 MSFC가 활성화된 HSRP(Hot Standby Router Protocol) 그룹에 연결된 모든 MAC 주소도 표시합니다. 위의 **show mls cef mac** 명령의 출력은 MSFC가 VLAN 10 및 VLAN 100에 대해 HSRP-active임을 의미합니다. MSFC2에서 다음 명령을 실행하여 이 명령이 올바른지 확인할 수 있습니다.

```
Cat6k-MSFC2# show standby brief
P indicates configured to preempt.
|
Interface Grp Prio P State Active addr Standby addr Group addr
Vl110 10 200 P Active local 192.168.10.2 192.168.10.254
Vl111 11 100 P Standby 192.168.11.1 local 192.168.11.254
Vl198 98 200 Standby 192.168.98.2 local 192.168.98.5
Vl199 99 200 Standby 192.168.99.2 local 192.168.99.5
Vl1100 100 200 P Active local 192.168.100.2 192.168.100.254
Vl1101 101 100 P Standby 192.168.101.2 local 192.168.101.254
```

보시다시피, 상태는 VLAN 10 및 VLAN 100에 대해서만 *Active*. 상태는 구성된 다른 모든 HSRP 그룹에 대해 *standby*입니다. 어떤 이유로든 상태가 다른 VLAN에 대해 시작되는 경우 `show mls cef mac` 명령의 출력은 이 추가 VLAN이 활성 상태가 아님을 반영해야 합니다.

`show mls cef mac` 명령 출력과 명령 출력 사이에 불일치가 있는 경우 이 명령을 실행하면 `show mls cef mac` 명령 목록에서 추가 및 제거된 MAC 주소에 대한 자세한 정보를 제공할 수 있습니다.

```
Cat6k-MSFC2#Cat6k> (enable) show mls rlog 12
SWLOG at 82a7f410: magic 1008, size 51200, cur 82a81ca4, end 82a8bc20
Current time is: 12/28/01,17:09:15
1781 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1780 12/28/01,11:40:05:(RouterConfig)Router_Cfg: process add(3) router intf for mNo 15/1
VLAN 99
1779 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1778 12/28/01,11:40:05:(RouterConfig)Router_Cfg: process add(3) router intf for mNo 15/1
VLAN 99
1777 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1776 12/28/01,11:40:05:(RouterConfig)Router_Cfg: Process add mls entry for mod 15/1
VLAN 99 i/f 1, proto 3, LC 0
1775 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1774 12/28/01,11:40:05:(RouterConfig)Router_Cfg: Process add mls entry for mod 15/1
VLAN 99 i/f 1, proto 2, LC 0
```

이 명령은 `show mls cef mac` 명령 테이블에서 MAC 주소를 추가하거나 제거할 때마다 메시지를 제공합니다.

[새도우 TCAM](#)

이 문서에서는 Supervisor Engine 2에서 `show mls entry cef` 명령 테이블을 확인하는 방법에 대해 설명했습니다. 이 명령은 PFC2의 실제 ASIC(application-specific integrated circuit) 프로그래밍을 정확하게 나타내지 않습니다. 이 ASIC 설정의 새도우 복사본만 나타냅니다. 실제 하드웨어 설정이 새도우 TCAM에 표시되는 것과 일치하지 않아 일부 패킷이 잘못된 다음 홉으로 전달되는 몇 가지 알려진 문제가 있습니다. 이러한 문제는 Cisco 버그 ID CSCdv49956 ([등록된 고객만 이](#)) 및 CSCdu85211 ([등록된 고객만 해당](#))에 설명되어 있으며, 모두 CatOS 소프트웨어 버전 6.3(3), 7.1(1) 이상에서 고정되어 있습니다.

[기본 라우팅 끊김](#)

초기 버전의 코드에서 버그가 발견되어 기본 경로로 전달이 EIGRP(Enhanced Interior Gateway Routing Protocol) 또는 OSPF에서 작동하지 않습니다. 이 내용은 Cisco 버그 ID CSCdt54036 ([등록된 고객만 해당](#)) 및 Supervisor Engine 이미지의 경우 CatOS 소프트웨어 버전 6.1(3) 이상과 MSFC2 이미지의 경우 Cisco IOS Software Release 12.1(6)E1에 고정되어 있습니다.

[관련 정보](#)

- [MSFC를 사용하여 Catalyst 6000 스위치에서 IP MLS 구성 및 문제 해결](#)
- [LAN 제품 지원 페이지](#)
- [LAN 스위칭 지원 페이지](#)
- [툴 및 유틸리티](#)

- [Technical Support - Cisco Systems](#)