

Supervisor Engine 720 및 Cisco IOS System Software가 포함된 Catalyst 6500/6000 Series 스위치 CEF와 관련된 유니캐스트 IP 라우팅 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[CEF 개요](#)

[인접성 테이블](#)

[RP에서 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](#)

[문제 해결 단계](#)

[사례 연구 4:기본 라우팅](#)

[라우팅 테이블에 기본 경로가 있음](#)

[라우팅 테이블에 기본 경로가 없습니다.](#)

[기타 문제 해결 팁 및 알려진 문제](#)

[DFC 기반 라인 카드](#)

[IP 라우팅 비활성화](#)

[IP CEF와 MLS CEF의 차이점](#)

[관련 정보](#)

소개

이 문서는 Supervisor Engine 720, PFC3(Policy Feature Card 3), MSFC3(Multilayer Switch Feature Card 3)을 사용하여 Cisco Catalyst 6500/600 Series 스위치에서 유니캐스트 IP 라우팅을 트러블슈팅하기 위한 지침으로 사용됩니다. Cisco CEF(Express Forwarding)는 Supervisor Engine 720에서 유니캐스트 라우팅을 수행하는 데 사용됩니다. 이 문서는 Supervisor Engine 720, PFC3, MSFC3을 사용하는 Catalyst 6500/600 Series 스위치의 IP 라우팅에 대해서만 다룹니다. 이 문서는

수퍼바이저 엔진 1 또는 1A 레이어에 대해 Catalyst 6550000/600000000에 대해서는 유효하지 않습니다. 스위치 모듈(MSM). 이 문서는 Supervisor Engine에서 Cisco IOS® 소프트웨어를 실행하는 스위치에만 유효합니다. 이 문서는 Cisco Catalyst OS(CatOS) 시스템 소프트웨어에 유효하지 않습니다.

참고: 이 문서를 사용하여 Supervisor Engine 2 및 MSFC2를 사용하여 Catalyst 6500/6000 스위치에서 유니캐스트 IP 라우팅 문제를 해결할 수도 있습니다.

참고: 이 문서에서는 각각 MSFC 및 PFC 대신 RP(Route Processor) 및 SP(Switch Processor)라는 용어를 사용합니다.

[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 팀 표기 규칙을 참고하십시오.](#)

[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 720을 사용하는 Catalyst 6500/6000은 SP에 구현되는 하드웨어 기반 CEF 포워딩 메커니즘을 사용합니다. CEF는 주로 두 개의 테이블을 사용하여 라우팅에 필요한 정보를 저장합니다.

- FIB(Forwarding Information Base) 테이블
- 인접성 테이블

CEF는 FIB를 사용하여 IP 목적지 접두사 기반 스위칭 결정을 합니다. CEF는 가장 긴 일치 항목을 먼저 확인합니다. FIB는 라우팅 테이블 또는 정보 베이스와 개념적으로 비슷합니다. FIB는 IP 라우팅 테이블에 포함된 전달 정보의 미리 이미지를 유지 관리합니다. 네트워크에서 라우팅 또는 토폴로지 변경이 발생하면 IP 라우팅 테이블에서 업데이트가 수행됩니다. FIB는 변경 사항을 반영합니다. FIB는 IP 라우팅 테이블의 정보를 기반으로 다음 hop 주소 정보를 유지 관리합니다. FIB 항목과 라우팅 테이블 항목 간의 일대일 상관관계 때문에 FIB에는 알려진 모든 경로가 포함됩니다. 따라서 빠른 스위칭 및 최적 스위칭 같은 스위칭 경로와 연결된 경로 캐시 유지 관리가 필요하지 않습니다. 일치가 기본값이든 와일드카드든 FIB에는 항상 일치가 있습니다.

[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. 전체 FIB 항목에는 최종 IP 대상

에 도달할 수 있는 다음 홉에 대한 L2 재작성 정보가 들어 있는 인접성 테이블의 위치에 대한 포인터가 포함됩니다. Supervisor Engine 720 시스템에서 하드웨어 CEF가 Catalyst 6500/6000에서 작동하려면 MSFC3에서 IP CEF를 실행해야 합니다.

RP에서 FIB 및 인접성 테이블을 읽는 방법

SP의 FIB 테이블은 RP의 FIB 테이블과 정확히 같아야 합니다. RP에서 TCAM(ternary content addressable memory)은 FIB에 모든 IP 접두사를 저장합니다. 접두사의 정렬은 마스크 길이에 따라 발생하며 가장 긴 마스크로 시작합니다. 먼저 호스트 항목인 32의 마스크가 있는 모든 항목을 찾습니다. 다음으로 마스크 길이가 31인 모든 항목을 찾습니다. 마스크 길이가 0인 항목이 기본 항목인 경우 까지 계속됩니다. FIB는 순차적으로 읽고 첫 번째 적중은 일치로 사용됩니다. RP에서 다음 샘플 FIB 테이블을 고려하십시오.

```
Cat6500-A#show ip cef
Prefix                Next Hop                Interface
0.0.0.0/0             14.1.24.1               FastEthernet2/48
0.0.0.0/32            receive
14.1.24.0/24          attached                FastEthernet2/48
14.1.24.0/32          receive
14.1.24.1/32          14.1.24.1               FastEthernet2/48
14.1.24.111/32        receive
14.1.24.179/32        14.1.24.179             FastEthernet2/48
14.1.24.255/32        receive
100.100.100.0/24      attached                TenGigabitEthernet6/1
100.100.100.0/32      receive
100.100.100.1/32      100.100.100.1           TenGigabitEthernet6/1
100.100.100.2/32      receive
100.100.100.255/32    receive
112.112.112.0/24      attached                FastEthernet2/2
112.112.112.0/32      receive
112.112.112.1/32      receive
112.112.112.2/32      112.112.112.2           FastEthernet2/2
112.112.112.255/32    receive
127.0.0.0/8           attached                EOBC0/0
127.0.0.0/32          receive
127.0.0.51/32         receive
127.255.255.255/32    receive
Prefix                Next Hop                Interface
222.222.222.0/24      100.100.100.1           TenGigabitEthernet6/1
223.223.223.1/32      100.100.100.1           TenGigabitEthernet6/1
224.0.0.0/4           drop
224.0.0.0/24          receive
255.255.255.255/32    receive
```

각 항목은 다음 필드로 구성됩니다.

- Prefix(접두사) - 관련된 대상 IP 주소 또는 IP 서브넷
- Next Hop—이 접두사와 연결된 다음 가능한 Next Hop 값은 다음과 같습니다. receive - MSFC 인터페이스와 연결된 접두사입니다. 이 항목에는 레이어 3(L3) 인터페이스의 IP 주소에 해당하는 32의 마스크가 포함된 접두사가 포함되어 있습니다. attached - 연결된 네트워크와 연결된 접두사입니다. 다음 홉의 IP 주소 drop(삭제) - 가 있는 항목과 일치하는 모든 패킷이 삭제됩니다.
- Interface(인터페이스) - 대상 IP 주소 또는 IP 서브넷에 대한 발신 인터페이스입니다.

전체 인접성 테이블을 보려면 다음 명령을 실행합니다.

```
Cat6500-A#show adjacency TenGigabitEthernet 6/1 detail
```

| Protocol | Interface | Address |
|----------|-----------------------|----------------------------------|
| IP | TenGigabitEthernet6/1 | 100.100.100.1(9) |
| | | 5570157 packets, 657278526 bytes |
| | | 00D0022D3800 |
| | | 00D0048234000800 |
| ARP | | 03:43:51 |
| | | Epoch: 0 |

문제 해결 방법

이 섹션에서는 문제 해결 예와 세부 정보를 제공합니다. 그러나 먼저, 이 섹션에서는 특정 IP 주소에 대한 연결성 또는 연결성 문제를 해결하는 방법을 요약합니다. SP의 CEF 테이블은 RP의 CEF 테이블을 미러링합니다. 따라서 RP에서 알려진 정보가 올바르면 SP는 IP 주소에 도달하기 위한 올바른 정보만 보유하고 있습니다. 따라서 항상 이 정보를 확인해야 합니다.

RP에서

다음 단계를 완료하십시오.

1. RP 테이블의 IP 라우팅에 있는 정보가 올바른지 확인합니다. `show ip route` 명령을 실행하고 출력에 예상 다음 홉이 포함되어 있는지 확인합니다. **참고:** `show ip route x.x.x.x` 명령을 대신 실행하는 경우 전체 라우팅 테이블을 찾아볼 필요가 없습니다. 출력에 예상 next hop이 포함되지 않은 경우 컨피그레이션 및 라우팅 프로토콜 인접 디바이스를 확인합니다. 또한 실행하는 라우팅 프로토콜과 관련된 기타 트러블슈팅 절차를 수행합니다.
2. next hop 또는 연결된 네트워크의 경우 최종 목적지에 RP에 올바른 ARP(Address Resolution Protocol) 항목이 있는지 확인합니다. `show ip arp next_hop_ip_address` 명령을 실행합니다. ARP 항목의 확인 및 항목에 올바른 MAC 주소가 포함되어 있는지 확인합니다. MAC 주소가 올바르지 않으면 다른 장치가 해당 IP 주소를 소유하고 있는지 확인해야 합니다. 결국 MAC 주소를 소유하는 디바이스를 연결하는 포트의 스위치 레벨을 추적해야 합니다. 불안정한 ARP 항목은 RP가 해당 호스트로부터 응답을 받지 못했음을 나타냅니다. 호스트가 실행 중인지 확인합니다. 호스트에서 스니퍼를 사용하여 호스트가 ARP 응답을 수신하고 올바르게 응답하는지 확인할 수 있습니다.
3. RP의 CEF 테이블에 올바른 정보가 포함되어 있고 인접성이 해결되었는지 확인합니다. 다음 단계를 완료하십시오. CEF 테이블의 다음 홉이 IP 라우팅 테이블의 다음 홉과 일치하는지 확인하려면 `show ip cef destination_network` 명령을 실행합니다. 이 섹션의 1단계에서 다음 홉입니다. `show adjacency detail`을 실행합니다. | `next_hop_ip_address` 명령을 시작하여 인접성이 올바른지 확인합니다. 이 항목의 ARP는 이 섹션의 2단계와 동일한 MAC 주소를 포함해야 합니다.

이 섹션의 1단계와 2단계에서 올바른 결과를 제공하지만 3a 또는 3b 단계에 장애가 발생하면 Cisco IOS Software CEF 문제가 발생합니다. 이 문제는 Catalyst 6500/6000과 관련된 플랫폼별 문제가 아닐 수 있습니다. ARP 테이블 및 IP 라우팅 테이블을 지워야 합니다.

SP에서

다음 단계를 완료하십시오.

1. SP에 저장되는 FIB 정보가 올바르고 RP의 CEF 테이블이 저장하는 정보와 일치하는지 확인합니다. **참고:** CEF 테이블의 정보는 RP 섹션에서의 3단계에서 가져옵니다. `show mls cef lookup destination_ip_network detail` 명령을 실행하고 인접성 항목이 있는지 확인합니다. 정보가 없는 경우 RP와 SP 간에 통신 문제가 발생합니다. 이 문제는 Catalyst 6500/6000 플랫폼별

기능과 관련이 있습니다. 실행하는 특정 Cisco IOS 소프트웨어 릴리스에 대해 알려진 버그가 없는지 확인합니다. 올바른 항목을 복원하려면 RP에서 **clear ip route** 명령을 실행합니다.

2. SP에서 인접성 테이블을 확인하려면 **show mls cef adjacency entry adjacency_entry_number detail** 명령을 실행합니다. 엔트리에 RP 섹션의 2단계 및 3b에서 확인한 주소와 동일한 목적지 MAC 주소가 포함되어 있는지 확인합니다. SP의 인접성이 3b단계에서 다음 홉의 인접성과 일치하지 않으면 RP와 SP 간의 내부 통신 문제가 발생할 수 있습니다. 올바른 정보를 복원하려면 인접성을 지워 보십시오.

사례 연구 1: 직접 연결된 네트워크의 호스트에 연결

이 간단한 사례는 이러한 호스트 간의 연결에 대한 연구를 제공합니다.

- IP 주소가 112.112.112.2인 네트워크 112.112.112.0/24의 호스트 A
- IP 주소가 222.222.222.2인 네트워크 222.222.222.0/24의 호스트 B

관련 RP 컨피그레이션입니다.

```
interface TenGigabitEthernet4/1
ip address 100.100.100.1 255.255.255.0
```

```
! interface GigabitEthernet5/5
ip address 222.222.222.1 255.255.255.0
```

중요 참고 사항: Supervisor Engine 720 및 MSFC3을 사용하는 Catalyst 6500/6000 플랫폼은 하드웨어에서 CEF를 사용하여 라우팅을 수행합니다. CEF에 대한 컨피그레이션 요건이 없으며 MSFC3에서 CEF를 비활성화할 수 없습니다.

문제 해결 단계

IP 주소 222.222.222.2에 도달할 경로를 확인하려면 이 문서의 [Troubleshooting Method](#) 섹션에 있는 절차를 따르십시오.

1. IP 라우팅 테이블을 확인하려면 다음 두 명령 중 하나를 실행합니다.

```
Cat6500-B#show ip route 222.222.222.2
Routing entry for 222.222.222.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Redistributing via eigrp 100
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet5/5
    Route metric is 0, traffic share count is 1
```

또는

```
Cat6500-B#show ip route | include 222.222.222.0
C    222.222.222.0/24 is directly connected, GigabitEthernet5/5
```

이러한 명령 출력에서 대상이 직접 연결된 서브넷에 있음을 확인할 수 있습니다. 따라서 목적지에 가는 다음 홉은 없습니다.

2. RP에서 ARP 항목을 확인합니다. 이 경우 대상 IP 주소에 대한 ARP 항목이 있는지 확인합니다. 다음 명령을 실행합니다.

```
Cat6500-B#show ip arp 222.222.222.2
Protocol  Address          Age (min)  Hardware Addr  Type   Interface
Internet  222.222.222.2    41         0011.5c85.85ff ARPA    GigabitEthernet5/5
```

3. RP에서 CEF 및 인접성 테이블을 확인합니다. CEF 테이블을 확인하려면 다음 명령을 실행합

니다.

```
Cat6500-B#show ip cef 222.222.222.2
222.222.222.2/32, version 10037, epoch 0, connected, cached adjacency
 222.222.222.2
0 packets, 0 bytes
  via 222.222.222.2, GigabitEthernet5/5, 0 dependencies
   next hop 222.222.222.2, GigabitEthernet5/5
   valid cached adjacency
```

마스크 길이가 32인 유효한 CEF 항목이 있음을 확인할 수 있습니다. 또한 유효한 캐시된 인접성이 있음을 확인할 수 있습니다. 인접성 테이블을 확인하려면 다음 명령을 실행합니다.

```
Cat6500-B#show adjacency detail | begin 222.222.222.2
IP          GigabitEthernet5/5      222.222.222.2(7)
                                481036 packets, 56762248 bytes
                                00115C8585FF
                                00D0022D38000800
                                ARP          03:10:29
                                Epoch: 0
```

이 출력은 인접성이 있음을 보여줍니다. 인접성의 대상 MAC 주소는 이 섹션의 2단계 ARP 테이블에 있는 MAC 주소와 동일한 정보를 표시합니다.

4. SP 관점에서 올바른 CEF/FIB 항목이 있는지 확인합니다. FIB에는 두 가지 흥미로운 항목이 있습니다. 다음 출력에 표시되는 대상 IP 주소의 항목:

```
Cat6500-B#show mls cef ip 222.222.222.2 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority
       bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket
       sel
       V0 - Vlan 0, C0 - don't comp bit 0, V1 - Vlan 1, C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(90      ): E | 1 FFF 0 0 0 0   255.255.255.255
V(90      ): 8 | 1 0   0 0 0 0   222.222.222.2      (A:327680 ,P:1,D:0,m:0 ,
B:0 )
```

이 항목은 이미 알려진 next hop이 있는 호스트 항목입니다. 이 경우 다음 홉은 대상 자체입니다. 다음 출력에 표시된 대로 대상 네트워크에 해당하는 항목입니다.

```
Cat6500-B#show mls cef ip 222.222.222.0 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority
       bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket
       sel
       V0 - Vlan 0, C0 - don't comp bit 0, V1 - Vlan 1, C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(88      ): E | 1 FFF 0 0 0 0   255.255.255.255
V(88      ): 8 | 1 0   0 0 0 0   222.222.222.0      (A:13      ,P:1,D:0,m:0 ,
B:0 )
M(3207    ): E | 1 FFF 0 0 0 0   255.255.255.0
V(3207    ): 8 | 1 0   0 0 0 0   222.222.222.0      (A:14      ,P:1,D:0,m:0 ,
B:0 )
```

이 항목은 연결된 FIB 항목입니다. 이 엔트리에 도달하는 모든 패킷은 추가 처리를 위해 RP로 리디렉션됩니다. 이 프로세싱에는 주로 ARP 전송과 ARP 확인 대기 작업이 포함됩니다. FIB는 순서대로 찾아지며 가장 긴 마스크 길이로 시작합니다. 대상 IP 주소에 대한 항목과 대상 네트워크에 대한 항목이 모두 있는 경우 SP는 마스크 32가 있는 첫 번째 항목을 사용합니다. 이 항목은 호스트 항목입니다. 덜 구체적인 FIB 테이블 항목은 고려하지 않습니다. /32 항목이 없으면 SP는 대상 네트워크의 항목인 두 번째 항목을 사용합니다. 이 항목이 연결된 항목인 것처럼

SP는 추가 처리를 위해 패킷을 RP로 리디렉션합니다.RP는 대상 마스크에 대한 ARP 요청을 보낼 수 있습니다.ARP 회신을 수신하면 RP의 해당 호스트에 대해 ARP 테이블 및 인접성 테이블이 완성됩니다.

5. 마스크 길이가 32인 올바른 FIB 항목이 있는 경우 해당 호스트에 대해 인접성이 올바르게 입력되었는지 확인합니다.다음 명령을 실행합니다.

```
Cat6500-B#show mls cef adjacency entry 327680 detail
```

```
Index: 327680 smac: 00d0.022d.3800, dmac: 0011.5c85.85ff
mtu: 1518, vlan: 1021, dindex: 0x0, l3rw_vld: 1
format: MAC_TCP, flags: 0x8408
delta_seq: 0, delta_ack: 0
packets: 0, bytes: 0
```

참고: 인접성이 채워지며 대상 MAC(d_{mac}) 필드에는 호스트 B의 유효한 MAC 주소가 포함됩니다. 이 주소는 이 섹션의 2단계와 3b단계에서 확인한 주소입니다.**참고:** 및 수는 0입니다. 인그레스 모듈에 DFC(Distributed Forwarding Card)가 있는 경우 패킷/바이트 수를 가져오려면 모듈에 로그인해야 합니다.Other Troubleshooting [Tips and Known Issues\(기타 문제 해결 팁 및 알려진 문제\)](#) 섹션에서는 이 프로세스에 대해 설명합니다.

발언 및 결론

문제 해결 [단계](#)의 4단계에서 언급했듯이, 일치하는 FIB 항목이 두 개 있습니다.제품:

- 네트워크 항목(이 경우 222.222.222.0/24) - 이 항목은 항상 표시되며 MSFC의 라우팅 및 CEF 테이블에서 직접 가져옵니다.이 네트워크는 항상 라우팅 테이블에 직접 연결됩니다.
- 대상 호스트 항목(이 경우 222.222.222.2/32) - 이 항목이 반드시 없을 수도 있습니다.항목이 없으면 SP에서 네트워크 항목을 사용하며 다음 이벤트가 발생합니다.SP는 패킷을 RP에 전달합니다.PFC의 FIB 테이블은 마스크 길이가 32인 호스트 항목을 생성합니다. 그러나 아직 완전한 CEF 인접성이 없으므로 유형으로 인접성이 생성됩니다.해당 대상에 대한 후속 패킷이 /32 엔트리에 도달하고 패킷이 삭제됩니다.동시에 RP로 전송된 원래 패킷은 MSFC를 트리거하여 ARP 요청을 전송합니다.ARP의 해결 시 ARP 항목이 완료됩니다.RP에서 인접성이 완료됩니다.인접성 업데이트가 SP로 이동하여 기존 인접성을 완료합니다.SP는 MAC 주소 재작성을 반영하기 위해 호스트 인접성을 변경합니다.인접성 유형이 연결된 인터페이스로 변경됩니다.ARP의 해결을 기다리는 동안 인접성을 설치하는 이 메커니즘에는 이름이 "ARP throttle"입니다.ARP 스로틀은 모든 패킷을 RP로 전달하거나 여러 ARP 요청을 생성하지 않도록 하는 데 유용합니다.RP로 전송되는 첫 번째 몇 개의 패킷만 있고, PFC는 인접성이 완료될 때까지 나머지 패킷을 삭제합니다.또한 ARP 스로틀을 사용하면 직접 연결된 네트워크에서 존재하지 않거나 응답하지 않는 호스트로 전달되는 트래픽을 삭제할 수 있습니다.

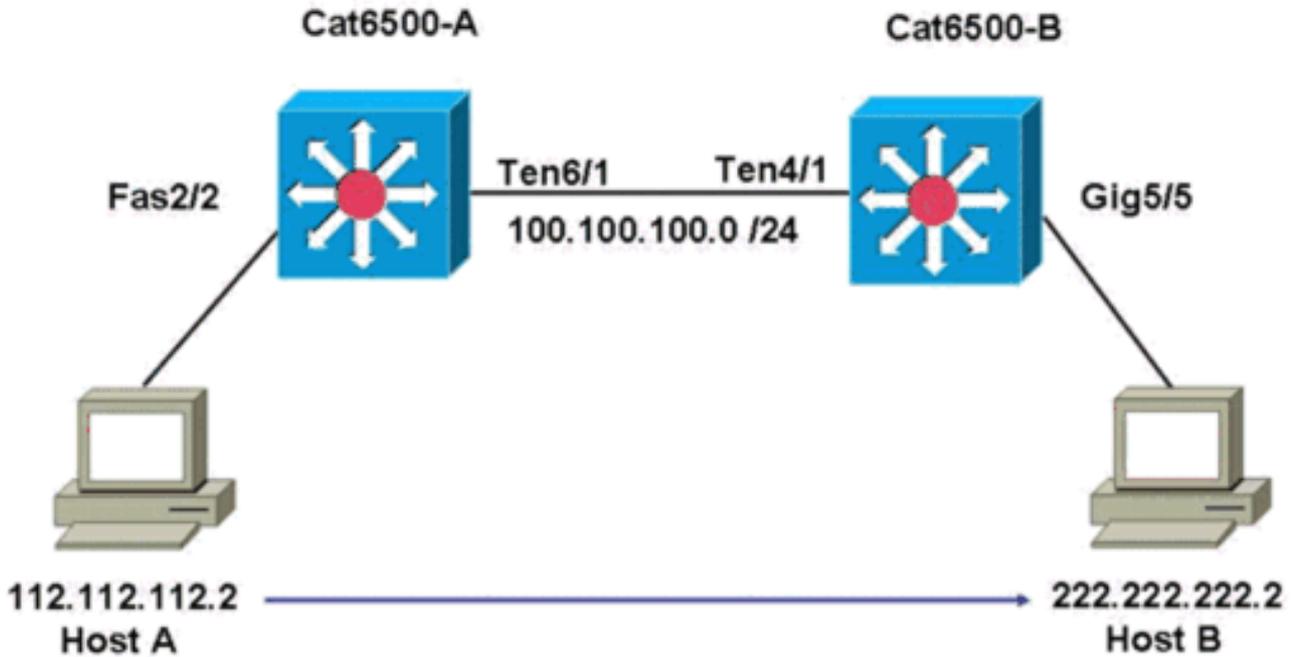
서로 다른 두 VLAN에서 두 사용자 간의 연결을 트러블슈팅할 때 다음 사항을 고려해야 한다는 점을 항상 염두에 두십시오.

- 대상 IP 주소 호스트 B를 만들기 위해 [Troubleshooting Method](#)를 사용하여 호스트 A에서 호스트 B로 이동하는 트래픽
- 동일한 트러블슈팅 [방법](#)을 사용하지만 목적지가 호스트 A로 사용되는 호스트 B에서 호스트 A로 이동하는 트래픽

또한 소스의 기본 게이트웨이에서 출력을 가져와야 합니다.호스트 A에서 호스트 B로 이동하는 트래픽과 호스트 B에서 호스트 A로 이동하는 트래픽이 반드시 동일하지는 않습니다.

[사례 연구 2:원격 네트워크에 연결](#)

이 섹션의 다이어그램에서 IP 주소가 222.222.222.2인 112.112.112.2 ping 호스트 B인 호스트 A를 사용합니다. 그러나 이번에는 호스트 B가 Cat6500-A 스위치에 직접 연결되어 있지 않습니다. 호스트 B는 두 개의 라우팅된 홉입니다. Cat6500-B 스위치에서 CEF 라우팅 경로를 따르려면 동일한 방법을 사용합니다.



문제 해결 단계

다음 단계를 완료하십시오.

1. Cat6500-A에서 라우팅 테이블을 확인하려면 다음 명령을 실행합니다.

```
Cat6500-A#show ip route 222.222.222.2
Routing entry for 222.222.222.0/24
  Known via "ospf 100", distance 110, metric 2, type intra area
  Last update from 100.100.100.1 on TenGigabitEthernet6/1, 00:00:37 ago
  Routing Descriptor Blocks:
    * 100.100.100.1, from 222.222.222.1, 00:00:37 ago, via TenGigabitEthernet6/1
      Route metric is 2, traffic share count is 1
```

이 출력에서 IP 주소 222.222.222.2을 사용하여 호스트 B에 도달하기 위해 OSPF(Open Shortest Path First) 프로토콜 경로가 있음을 확인할 수 있습니다. 다음 홉으로 TenGigabitEthernet6/1을 사용하여 IP 주소 100.100.100.1을 사용하여 호스트에 연결해야 합니다.

2. RP에서 ARP 테이블을 확인하려면 다음 명령을 실행합니다. 참고: 최종 목적지가 아닌 다음 홉의 ARP 항목을 확인합니다.

```
Cat6500-A#show ip arp 100.100.100.1
Protocol Address Age (min) Hardware Addr Type Interface
Internet 100.100.100.1 27 00d0.022d.3800 ARPA TenGigabitEthernet6/1
```

3. RP에서 CEF 테이블 및 인접성 테이블을 확인하려면 다음 명령을 실행합니다.

```
Cat6500-A#show ip cef 222.222.222.2
222.222.222.0/24, version 6876, epoch 0, cached adjacency 100.100.100.1
0 packets, 0 bytes
  via 100.100.100.1, TenGigabitEthernet6/1, 0 dependencies
    next hop 100.100.100.1, TenGigabitEthernet6/1
```

valid cached adjacency

대상 네트워크에 대한 CEF 항목이 있음을 확인할 수 있습니다. 또한 다음 홉의 결과는 1단계의 라우팅 테이블에 있는 것과 일치합니다.

4. 다음 홉의 인접성 테이블을 확인하려면 다음 명령을 실행합니다.

```
Cat6500-A#show adjacency detail | begin 100.100.100.1
IP          TenGigabitEthernet6/1      100.100.100.1(9)
                2731045 packets, 322263310 bytes
                00D0022D3800
                00D0048234000800
                ARP          03:28:41
                Epoch: 0
```

다음 홉에 유효한 인접성이 있으며, 대상 MAC 주소는 2단계의 ARP 항목과 일치합니다.

5. SP에서 FIB 테이블을 확인하려면 다음 명령을 실행합니다.

```
Cat6500-A#show mls cef ip lookup 222.222.222.2 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0, C0 - don't comp bit 0, V1 - Vlan 1, C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(3203  ): E | 1 FFF  0 0 0 0   255.255.255.0
V(3203  ): 8 | 1 0   0 0 0 0   222.222.222.0   (A:163840 ,P:1,D:0,m:0 ,B:0 )
```

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

6. SP에서 인접성을 확인하려면 다음 명령을 실행합니다.

```
Cat6500-A#show mls cef adjacency entry 163840 detail

Index: 163840 smac: 00d0.0482.3400, dmac: 00d0.022d.3800
            mtu: 1518, vlan: 1018, dindex: 0x0, l3rw_vld: 1
            format: MAC_TCP, flags: 0x8408
            delta_seq: 0, delta_ack: 0
            packets: 726, bytes: 85668
```

참고: 및 카운터는 실시간으로 이루어집니다. 트래픽이 중지되면 카운터가 0으로 돌아갑니다.

발언 및 결론

이러한 [트러블슈팅 단계](#)는 원격 네트워크에 연결하기 위해 Cat6500-A 스위치에서 연결을 확인합니다. 이 단계는 [사례 연구 1](#) 섹션의 [문제 해결 단계](#)와 유사합니다. [직접 연결된 네트워크의 호스트에 대한 연결](#). 그러나 몇 가지 차이점이 있습니다. [사례 연구 2](#)의 [트러블슈팅 단계](#)에서 [원격 네트워크에 대한 연결](#)을 수행하려면 다음을 수행해야 합니다.

- IP 라우팅 테이블, CEF 테이블 및 FIB에서 최종 대상을 확인합니다. 1, 3, 5단계에서 이 체크 인을 수행합니다.
- ARP 테이블 및 인접성 테이블에서 다음 hop 정보를 확인합니다. 2단계와 4단계에서 이 체크 인을 수행합니다.
- 최종 대상의 인접성을 확인합니다. 6단계에서 이 검사를 수행합니다.

사례 연구 3: 여러 개의 다음 홉으로 로드 밸런싱

문제 해결 단계

이 사례 연구에서는 동일한 목적지 네트워크에 연결하기 위해 몇 개의 다음 홉과 여러 경로를 사용할 수 있는 경우 어떤 일이 발생하는지 설명합니다.

- 라우팅 테이블을 확인하여 동일한 목적지 IP 주소에 연결할 수 있는 다른 경로와 다른 다음 홉이 있는지 확인합니다. 이 라우팅 테이블의 샘플 섹션에서는 대상 IP 주소 222.222.222.2에 도달하기 위해 사용할 수 있는 2개의 경로와 2개의 다음 홉이 있습니다.

```
Cat6500-A#show ip route | begin 222.222.222.0
O    222.222.222.0/24
      [110/2] via 100.100.100.1, 00:01:40, TenGigabitEthernet6/1
      [110/2] via 111.111.111.2, 00:01:40, FastEthernet2/1
```

- 다음 세 홉의 각 ARP 항목을 확인합니다. 다음 단계를 완료하십시오. 대상에 대한 CEF 테이블을 확인합니다. 대상에 RP의 CEF 테이블에 두 개의 서로 다른 항목이 표시됩니다. Cisco IOS Software CEF는 서로 다른 경로 간에 로드 공유를 수행할 수 있습니다.

```
Cat6500-A#show ip cef 222.222.222.2
222.222.222.0/24, version 6893, epoch 0
0 packets, 0 bytes
  via 100.100.100.1, TenGigabitEthernet6/1, 0 dependencies
    traffic share 1
    next hop 100.100.100.1, TenGigabitEthernet6/1
    valid adjacency
  via 111.111.111.2, FastEthernet2/1, 0 dependencies
    traffic share 1
    next hop 111.111.111.2, FastEthernet2/1
    valid adjacency
0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
        internal 0 packets, 0 bytes
```

다음 두 홉의 ARP 항목을 확인합니다.

```
Cat6500-A#show ip arp 100.100.100.1
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 100.100.100.1    13        00d0.022d.3800 ARPA   TenGigabit
Ethernet6/1
Cat6500-A#show ip arp 111.111.111.2
Protocol Address      Age (min)  Hardware Addr  Type   Interface
Internet 111.111.111.2    0         00d0.022d.3800 ARPA   FastEthernet2/1
```

RP 인접성 테이블에서 두 인접성을 확인합니다.

```
Cat6500-A#show adjacency detail
Protocol Interface      Address
IP          TenGigabitEthernet6/1  100.100.100.1(23)
62471910 packets, 7371685380 bytes
00D0022D3800
00D0048234000800
ARP          03:34:26
Epoch: 0
IP          FastEthernet2/1      111.111.111.2(23)
0 packets, 0 bytes
00D0022D3800
Address
00D0048234000800
ARP          03:47:32
Epoch: 0
```

2b단계와 2c단계의 정보가 일치해야 합니다.

- 동일한 대상에 대해 두 개의 서로 다른 FIB 항목이 설치되어 있습니다. PFC의 하드웨어 CEF는 동일한 대상에 대해 최대 16개의 서로 다른 경로 공유를 로드할 수 있습니다. 기본값은 src_dst IP 로드 공유입니다.

```
Cat6500-A#show mls cef ip 222.222.222.0
Codes: decap - Decapsulation, + - Push Label
Index Prefix      Adjacency
3203 222.222.222.0/24 Te6/1          , 00d0.022d.3800 (Hash: 007F)
```

4. 트래픽을 전달하는 데 사용되는 정확한 경로를 확인합니다. 다음 명령을 실행합니다.

```
Cat6500-A#show ip cef exact-route 111.111.111.2 222.222.222.2
111.111.111.2 -> 222.222.222.2 : TenGigabitEthernet6/1 (next hop 100.100.100.1)
```

사례 연구 4: 기본 라우팅

라우팅 테이블이 어떤 모양이든지 Supervisor Engine 720에는 다른 이전 항목과 일치하지 않는 패킷을 전달하는 FIB 항목이 항상 있습니다. 이 항목을 보려면 다음 명령을 실행합니다.

```
Cat6500-A#show mls cef ip 0.0.0.0
```

```
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 0.0.0.0/32 receive
134368 0.0.0.0/0 Fa2/48 , 000c.3099.373f
134400 0.0.0.0/0 drop
```

세 가지 항목이 있습니다. 이 기본값은 두 가지 유형 중 하나일 수 있습니다.

- [라우팅 테이블에 기본 경로가 있음](#)
- [라우팅 테이블에 기본 경로가 없습니다.](#)

라우팅 테이블에 기본 경로가 있음

먼저 RP 라우팅 테이블에 기본 경로가 있는지 확인합니다. 목적지가 0.0.0.0인 경로를 찾거나 라우팅 테이블을 볼 수 있습니다. 기본 경로는 별표(*)로 표시됩니다. 여기서 기본 경로는 굵은 글꼴 텍스트에도 나타납니다.

```
Cat6500-A#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:
  * 14.1.24.1
    Route metric is 0, traffic share count is 1
```

이 경우 기본 경로가 RP 라우팅 테이블에 있으며 구성된 " " 경로를 통해 알려집니다.

참고: CEF 동작은 고정, OSPF, RIP(Routing Information Protocol) 또는 다른 방법으로 이 기본 경로를 학습하는 방법에 관계없이 동일합니다.

기본 경로가 있는 경우 항상 마스크 길이가 0인 CEF 항목이 있습니다. 이 항목은 다른 접두사와 일치하지 않는 모든 트래픽을 전달합니다.

```
Cat6500-A#show mls cef ip 0.0.0.0
```

```
Codes: decap - Decapsulation, + - Push Label
Index Prefix Adjacency
64 0.0.0.0/32 receive
134368 0.0.0.0/0 Fa2/48 , 000c.3099.373f
134400 0.0.0.0/0 drop
```

CEF는 각 패킷에 대해 순차적으로 FIB를 찾아보고 가장 긴 매칭부터 시작합니다. 따라서 이 기본 FIB는 다른 일치 항목을 찾을 수 없는 패킷에 대해서만 사용됩니다.

라우팅 테이블에 기본 경로가 없습니다.

```
Cat6500-B#show ip route 0.0.0.0
% Network not in table
```

라우팅 테이블에 기본 경로가 없는 경우 Supervisor Engine 720에는 마스크 길이가 0인 FIB 항목이 여전히 있습니다. 이 FIB 항목은 FIB의 다른 항목과 일치하지 않는 패킷과 함께 사용되며 결과적으로 삭제됩니다. 이 삭제는 기본 경로가 없으므로 유용합니다. 이러한 패킷을 RP로 전달할 필요가 없습니다. RP는 패킷을 삭제합니다. 이 FIB 항목을 사용하는 경우 하드웨어에서 이러한 불필요한 패킷의 삭제를 확인합니다. 이 드롭으로 RP의 불필요한 사용률이 방지됩니다. 그러나 패킷이 IP 주소 0.0.0.0으로 향할 경우 해당 패킷은 RP로 이동합니다.

```
Cat6500-B#show mls cef ip 0.0.0.0
```

```
Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
67     0.0.0.0/32             receive
134400 0.0.0.0/0              drop
```

참고: FIB 테이블이 가득 찬 드문 경우에는 FIB 삭제 항목이 여전히 존재합니다. 그러나 엔트리와 일치하는 패킷의 삭제 대신 패킷은 RP로 이동합니다. 이는 FIB에 256,000개 이상의 접두사가 있고 전체 라우팅 테이블에 필요한 공간이 부족한 경우에만 발생합니다.

기타 문제 해결 팁 및 알려진 문제

DFC 기반 라인 카드

트래픽에 대한 인그레스 모듈이 DFC 기반 라인 카드인 경우, 전달 결정은 모듈에서 로컬로 수행됩니다. 하드웨어 패킷 카운터를 확인하려면 모듈에 대한 원격 로그인을 수행합니다. 그런 다음 이 섹션에 나와 있는 대로 명령을 실행합니다.

사례 [연구 2](#)의 예로 [활용: 원격 네트워크에 연결합니다](#). Cat6500-B의 경우 트래픽이 DFC가 있는 모듈 4로 들어갑니다. 모듈에 대한 원격 로그인을 위해 다음 명령을 실행합니다.

```
Cat6500-B#remote login module 4
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Cat6500-B-dfc4#
```

그런 다음 모듈에서 CEF FIB 정보를 확인할 수 있습니다.

```
Cat6500-B-dfc4#show mls cef ip 222.222.222.2 detail
Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0, C0 - don't comp bit 0, V1 - Vlan 1, C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(90   ): E | 1 FFF  0 0 0 0   255.255.255.255
V(90   ): 8 | 1 0   0 0 0 0   222.222.222.2      (A:294912 ,P:1,D:0,m:0 ,B:0 )
```

그런 다음 하드웨어 카운터로 인접성 정보를 확인할 수 있습니다.

```
Cat6500-B-dfc4#show mls cef adjacency entry 294912 detail
Index: 294912 smac: 00d0.022d.3800, dmac: 0011.5c85.85ff
mtu: 1518, vlan: 1021, dindex: 0x0, l3rw_vld: 1
format: MAC_TCP, flags: 0x8408
delta_seq: 0, delta_ack: 0
packets: 4281043, bytes: 505163074
```

IP 라우팅 비활성화

Cisco IOS Software 릴리스 12.1(20)E 이상에서는 Catalyst 6500 Series 스위치에 대해 IP 라우팅 비활성화 지원이 제거되었습니다. 다음 예에서는 다음과 같이 이러한 스위치에서 IP 라우팅을 비활성화할 수 없습니다.

```
Cat6500(config)#no ip routing
Cannot disable ip routing on this platform
```

no ip routing 명령은 Cisco IOS 라우터에서 IP 라우팅을 비활성화하는 데 사용되는 Cisco IOS Software 명령입니다. 일반적으로 이 명령은 로우엔드 라우터에서 사용됩니다.

no ip routing 명령은 **service internal** 명령이 스위치에서 이미 활성화된 경우에만 허용됩니다. 그러나 스위치가 다시 로드되면 컨피그레이션에 저장되지 않으며 손실됩니다. Cisco에서는 Cisco IOS System 소프트웨어를 실행하는 Catalyst 6000/6500 Series 스위치에서 IP 라우팅을 비활성화하지 않는 것이 좋습니다.

이 문제를 해결하려면 **ip route 0.0.0.0 0.0.0.0 a.b.c.d** 명령을 사용합니다. 이 명령에서 **a.b.c.d**는 기본 게이트웨이의 IP 주소입니다. 다음 두 항목이 모두 참인 경우 라우팅 프로세스가 사용되지 않습니다.

- 스위치의 모든 인터페이스를 L2 포트로 구성하려면 switchport 명령을 사용합니다.
- 스위치에 구성된 스위치드 가상 인터페이스(SVI)(VLAN 인터페이스)가 없습니다.

IP CEF와 MLS CEF의 차이점

show mls cef exact-route source-ip 주소 **dest-ip** 주소 및 **show ip cef exact-route source-ip** 주소 **dest-ip** 주소의 출력은 IP CEF를 사용할 때 패킷이 소프트웨어 스위치드이고 MLS CEF를 사용할 때 패킷이 하드웨어 스위치드(hardware switched)되기 때문에 다릅니다. 대부분의 패킷이 하드웨어 스위칭되므로 대상에 도달하기 위한 next-hop을 보는 데 가장 좋은 명령은 **show mls cef exact-route source-ip address dest-ip** 주소입니다.

관련 정보

- [Supervisor Engine 2 및 Running CatOS System Software를 사용하여 Catalyst 6500/6000 Series 스위치에서 CEF를 포함하는 유니캐스트 IP 라우팅 문제 해결](#)
- [MSFC를 사용하여 Catalyst 6500/6000 스위치에서 IP MLS 구성 및 문제 해결](#)
- [LAN 제품 지원 페이지](#)
- [LAN 스위칭 지원 페이지](#)
- [툴 및 리소스](#)
- [기술 지원 및 문서 - Cisco Systems](#)