MPLS의 Traceroute 명령

목차

소개

이 문서에서는 **traceroute** 명령이 MPLS(Multiprotocol Label Switching) 환경에서 작동하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 MPLS 지식

자세한 내용은 초보자용 MPLS FAQ를 참조하십시오.

사용되는 구성 요소

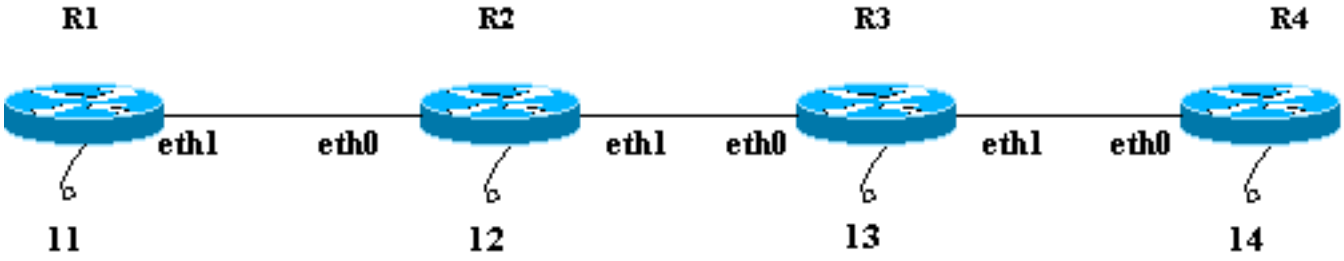
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

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

일반 traceroute 명령

이 섹션에서는 기존 traceroute 명령의 작동 방식에 대해 설명합니다.이 다이어그램은 라우터 1(R1) 및 라우터 4(R4)가 PE(Provider Edge) 라우터이고 라우터 2(R2) 및 라우터 3(R3)이 제공자(P) 라우터인 통신 사업자 설정을 보여줍니다.



이 예에서는 R1에서 R4 루프백 14로 traceroute를 실행합니다. R1은 임의의 대상 포트 값이 32000보다 큰 UDP(User Datagram Protocol) 데이터그램을 사용합니다. 포트 번호에 대해 이러한 높은 값을 선택하면 해당 포트가 원하는 수신자에 존재하지 않는지 확인합니다.이 데이터그램을 IP 패킷에 넣습니다.

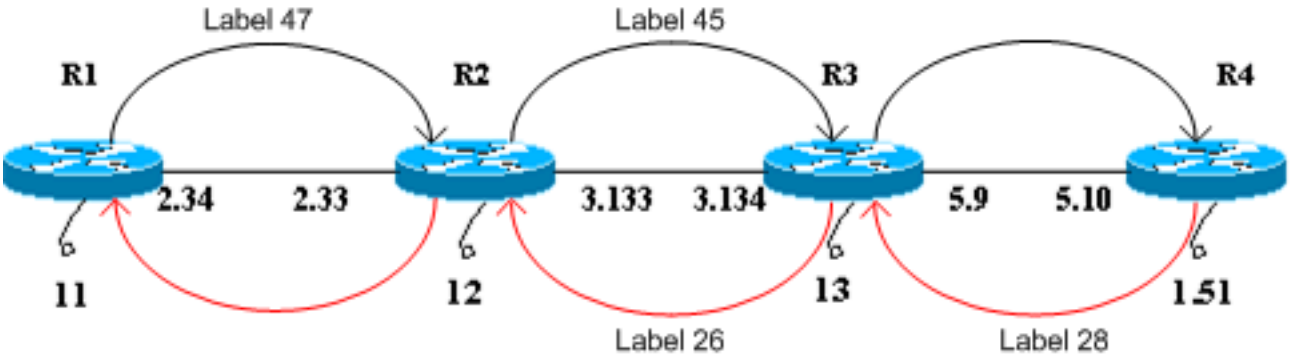
참고: 이 문서에서 IP 패킷이 언급될 때마다 UDP 데이터그램이 포함된 IP 패킷입니다.

정상적인 traceroute 명령에 대한 이벤트 **시퀀스입니다**.

1. R1은 목적지 주소가 14이고 TTL(Time to Live)이 1인 IP 패킷을 eth1 인터페이스를 통해 전송합니다.
2. R2는 패킷을 수신하고 패킷의 TTL이 의도한 수신자가 아니며 1임을 기록합니다. 패킷을 삭제하고 TTL 만료 ICMP(Internet Control Message Protocol) 메시지를 R1로 전송합니다. 이 ICMP 메시지의 소스 주소는 R2 eth0의 IP 주소(원래 패킷을 받은 인터페이스의 주소)입니다.
3. ICMP 메시지를 수신하면 R1은 TTL 2가 eth1 인터페이스를 통해 14로 향하는 다른 IP 패킷을 전송합니다.
4. R2는 패킷을 수신하고 패킷이 의도된 수신자가 아니며 R3을 통해 수신자에게 도달할 수 있음을 기록합니다. TTL을 감소시키고(2에서 1) 패킷을 R3에 전달합니다. R3은 패킷을 수신하고 수신자가 아님을 확인합니다.TTL은 1입니다. 패킷을 삭제하고 eth0 주소를 소스 주소로 사용하여 TTL 만료 ICMP 메시지를 R1로 보냅니다.
5. R1은 ICMP 메시지를 수신하고 TTL 값이 3인 eth1 인터페이스를 통해 다른 IP 패킷을 14로 전송합니다. 도중에 R2와 R3는 TTL을 감소시키고 R4에 전달합니다. R4는 패킷을 가져오고, 패킷이 의도한 수신자임을 확인한 후 UDP 데이터그램의 포트 값에 연결을 시도합니다.R4는 이 포트가 없음을 발견하여 ICMP 오류 메시지를 R1로 전송합니다.이전과 마찬가지로 이 ICMP 메시지의 소스 주소는 R4의 eth0입니다. **traceroute** 프로그램은 이제 해당 소스 주소가 있는 모든 ICMP 오류 메시지를 포함하고 대상에 대한 전체 경로를 가집니다.

MPLS traceroute 명령

모든 라우터, R1~R4를 제외하고 이제 IP 포워딩 대신 레이블 스위칭을 수행합니다. Normal traceroute Command 섹션에 자세히 설명되어 있는 이 시나리오를 생각해 보십시오.이 다이어그램은 테스트 베드 설정입니다.테스트 베드에 표시된 모든 인터페이스는 10.13.0.0 네트워크에 있습니다.



이 문서의 목적은 다음과 같습니다.

- R1은 47이라는 레이블을 사용하여 R4에 연결하고 패킷을 R2로 전달합니다.
- R2는 45라는 레이블을 사용하여 R4에 연결하고 패킷을 R3에 전달합니다.
- R3는 레이블을 팝업하고 패킷을 R4로 전달합니다.
- R4는 28이라는 레이블을 사용하여 R1에 연결하고 패킷을 R3에 전달합니다.
- R3는 26이라는 레이블을 사용하여 R1에 연결하고 패킷을 R2로 전달합니다.
- R2는 레이블을 팝업하고 패킷을 R1에 전달합니다.

이 단계에서는 R1에서 R4 루프백 10.13.1.51로 **traceroute를** 수행하기 위해 이벤트의 순서를 보여줍니다.

1. R1은 레이블이 47이고 TTL이 1인 레이블 전환 패킷을 R2로 보냅니다. IP 패킷의 TTL 필드는 레이블 헤더의 TTL 필드에 복사됩니다.
2. R2는 의도된 수신자가 아니며 TTL은 1입니다. 패킷을 삭제하고 일반 IP 패킷과 마찬가지로 TTL 만료 ICMP 메시지를 생성합니다.이 경우 ICMP 메시지 패킷은 MPLS에 대한 ICMP 확장별로 생성됩니다.
3. R2는 ICMP 메시지에 레이블 47(만료된 수신 레이블)을 추가합니다.패킷을 R1로 직접 전송하지 않습니다.대신 LFIB(Label Forwarding Information Base)를 평가하고 47이라는 레이블로 수신된 패킷에 45라는 레이블을 사용해야 한다는 것을 발견했습니다. 패킷에 45라는 레이블을 지정하고 TTL-expired ICMP 메시지를 R3로 전송합니다.
4. R3은 레이블을 팝업하고 R4로 전송합니다. R4는 대상이 R1임을 확인하고 메시지에 28이라는 레이블을 부여하여 R3과 R2를 통해 R1로 전송합니다.
5. ICMP 오류 메시지는 R1로 다시 전송되기 전에 반대쪽 끝까지 전달됩니다. 다음 예는 그림을 제공합니다

.

R4의 이더넷 인터페이스에서 스니핑된 패킷은 단계 1-5를 확인합니다. 스니퍼 출력에서 **1은 인바운드 패킷이고 2 R4**의 아웃바운드 패킷입니다. 이 토론을 반영하기 위해 출력 형식이 지정되며 메모할 지점은 굵은 글꼴입니다.

```
Frame 1 (182 on wire, 182 captured)
```

```
Ethernet II
Destination: 00:04:4e:7a:74:00 (Cisco_7a:74:00)
Source: 00:03:fd:1c:86:84 (Cisco_1c:86:84)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0x1b8e (correct)
Source: 10.13.2.33 (10.13.2.33)
Destination: 10.13.2.34 (10.13.2.34)
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (TTL equals 0 during transit)
Checksum: 0x0c88 (correct)
Data (140 bytes)
04500 001c 9e19 0000 0111 044a 0a0d 0222E.........J..."
100a0d 0133 989d 829a 0008 cd37 0000 0000...3.......7....
200000 0000 0000 0000 0000 0000 0000 0000................
300000 0000 0000 0000 0000 0000 0000 0000................
400000 0000 0000 0000 0000 0000 0000 0000................
500000 0000 0000 0000 0000 0000 0000 0000................
600000 0000 0000 0000 0000 0000 0000 0000................
700000 0000 0000 0000 0000 0000 0000 0000................
802000 edf2 0008 0101 0002 f101...........

Frame 2 (186 on wire, 186 captured)
Ethernet II
Destination: 00:03:fd:1c:86:84 (Cisco_1c:86:84)
Source: 00:04:4e:7a:74:00 (Cisco_7a:74:00)
Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header
MPLS Label: Unknown (28)
MPLS Experimental Bits: 6
MPLS Bottom Of Label Stack: 1
MPLS TTL: 253
Internet Protocol
Version: 4
Header length: 20 bytes
Time to live: 253
Protocol: ICMP (0x01)
Header checksum: 0x1c8e (correct)
Source: 10.13.2.33 (10.13.2.33)
Destination: 10.13.2.34 (10.13.2.34)
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (TTL equals 0 during transit)
Checksum: 0x0c88 (correct)
Data (140 bytes)
04500 001c 9e19 0000 0111 044a 0a0d 0222E.........J..."
100a0d 0133 989d 829a 0008 cd37 0000 0000...3.......7....
200000 0000 0000 0000 0000 0000 0000 0000................
300000 0000 0000 0000 0000 0000 0000 0000................
400000 0000 0000 0000 0000 0000 0000 0000................
500000 0000 0000 0000 0000 0000 0000 0000................
600000 0000 0000 0000 0000 0000 0000 0000................
700000 0000 0000 0000 0000 0000 0000 0000................
802000 edf2 0008 0101 0002 f101...........
```

출력의 프레임 1에서 **R4**가 수신한 첫 번째 패킷은 R2(원래 패킷을 받은 인터페이스 10.13.2.33)에서 R1(10.13.2.34)으로 TTL 만료 ICMP 메시지입니다. ICMP 메시지의 데이터

부분(0x89 바이트, 첫 번째 니블 0x8A)에서 MPLS 레이블(20바이트)이 만료되고 해당 값은 0x02F 또는 47입니다. 이것은 TTL이 1인 패킷의 수신 레이블입니다. R2는 ICMP 오류 메시지에 이 레이블을 추가합니다.출력 **2**에서 은 MPLS 으로 표시되며 이는 MPLS 패킷임을 의미합니다.R4는 레이블 28을 프레임 1에 놓고 레이블 전환 경로를 통해 R1에 전달합니다.프레임의 MPLS 헤더는 굵게 표시됩니다.또한 패킷의 TTL 부분을 참조하는 경우 프레임 1에서는 해당 값이 254이고 프레임 2에서는 253입니다. R4는 1씩 감소했습니다.

6. R1은 ICMP 메시지를 수신하고 레이블이 47이고 TTL이 2인 다른 패킷을 R2로 보냅니다. R2는 레이블을 스왑, TTL(2에서 1로) 감소 및 R3으로 전달합니다. 2단계에서와 같이 R3은 R4로 만료된 수신 레이블과 함께 TTL 만료 ICMP 메시지를 보낸 다음 R4로 다시 전송합니다 .여기에 표시된 R4의 스니퍼 출력은 6단계를 확인합니다.

```
Frame 3 (182 on wire, 182 captured)
Ethernet II
Destination: 00:04:4e:7a:74:00 (Cisco_7a:74:00)
Source: 00:03:fd:1c:86:84 (Cisco_1c:86:84)
Type: IP (0x0800)
Internet Protocol
Version: 4
Header length: 20 bytes
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0x146f (correct)
Source: 10.13.3.134 (10.13.3.134)
Destination: 10.13.2.34 (10.13.2.34)
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (TTL equals 0 during transit)
Checksum: 0x0c88 (correct)
Data (140 bytes)
04500 001c 9e1b 0000 0211 0348 0a0d 0222E.........H..."
100a0d 0133 9292 829b 0008 d341 0000 0000...3.......A....
200000 0000 0000 0000 0000 0000 0000 0000................
300000 0000 0000 0000 0000 0000 0000 0000................
400000 0000 0000 0000 0000 0000 0000 0000................
500000 0000 0000 0000 0000 0000 0000 0000................
600000 0000 0000 0000 0000 0000 0000 0000................
700000 0000 0000 0000 0000 0000 0000 0000................
802000 0df3 0008 0101 0002 d101..........

Frame 4 (186 on wire, 186 captured)
Ethernet II
Destination: 00:03:fd:1c:86:84 (Cisco_1c:86:84)
Source: 00:04:4e:7a:74:00 (Cisco_7a:74:00)
Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header
MPLS Label: Unknown (28)
MPLS Experimental Bits: 6
MPLS Bottom Of Label Stack: 1
MPLS TTL: 254
Internet Protocol
Version: 4
Header length: 20 bytes
Time to live: 254
Protocol: ICMP (0x01)
Header checksum: 0x156f (correct)
Source: 10.13.3.134 (10.13.3.134)
Destination: 10.13.2.34 (10.13.2.34)
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (TTL equals 0 during transit)
```

```
Checksum: 0x0c88 (correct)
Data (140 bytes)
04500 001c 9e1b 0000 0211 0348 0a0d 0222E.........H..."
100a0d 0133 9292 829b 0008 d341 0000 0000...3.......A....
200000 0000 0000 0000 0000 0000 0000 0000................
300000 0000 0000 0000 0000 0000 0000 0000................
400000 0000 0000 0000 0000 0000 0000 0000................
500000 0000 0000 0000 0000 0000 0000 0000................
600000 0000 0000 0000 0000 0000 0000 0000................
700000 0000 0000 0000 0000 0000 0000 0000................
802000 0df3 0008 0101 0002 d101..........
```

프레임 **3 출력**에서 프레임 3이 R3에서 R1까지의 ICMP 패킷인지 확인할 수 있습니다. 소스 주소(10.13.3.134)은 원래 패킷이 수신되는 주소입니다.ICMP 오류 메시지에는 데이터 부분의 끝에 만료된 레이블 정보가 포함됩니다.이 값의 값은 0x02d(45)입니다. **4는** R4에서 R1로 전송되는 MPLS 패킷입니다.

7. ICMP 메시지를 수신하면 R1은 레이블이 47이고 TTL이 3인 다른 패킷을 보냅니다. 이 과정에서 R2와 R3는 TTL을 줄이고 패킷을 R4로 전달합니다. R4는 의도한 수신자임을 알리고 UDP 데이터그램 포트에 연결할 수 없는 것을 찾습니다.ICMP 메시지를 R1에서 R3 및 R2로 전송합니다.이 스니퍼 출력에서 주목해야 할 중요한 사항은 굵은 글꼴로 표시됩니다.

```
Frame 5 (60 on wire, 60 captured)
Ethernet II
Destination: 00:04:4e:7a:74:00 (Cisco_7a:74:00)
Source: 00:03:fd:1c:86:84 (Cisco_1c:86:84)
Type: IP (0x0800)
Trailer: 000000000000000000000000000000000...
Internet Protocol
Version: 4
Header length: 20 bytes
Time to live: 1
Protocol: UDP (0x11)
Header checksum: 0x0446 (correct)
Source: 10.13.2.34 (10.13.2.34)
Destination: 10.13.1.51 (10.13.1.51)
User Datagram Protocol
Source port: 37647 (37647)
Destination port: 33436 (33436)
Length: 8
Checksum: 0xd2c3 (correct)

Frame 6 (74 on wire, 74 captured)
Ethernet II
Destination: 00:03:fd:1c:86:84 (Cisco_1c:86:84)
Source: 00:04:4e:7a:74:00 (Cisco_7a:74:00)
Type: MPLS label switched packet (0x8847)
MultiProtocol Label Switching Header
MPLS Label: Unknown (28)
MPLS Experimental Bits: 6
MPLS Bottom Of Label Stack: 1
MPLS TTL: 255
Internet Protocol
Version: 4
Header length: 20 bytes
Time to live: 255
Protocol: ICMP (0x01)
Header checksum: 0x5694 (correct)
Source: 10.13.5.10 (10.13.5.10)
Destination: 10.13.2.34 (10.13.2.34)
Internet Control Message Protocol
Type: 3 (Destination unreachable)
```

```
Code: 3 (Port unreachable)
Checksum: 0x1485 (correct)
Data (28 bytes)
04500 001c 9e1d 0000 0111 0446 0a0d 0222E.........F..."
100a0d 0133 930f 829c 0008 d2c3...3........
```

5는 UDP 데이터그램이 R1에서 R4로 전송되었음을 보여줍니다. UDP 데이터그램의 대상 포트 값은 Normal traceroute 명령 섹션에서 설명한 대로 33436(32000보다 큼)입니다.프레임 6에서 R4는 ICMP 유형 및 코드를 R1에 전송합니다. R2 및 R3의 모든 이전 ICMP 메시지의 유형 필드가 time-to-live exceeded로 .확장 traceroute 명령의 출력은 다음과 같습니다.

```
R1#traceroute
Protocol [ip]:
Target IP address: 10.13.1.51
Source address: 10.13.2.34
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]: 1
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 10.13.1.51
1 10.13.2.33 [MPLS: Label 47 Exp 0] 0 msec
2 10.13.3.134 [MPLS: Label 45 Exp 0] 0 msec
3 10.13.5.10 4 msec
R1#
```

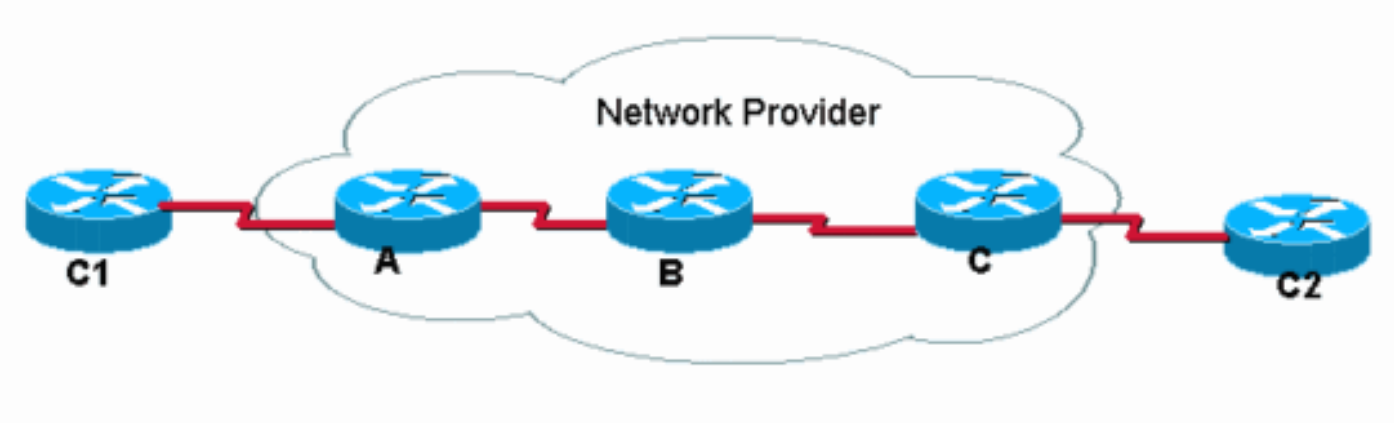
기본적으로 traceroute 명령은 각 TTL 값에 대해 3개의 프로브를 사용합니다.TTL이 1인 3개의 패킷, TTL이 2인 3개의 패킷 등을 전송합니다.이 **traceroute** 명령은 단일 프로브로 실행되므로 추적 및 디버깅이 쉽습니다.출력에 표시된 대로 traceroute 명령에는 만료된 레이블 값도 표시됩니다.

no mpls ip propagate-ttl 명령

MPLS를 구성할 때 IP 패킷이 MPLS 도메인으로 전달될 때 LSR(Label Switch Router)에 의해 레이블이 지정됩니다.이 레이블에는 TTL 필드에 값이 있어야 합니다.기본적으로 LSR은 수신 패킷의 IP 헤더에 있는 TTL 필드를 읽고, 1 만큼 줄이며, 남아 있는 것을 MPLS 헤더의 TTL 필드에 복사합니다.코어 LSR은 맨 위 레이블만 살펴봅니다.TTL 값이 0에 도달하지 않으면 패킷이 전달됩니다.레이블을 표시하는 이그레스 에지 LSR은 레이블 TTL 필드에 남아 있는 항목을 IP 헤더의 TTL 필드로 복사한 다음 MPLS 도메인 외부로 IP 패킷을 전달합니다.

이 동작은 no mpls ip propagate-ttl configuration 명령을 사용하여 변경할 수 있습니다.인그레스 에지 LSR은 255 값을 적용할 때 레이블의 TTL 값으로 사용합니다.이그레스 에지 LSR은 레이블을 팝업할 때 레이블 TTL 값을 IP 헤더에 복사하지 않습니다.결과적으로 IP 헤더 TTL은 MPLS 코어에서 가져온 홉을 반영하지 않습니다.따라서 고객이 네트워크의 한 쪽에서 다른 쪽으로 **traceroute**를 수행할 때 MPLS 코어 네트워크의 라우터는 traceroute 정보에 나타나지 않습니다.인그레스 및 이그레스 에지 LSR에서 TTL 전파를 비활성화하는 것이 중요합니다.그렇지 않으면 MPLS 도메인을 떠날 때 IP 헤더의 값이 IP 헤더를 입력한 때보다 더 높을 수 있습니다.

예를 들면 다음과 같습니다.



C1은 **traceroute**를 C2로 수행합니다. 기본 IP TTL 전파 작업을 통해 **C**1의 traceroute는 다음과 같습니다.

```
C1#traceroute C2.cust.com

Tracing the route to C2.cust.com
  1 A.provider.net       44 msec  36 msec  32 msec
  2 B provider.net      164 msec  132 msec  128 msec
  3 C.provider.net148 msec  156 msec  152 msec
  4 C2.cust.com         180 msec  *  181 msec
```

이 출력은 MPLS 네트워크에서 일반적인 traceroute 동작을 보여줍니다.레이블이 지정된 패킷의 레이블 헤더는 원래 IP 패킷의 TTL 값을 전달하므로 경로의 경로는 TTL을 초과하는 패킷을 삭제합니다.따라서 traceroute**는** 경로의 모든 라우터를 표시합니다.동작은 다음과 같습니다.

1. 첫 번째 패킷은 TTL이 1인 IP 패킷입니다. 라우터 A는 TTL을 줄이고 패킷이 0에 도달하기 때문에 패킷을 삭제합니다. ICMP TTL 초과 메시지가 소스로 전송됩니다.
2. 전송된 두 번째 패킷은 TTL이 2인 IP 패킷입니다. 라우터 A는 TTL을 줄이고, 패킷에 레이블을 지정하며, 패킷을 라우터 B에 전달합니다.
3. 라우터 B는 MPLS 헤더의 TTL 값을 줄이고, 패킷을 삭제하고, ICMP TTL 초과 메시지를 소스로 전송합니다.삭제된 MPLS 패킷이므로 ICMP 메시지의 반환 주소는 MPLS 패킷 내부의 IP 헤더의 소스 주소에서 파생되어야 합니다.그러나 이 IP 주소는 실제로 라우터 B에 알려지지 않을 수 있으므로 라우터 B는 삭제된 패킷이 이동하던 LSP(Label Switched Path)를 따라 ICMP 메시지를 전달합니다(라우터 C 방향으로). LSP의 끝에서 레이블이 제거되고 ICMP 메시지는 IP 헤더의 목적지 주소(라우터 C1 방향)에 따라 전달됩니다.
4. 세 번째 패킷(TTL은 3)은 IP 헤더의 TTL을 기반으로 현재 라우터 C가 패킷을 삭제하는 패킷이라는 점을 제외하고 이전 패킷과 유사한 처리를 경험합니다.Router B - penultimate hop이 팝업되어 이전에 레이블을 제거했으며 TTL이 IP 헤더에 복사되었습니다.
5. 네 번째 패킷(TTL은 4)은 IP 헤더의 TTL을 검사하는 최종 대상에 도달합니다.

글로벌 컨피그레이션 모드에서 no mpls ip propagate-ttl 명령을 사용하여 IP TTL 전파를 비활성화하면 TTL 값이 IP 헤더에 복사되지 않고 C1에서 C2로의 **traceroute는** 다음과 같습니다.

```
C1#traceroute C2.cust.com

Tracing the route to C2.cust.com
  1 A.provider.net    44 msec  36 msec  32 msec
  2 C2.cust.com      180 msec  *  181 msec
```

traceroute 명령**이** 이 상황에서 사용되는 경우 ICMP 응답은 IP 헤더에 저장된 실제 TTL을 확인하는 라우터에서만 수신됩니다.이 경우 라우터 C1은 **traceroute** 명령(표시된 대로)을 실행하지만 코어 라우터는 레이블과 TTL을 복사하지 않습니다.이 동작은 다음과 같습니다.

1. 첫 번째 패킷은 TTL이 1인 IP 패킷입니다. 라우터 A는 TTL을 줄이고 패킷을 삭제하고 ICMP TTL 초과 메시지를 소스로 전송합니다.
2. 두 번째 패킷은 TTL이 2인 IP 패킷입니다. 라우터 A는 TTL을 줄이고, 패킷에 레이블을 지정하며, MPLS 헤더의 TTL을 255로 설정합니다.
3. 라우터 B는 MPLS 헤더의 TTL을 254로 줄이고, MPLS 레이블을 제거하고, MPLS 헤더의 TTL 값을 IP 헤더의 TTL 필드에 복사합니다.
4. 라우터 C는 IP TTL을 줄이고 패킷을 다음 홉의 라우터 C2로 전송합니다. 패킷이 최종 대상에 도달했습니다.

관련 정보

- Ping 및 Traceroute 명령 이해
- mpls ip propagate-ttl 명령
- MPLS 기술 지원 페이지
- Technical Support - Cisco Systems