El comando traceroute en MPLS

Contenido

Introducción

Este documento explica cómo funciona el comando traceroute en un entorno MPLS (Multiprotocol Label Switching).

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico del MPLS

Refiera a MPLS FAQ para los principiantes para más información.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

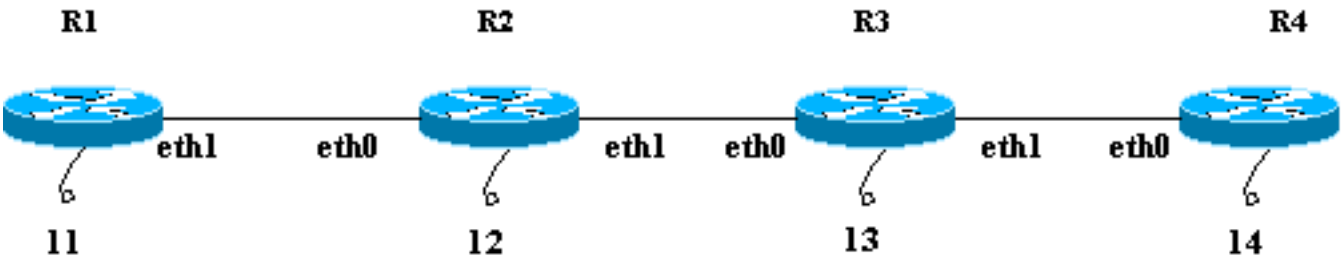
Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Comando traceroute normal

Esta sección describe cómo funciona un comando traceroute tradicional. Este diagrama muestra un proveedor de servicio puesto donde router1 (r1) y el Router4 (R4) es Routers del borde del

proveedor (PE) y router2 (r2) y el router3 (R3) es el Routers del proveedor (p).



Este ejemplo dirige un comando traceroute al loopback 14 del R4 desde el R1. El r1 utiliza un datagrama del User Datagram Protocol (UDP) con un valor de puerto destino arbitrario mayor de 32000. Si usted selecciona tal valor alto para el número del puerto, se asegura de que tal puerto no exista en el receptor deseado. Pone este datagrama en un paquete del IP.

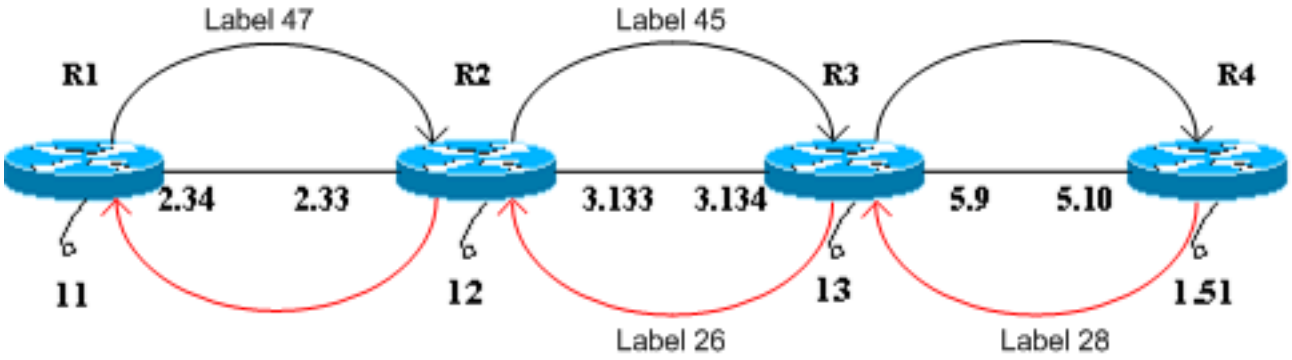
Nota: A lo largo de este documento, siempre que se menciona un paquete IP, se hace referencia a un paquete IP que contiene el datagrama UDP.

Esto es una Secuencia de eventos para un **comando traceroute** normal:

1. El r1 envía el paquete del IP con una dirección destino de 14 y un Time to Live (TTL) de 1 a través de su interfaz del eth1.
2. El r2 recibe el paquete y observa que no es el receptor deseado y TTL del paquete es 1. Cae el paquete y envía un mensaje del Internet Control Message Protocol (ICMP) del expirado TTL al r1. La dirección de origen de este mensaje ICMP es la dirección IP del R2 eth0 (la dirección de la interfaz que recibió el paquete original).
3. En el recibo del mensaje ICMP, el r1 envía otro paquete del IP destinado para 14 con TTL de 2 a través de su interfaz del eth1.
4. El r2 recibe el paquete y observa que no es el receptor deseado y el receptor deseado puede ser alcanzado con el R3. Decrements TTL (a partir el 2 a 1) y adelante el paquete al R3. El R3 recibe el paquete y ve que no es el receptor deseado. TTL es 1. Cae el paquete y envía un mensaje ICMP del expirado TTL al r1 con su direccionamiento del eth0 como la dirección de origen.
5. El r1 recibe el mensaje ICMP y envía otro paquete del IP a 14 a través de su interfaz del eth1 con un valor de TTL de 3. En la manera, el r2 y el R3 decrement TTL y lo pasan encendido al R4. R4 recibe el paquete, constata que es el destinatario previsto e intenta conectarse con el valor de puerto en el datagrama UDP. El R4 encuentra que este puerto no existe y que envía un `puerto` ICMP el mensaje de error `inalcanzable al` r1.Como antes, la dirección de origen de este mensaje ICMP es eth0 del R4. **El programa Traceoute** ahora tiene todos los mensajes de error ICMP con las direcciones de origen correspondientes y tiene la ruta completa al destino.

Comando traceroute MPLS

Considere esto el mismo escenario detallada en la sección de comando traceroute normal, a menos que todo el Routers, r1 con el R4, ahora haga el switching por etiquetas en vez de reenvío de IP. Se muestra la configuración de la plataforma de ensayo es este diagrama. Todas las interfaces mostradas en la plataforma de ensayo están en la red de 10.13.0.0.

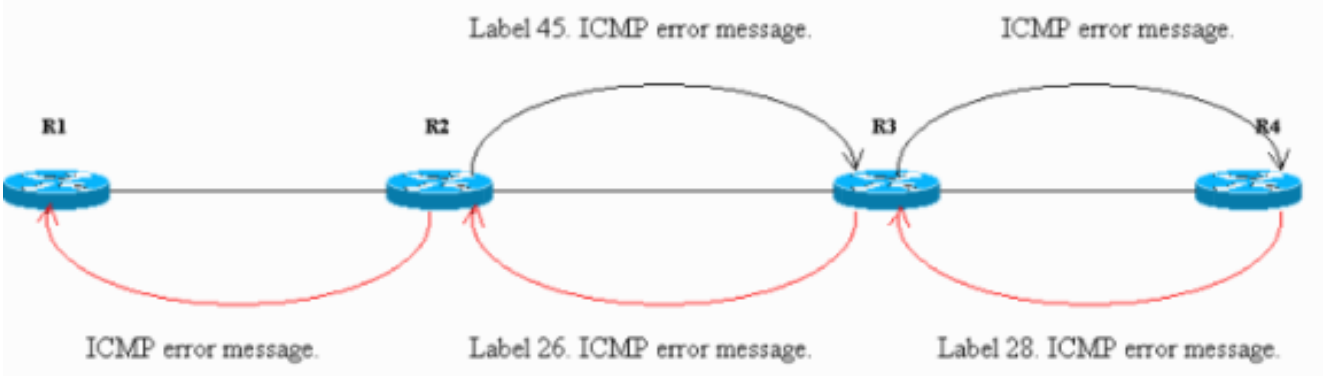


Con el fin de este documento, asuma eso:

- El r1 utiliza una escritura de la etiqueta de 47 para alcanzar el R4 y adelante los paquetes al r2.
- El r2 utiliza una escritura de la etiqueta de 45 para alcanzar el R4 y adelante los paquetes al R3.
- R3 salta la etiqueta y reenvía el paquete a R4.
- R4 utiliza una etiqueta de 28 para alcanzar R1 y reenvía paquetes a R3.
- El R3 utiliza una escritura de la etiqueta de 26 para alcanzar el r1 y adelante los paquetes al r2.
- El r2 hace estallar la escritura de la etiqueta y adelante el paquete al r1.

Estos pasos muestran la Secuencia de eventos para conducir un **traceroute del** r1 R4 al loopback 10.13.1.51.

1. R1 envía un paquete conmutado etiqueta con una etiqueta de 47 y un TTL de 1 al R2. El campo TTL del paquete IP se copia en el campo TTL del encabezado de etiqueta.
2. El r2 ve que no es el receptor deseado y TTL es 1. Cae el paquete y crea un mensaje ICMP del expirado TTL, como para un paquete del IP regular. En este caso, el paquete de mensaje ICMP se genera por las extensiones ICMP para el MPLS.
3. El r2 añade la escritura de la etiqueta al final del fichero 47 (la etiqueta entrante que expiró) al mensaje ICMP. No envía el paquete al r1 directamente. En lugar, consulta su Base de información de reenvío de etiquetas (LFIB) y encuentra que debe utilizar una escritura de la etiqueta de 45 para los paquetes recibidos con una escritura de la etiqueta de 47. Pone una escritura de la etiqueta de 45 en el paquete y envía el mensaje ICMP del expirado TTL al R3.
4. R3 salta la etiqueta y la envía a R4. R4 ve que el destino es R1, le da una etiqueta de 28 al mensaje y lo envía a través de R3 y R2 hacia R1.
5. El mensaje de error de ICMP viaja hasta el otro extremo antes de ser enviado de regreso a R1. Este ejemplo proporciona una ilustración:



Los paquetes olidos en la interfaz de Ethernet en el R4 confirman los pasos 1 – 5. En la salida del sniffer, el **capítulo 1** es el paquete de entrada y el **capítulo 2** es el paquete saliente del R4. La salida está formateada para reflejar esta discusión y los puntos destacados se encuentran en negrita.

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 00**02 f**101..... **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.....

En el **capítulo 1 de la** salida, el primer paquete recibido por el R4 es el mensaje ICMP del expirado TTL del r2 (10.13.2.33, la interfaz en la cual el paquete original fue recibido) al r1 (10.13.2.34). En la porción de datos del mensaje ICMP, en los bytes 0x89 y el primer nibble de 0x8A, se expira la escritura de la etiqueta MPLS (20 bytes) y su valor es 0x02F, o 47. Ésta es la etiqueta entrante del paquete con TTL de 1. r2 añade esta escritura de la etiqueta al final del fichero en el mensaje de error ICMP.En el **capítulo 2 de la** salida, muestran el `tipo` como `Switched Packet de la escritura de la etiqueta MPLS`, así que significa que es un paquete MPLS. El R4 pone una escritura de la etiqueta de 28 para capítulo 1 y adelante lo al r1 a través de la trayectoria del Label-Switching. El encabezado MPLS en la trama está en intrépido. También, si usted refiere a la porción de TTL del paquete, en el capítulo 1 su valor es 254, y en el capítulo 2 es 253. El R4 decremented lo por 1.

6. El r1 recibe el mensaje ICMP y envía otro paquete con una escritura de la etiqueta de 47 y TTL de 2 al r2. R2 cambia etiquetas, disminuye TTL (de 2 a 1) y reenvía a R3. Como en el paso 2, el R3 envía un mensaje ICMP del expirado TTL añadido al final del fichero con la etiqueta entrante que expiró al R4, y el R4 después lo envía de nuevo al r1.El sniffer hecho salir en el R4, mostrado aquí, confirma el paso 6:

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.....

Del capítulo 3 hecho salir, usted puede determinar ese capítulo 3 es los paquetes icmp del R3 al r1. La dirección de origen (10.13.3.134) es el direccionamiento en el cual se recibe el paquete original. El mensaje de error ICMP contiene la información de etiqueta vencida al final de la porción de datos. Su valor es 0x02d, que es 45. **El capítulo 4** es el paquete MPLS que se envía del R4 al r1.

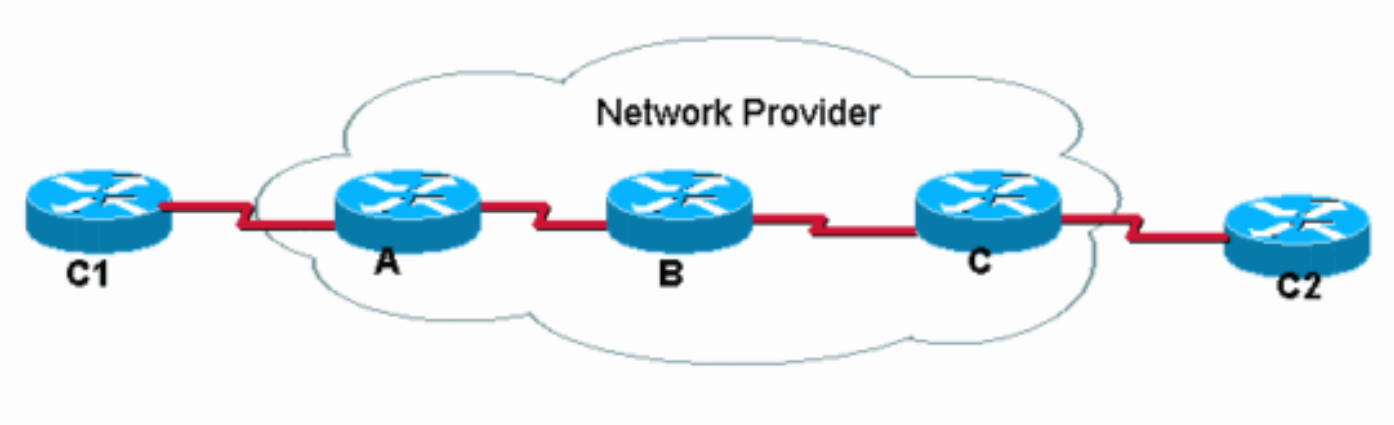
7. Tras el recibo del mensaje ICMP, el r1 envía otro paquete con una escritura de la etiqueta de 47 y TTL de 3. En su manera, el r2 y el R3 decrement TTL y remiten el paquete al R4. El R4 observa que es el receptor deseado y encuentra al puerto de datagrama UDP inalcanzable. Envía un mensaje inalcanzable del puerto ICMP al r1 con el R3 y el r2.En esta salida del sniffer, los puntos importantes que se observarán están en la negrilla:
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: 0000000000000000000000000000000000... 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..... **El capítulo 5** muestra que el datagrama de UDP es enviado por el r1 al R4. El valor de puerto destino en el datagrama de UDP es 33436 (mayor de 32000), como se debate en la sección de comando traceroute normal.En el **capítulo 6**, el R4 envía un destino el tipo inalcanzable ICMP y un puerto código inalcanzable al r1. Todo los mensajes ICMP anteriores del r2 y del R3 tenían el campo definido del tipo mientras que el Tiempo para vivir se excedió. A continuación, se muestra el resultado del comando extended traceroute: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# Por abandono, el **comando traceroute** utiliza tres sondas para cada valor de TTL. Envía tres paquetes con TTL de 1, tres paquetes con TTL de 2, y así sucesivamente. Publican este **comando traceroute** con una sola sonda, así que es fácil localizar y hacer el debug de. Como se ve en la salida, el **comando traceroute** muestra el valor de etiqueta expirado, también.

Comando no mpls ip propagate-ttl

Cuando usted configura el MPLS, una escritura de la etiqueta es impuesta por el Label Switch Router (LSR) cuando un paquete del IP se remite en el dominio MPLS. Esta etiqueta debe tener un valor en el campo TTL. Por abandono, el LSR lee el campo de TTL en el encabezado IP del paquete entrante, decrements lo por 1, y copia qué se deja en el campo de TTL del encabezado MPLS. La base LSR mira solamente la escritura de la etiqueta más suprema. Si el valor de TTL no alcanza 0, se remite el paquete. El LSR de borde de egreso que elimina las etiquetas copia lo que quedó en el campo TTL de etiquetas en el campo TTL del encabezado IP y luego, reenvía el paquete IP fuera del dominio MPLS.

Este comportamiento se puede cambiar con el ningún comando configuration de propagación-TTL del IP de los mpls. El borde de ingreso LSR usa el valor 255 como el valor TTL en la etiqueta al imponerlo. El LSR de borde de egreso no copia el valor TTL de la etiqueta en un encabezado IP cuando dispara la etiqueta.B El resultado neto es que el encabezado IP TTL no refleja los saltos tomados a través de la base MPLS; tan cuando los clientes realizan un **traceroute** a partir de un lado de su red a otro lado, el Routers en la red del núcleo MPLS no aparece en la **información del Traceroute**. Es importante inhabilitar la propagación de TTL en el ingreso y el borde LSR de la salida. Si no, el encabezado IP puede tener un valor más alto cuando sale del dominio MPLS que tenía cuando lo ingresó.

Aquí tiene un ejemplo:



El c1 realiza un **traceroute al** C2. Con la operación de la propagación de TTL del IP predeterminado, el **traceroute** en el c1 parece esto:

```
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.net 148 msec 156 msec 152 msec 4
C2.cust.com 180 msec * 181 msec
```

Este resultado ilustra el comportamiento típico de la ruta de rastreo en una red MPLS. Como la encabezado de la escritura de la etiqueta de un paquete etiquetado lleva el valor de TTL del paquete del IP original, las rutas en los trayectos descarta paquetes para los cuales se excede TTL. En consecuencia, la ruta de seguimiento muestra todos los routers en el trayecto. El comportamiento es éste:

1. El primer paquete es un paquete del IP con TTL igual a 1. routers que A decrements TTL y que cae el paquete porque alcanza 0. Un mensaje TTL-excedido ICMP se envía a la fuente.
2. El segundo paquete enviado es un paquete IP con un TTL igual a 2. El Router A disminuye el TTL, etiqueta el paquete y lo reenvía al Router B.
3. El router B disminuye el valor de TTL en el encabezado de MPLS, abandona el paquete y envía un mensaje ICMP TTL-exceeded a la fuente. Ya que lo que se eliminó era un paquete MPLS, la dirección de retorno para el mensaje ICMP debe obtenerse desde la dirección de origen en el encabezado IP dentro del paquete MPLS. Pero esa dirección IP no se puede

saber realmente al router B, tan el router B adelante los mensajes ICMP a lo largo de la misma trayectoria conmutada de etiquetas (LSP) que viajaba el paquete perdidos (en la dirección hacia el router C). En el final del LSP, se quita la escritura de la etiqueta y los mensajes ICMP se remiten según la dirección destino en el encabezado IP (hacia el c1 del router).

4. El tercer paquete (TTL es 3) experimenta un procesamiento similar al de los paquetes anteriores, excepto que el router C ahora es el que coloca el paquete, basado en el TTL del encabezado IP. El Router B, debido a la explosión del penúltimo salto, ha eliminado previamente la etiqueta y el TTL se copió en el encabezado IP.
5. El cuarto paquete (TTL es 4) alcanza el destino final donde se evalúa el TTL del encabezado de IP.

Si la propagación de TTL IP se inhabilita con el comando no mpls ip propagate-ttl en el modo de configuración global, el valor de TTL no se copia en el encabezado IP y el **traceroute** en el c1 al C2 parece esto:

```
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
```

Cuando utilizan al **comando traceroute** en esta situación, las respuestas de ICMP se reciben solamente de eso Routers que vea TTL real salvado en el encabezado IP. En esta situación, el c1 del router está ejecutando un **comando traceroute** (como se muestra), pero los routeres del núcleo no copian TTL a y desde la escritura de la etiqueta. Da lugar a este comportamiento:

1. El primer paquete es un paquete del IP con TTL igual a 1. routers que A decrements TTL, cae el paquete, y envía un mensaje TTL-excedido ICMP a la fuente.
2. El segundo paquete es un paquete del IP con TTL igual al router 2. que A decrements TTL, etiqueta el paquete, y fija TTL en el encabezado MPLS a 255.
3. El theTTL de los decremetns del router B en el encabezado MPLS a 254, quita la escritura de la etiqueta MPLS, y copia el valor de TTL en el encabezado MPLS en el campo de TTL del encabezado IP.
4. El C del router decrements el IP TTL y envía el paquete al Next Hop Router C2. El paquete ha llegado al destino final.

Información Relacionada

- Comprensión de los comandos ping y traceroute
- Comando mpls ip propagate-ttl
- Página de soporte de la tecnología MPLS
- Soporte Técnico - Cisco Systems