

# MPLS中的Traceroute命令

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[正常traceroute命令](#)

[MPLS traceroute指令](#)

[no mpls ip propagate-ttl命令](#)

[相關資訊](#)

## 簡介

本檔案將說明traceroute指令在多重通訊協定標籤交換(MPLS)環境中運作的方式。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 基本MPLS知識

有關詳細資訊，請參閱[初學者的MPLS常見問題](#)。

### 採用元件

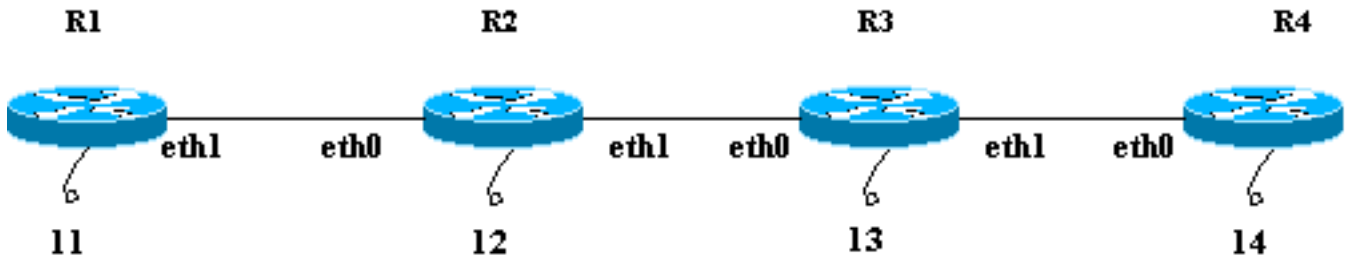
本文件所述內容不限於特定軟體和硬體版本。

### 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## 正常traceroute命令

本節介紹傳統traceroute命令的運作方式。此圖顯示了一個服務提供商設定，其中路由器1(R1)和路由器4(R4)是提供商邊緣(PE)路由器，路由器2(R2)和路由器3(R3)是提供商(P)路由器。



此示例從R1對R4環回14執行tracert。R1使用任意目標埠值大於32000的使用者資料包協定(UDP)資料包。如果為埠號選擇如此高的值，它將確保目標收件人上不存在這樣的埠。將此資料包放入IP封包中。

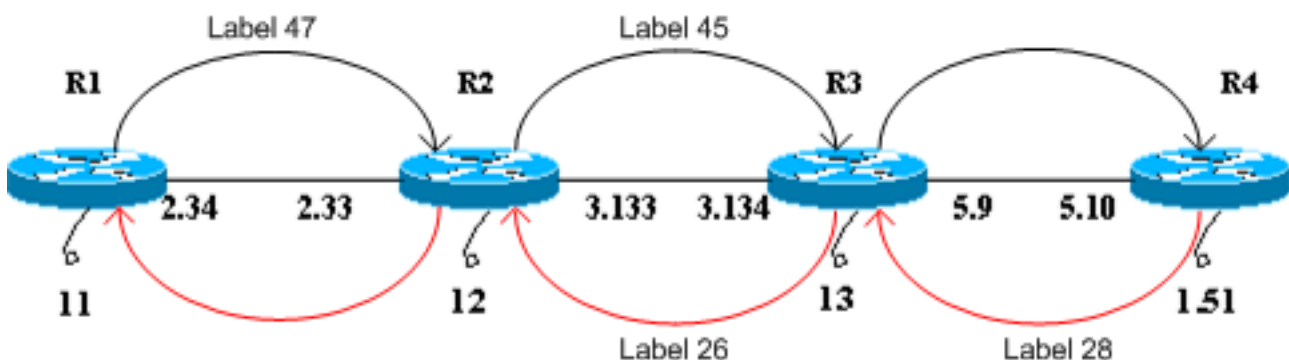
**注意：**在本文檔中，無論何時提到IP資料包，它都是包含UDP資料包的IP資料包。

以下是一般tracert指令的事件序列：

1. R1通過其eth1介面傳送目的地為14、生存時間(TTL)為1的IP資料包。
2. R2收到該資料包，並注意到該資料包不是預期的接收方，並且資料包的TTL為1。它丟棄該資料包並將一條TTL到期的網際網路控制消息協定(ICMP)消息傳送到R1。此ICMP消息的源地址是R2 eth0的IP地址（接收原始資料包的介面的地址）。
3. 在收到ICMP消息後，R1通過其eth1介面傳送另一個目的地為14、TTL為2的IP資料包。
4. R2收到該資料包，並註明該資料包不是預定接收方，而且該預定接收方可以通過R3到達。它遞減TTL（從2到1）並將該資料包轉發到R3。R3收到該資料包，並發現它不是預定接收方。TTL為1。它會捨棄該封包，並向R1傳送一則TTL過期的ICMP訊息，並將其eth0位址作為來源位址。
5. R1收到ICMP訊息，並透過其eth1介面將另一個IP封包傳送到14，其TTL值為3。在此過程中，R2和R3遞減TTL並將其傳遞到R4。R4會取得封包，判斷其為預期接收者，並嘗試連線到UDP資料包中的連線埠值。R4發現此埠不存在，並向R1傳送ICMP `port unreachable`錯誤消息。與以前一樣，此ICMP消息的源地址是R4的eth0。**tracert**程式現在包含所有具有相應源地址的ICMP錯誤消息，並具有到達目標的完整路由。

## MPLS tracert指令

請考慮在[Normal tracert命令](#)部分詳述的相同場景，但所有路由器（R1至R4）現在都執行標籤交換而不是IP轉發。測試台設定如圖所示。測試台中顯示的所有介面都位於10.13.0.0網路中。



就本檔案而言，假設：

- R1使用標籤47到達R4並將資料包轉發到R2。
- R2使用標籤45到達R4並將資料包轉發到R3。

- R3彈出標籤並將資料包轉發到R4。
- R4使用標籤28到達R1並將資料包轉發到R3。
- R3使用標籤26到達R1並將資料包轉發到R2。
- R2彈出標籤並將資料包轉發到R1。

這些步驟顯示事件序列，以執行tracert ( 從R1到R4環回10.13.1.51 )。

1. R1將標籤為47且TTL為1的標籤交換資料包傳送到R2。IP資料包的TTL欄位將複製到標籤報頭的TTL欄位。
2. R2發現它不是預期接收方，TTL為1。它會丟棄資料包並建立TTL過期ICMP消息，就像常規IP資料包一樣。在這種情況下，每個MPLS的ICMP擴展生成ICMP消息資料包。
3. R2將標籤47 ( 過期的傳入標籤 ) 附加到ICMP消息。它不會將資料包直接傳送到R1。相反，它會查詢其標籤轉發資訊庫(LFIB)，發現它應該對收到的標籤為47的資料包使用標籤45。它在資料包上放置標籤45，並向R3傳送TTL過期ICMP消息。
4. R3彈出標籤並將其傳送到R4。R4看到目的地是R1，為消息提供標籤28，然後通過R3和R2將其傳送到R1。
5. ICMP錯誤消息在發回R1之前會一直傳輸到另一端。以下示例提供圖示：



R4的乙太網路介面上的已監聽封包會確認步驟1-5。在監聽器輸出中，Frame 1是傳入封包，Frame 2是來自R4的傳出封包。輸出經過格式化，以反映此討論，且需注意的點以黑體顯示。

```

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.....
```

在輸出的<sub>1</sub>中，R4收到的第一個資料包是從R2（接收原始資料包的介面10.13.2.33）到R1(10.13.2.34)的TTL過期ICMP消息。在ICMP消息的資料部分（位元組0x89和第一個半位元組0x8A）中，MPLS標籤（20位元組）已過期，其值為0x02F或47。這是資料包的傳入標籤，TTL為1。R2在ICMP錯誤消息中附加此標籤。在輸出的<sub>2</sub>中，type顯示為MPLS，這意味著它是MPLS資料包。R4將標籤28放入幀1，並通過標籤交換路徑將其轉發到R1。幀中的MPLS報頭以粗體顯示。此外，如果參考資料包的TTL部分，則第1幀中的值是254，第2幀中的值是253。R4將其遞減1。

6. R1收到ICMP消息，並將另一個標籤為47、TTL為2的資料包傳送到R2。R2交換標籤，減少TTL（從2到1）並轉發到R3。如步驟2所示，R3傳送附加有傳入TTL過期的ICMP消息，該消息將傳回R4。此處顯示的R4上的監聽器輸出確認步驟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.....

```

從**Frame 3**輸出中，您可以確定第3幀是從R3到R1的ICMP資料包。源地址(10.13.3.134)是接收原始資料包的地址。ICMP錯誤消息在資料部分末尾包含過期的標籤資訊。其值為0x02d，即45。**Frame 4**是從R4傳送到R1的MPLS資料包。

- 收到ICMP訊息後，R1會傳送另一個封包，其標籤為47,TTL為3。在傳送過程中，R2和R3會遞減TTL並將封包轉送到R4。R4表示它是預期接收者，但發現UDP資料包連線埠無法連線。它通過R3和R2向R1傳送ICMP `port unreachable`消息。在此監聽器輸出中，需注意的重要事項以粗體顯示：

```

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: 00000000000000000000000000000000...
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.....

```

5顯示UDP資料包由R1傳送到R4。UDP資料包中的目標埠值為33436(大於32000)，如[Normal traceroute Command一節中所述](#)。在6中，R4向R1傳送ICMP型別和代碼。來自R2和R3的所有較早的ICMP訊息都將type欄位設定為time-to-live。延伸型traceroute指令的輸出如下：

```

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#

```

預設情況下，**traceroute**命令對每個TTL值使用三個探測。它會傳送三個封包 ( TTL為1 )、三個封包 ( TTL為2 )，以此類推。此**traceroute**指令以單一探針發出，因此很容易追蹤和偵錯。如輸出所示，**traceroute**指令也會顯示到期的標籤值。

## no mpls ip propagate-ttl命令

配置MPLS時，將IP資料包轉發到MPLS域時，標籤交換路由器(LSR)會實施標籤。此標籤必須在TTL欄位中有值。預設情況下，LSR讀取傳入資料包的IP報頭中的TTL欄位，將其遞減1，並將剩餘內容複製到MPLS報頭的TTL欄位。核心LSR只檢視最上面的標籤。如果TTL值未達到0，則轉發資料包。彈出標籤的出口邊緣LSR將標籤TTL欄位中的剩餘內容複製到IP報頭的TTL欄位，然後將IP資料包轉發到MPLS域之外。

可以使用**no mpls ip propagate-ttl** 配置命令更改此行為。施加入口邊緣LSR時，會使用值255作為標籤中的TTL值。彈出標籤時，出口邊緣LSR不會將標籤TTL值複製到IP標頭中。最終結果是IP報頭TTL並不反映跨MPLS核心的跳數；因此，當客戶從其網路的一端到另一端執行**traceroute**時，MPLS核心網路中的路由器不會顯示在**traceroute**資訊中。在輸入和輸出邊緣LSR中停用TTL傳播非常重要。否則，在離開MPLS域時，IP報頭可能具有比其輸入時更高的值。

以下提供範例：



C1執行到C2的**traceroute**。使用預設IP TTL傳播操作時，C1中的**traceroute**如下所示：

```
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
```

此輸出說明了MPLS網路中的典型**traceroute**行為。由於已標籤封包的標籤標頭會攜帶來自原始IP封包的TTL值，因此路徑中的路由會捨棄超過TTL的封包。因此，**traceroute**會顯示路徑中的所有路由器。行為如下：

1. 第一個封包是TTL等於1的IP封包。路由器A會遞減TTL並捨棄該封包，因為它達到0。系統會向來源傳送ICMP TTL超出訊息。
2. 第二個傳送的資料包是TTL等於2的IP資料包。路由器A遞減TTL，標籤資料包，然後將資料包轉發到路由器B。
3. 路由器B會遞減MPLS標頭中的TTL值，捨棄封包，並向來源傳送ICMP TTL超出訊息。由於是

MPLS資料包被丟棄，因此ICMP消息的返回地址必須從MPLS資料包內IP報頭中的源地址派生。但路由器B實際上可能不知道該IP地址，因此路由器B沿丟棄的資料包所行經的同一標籤交換路徑(LSP) ( 朝向路由器C ) 轉發ICMP消息。在LSP的末尾，標籤會刪除，並根據IP報頭中的目的地址 ( 向路由器C1 ) 轉發ICMP消息。

4. 第三個資料包 ( TTL是3 ) 的處理方法與之前的資料包類似，不同之處在於，根據IP報頭中的TTL，路由器C現在丟棄了資料包。路由器B由於倒數第二跳跳彈出，之前已移除標籤，且TTL已複製到IP報頭中。
5. 第四個封包 ( TTL為4 ) 到達檢查IP報頭的TTL的最終目的地。

如果在全域性配置模式下使用[no mpls ip propagate-ttl](#) 命令禁用IP TTL傳播，則不會在IP報頭中複製TTL值，並且C1到C2中的[traceroute](#)如下所示：

```
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
```

在此情況下使用[traceroute](#)指令時，只會從看到IP報頭中儲存的實際TTL的路由器收到ICMP應答。在這種情況下，路由器C1正在執行[traceroute](#)命令 ( 如圖所示 )，但核心路由器不會將TTL複製到標籤或從標籤複製。將導致以下行為：

1. 第一個封包是TTL等於1的IP封包。路由器A會遞減TTL、捨棄封包，並向來源傳送ICMP TTL超出訊息。
2. 第二個資料包是TTL等於2的IP資料包。路由器A遞減TTL，標籤資料包，並將MPLS報頭中的TTL設定為255。
3. 路由器B將MPLS報頭中的TTL降低到254，刪除MPLS標籤，並將MPLS報頭中的TTL值複製到IP報頭的TTL欄位中。
4. 路由器C遞減IP TTL，並將資料包傳送到下一跳路由器C2。資料包已到達最終目的地。

## 相關資訊

- [瞭解 Ping 和 Traceroute 命令](#)
- [mpls ip propagate-ttl命令](#)
- [MPLS技術支援頁面](#)
- [技術支援 - Cisco Systems](#)