MPLS LSP Ping, Traceroute, and AToM VCCV

As Multiprotocol Label Switching (MPLS) deployments increase and the traffic types they carry increase, the ability of service providers to monitor label switched paths (LSPs) and quickly isolate MPLS forwarding problems is critical to their ability to offer services. The MPLS LSP Ping, Traceroute, and AToM VCCV feature helps them mitigate these challenges.

The MPLS LSP Ping, Traceroute, and AToM VCCV feature can detect when an LSP fails to deliver user traffic.

- You can use MPLS LSP Ping to test LSP connectivity for IPv4 Label Distribution Protocol (LDP) prefixes, traffic engineering (TE) Forwarding Equivalence Classes (FECs), and AToM FECs.
- You can use MPLS LSP Traceroute to trace the LSPs for IPv4 LDP prefixes and TE tunnel FECs.
- Any Transport over MPLS Virtual Circuit Connection Verification (AToM VCCV) allows you to use MPLS LSP Ping to test the pseudowire (PW) section of an AToM virtual circuit (VC).

Internet Control Message Protocol (ICMP) ping and trace are often used to help diagnose the root cause when a forwarding failure occurs. The MPLS LSP Ping, Traceroute, and AToM VCCV feature extends this diagnostic and troubleshooting ability to the MPLS network and aids in the identification of inconsistencies between the IP and MPLS forwarding tables, inconsistencies in the MPLS control and data plane, and problems with the reply path.

The MPLS LSP Ping, Traceroute, and AToM VCCV feature uses MPLS echo request and reply packets to test LSPs. The Cisco implementation of MPLS echo request and echo reply are based on the Internet Engineering Task Force (IETF) Internet-Draft Detecting MPLS Data Plane Failures.

- Prerequisites for MPLS LSP Ping, Traceroute, and AToM VCCV, on page 1
- Restrictions for MPLS LSP Ping, Traceroute, and AToM VCCV, on page 2
- Information About MPLS LSP Ping, Traceroute, and AToM VCCV, on page 2

Prerequisites for MPLS LSP Ping, Traceroute, and AToM VCCV

Before you use the MPLS LSP Ping, Traceroute, and AToM VCCV feature, you should:

- Determine the baseline behavior of your Multiprotocol Label Switching (MPLS) network. For example:
  - What is the expected MPLS experimental (EXP) treatment?
  - What is the expected maximum size packet or maximum transmission unit (MTU) of the label switched path?
• What is the topology? What are the expected label switched paths? How many links in the label switching path (LSP)? Trace the paths of the label switched packets including the paths for load balancing.

• Understand how to use MPLS and MPLS applications, including traffic engineering, Any Transport over MPLS (AToM), and Label Distribution Protocol (LDP). You need to
  • Know how LDP is configured
  • Understand AToM concepts
  • Be able to troubleshoot a TE tunnel
• Understand label switching, forwarding, and load balancing.

Restrictions for MPLS LSP Ping, Traceroute, and AToM VCCV

• You cannot use MPLS LSP Traceroute to trace the path taken by Any Transport over Multiprotocol Label Switching (AToM) packets. MPLS LSP Traceroute is not supported for AToM. (MPLS LSP Ping is supported for AToM.) However, you can use MPLS LSP Traceroute to troubleshoot the Interior Gateway Protocol (IGP) LSP that is used by AToM.

• You cannot use MPLS LSP Ping or Traceroute to validate or trace MPLS Virtual Private Networks (VPNs).

• You cannot use MPLS LSP Traceroute to troubleshoot label switching paths (LSPs) that employ time-to-live (TTL) hiding.

Information About MPLS LSP Ping, Traceroute, and AToM VCCV

MPLS LSP Ping Operation

MPLS LSP Ping uses Multiprotocol Label Switching (MPLS) echo request and reply packets to validate a label switched path (LSP). Both an MPLS echo request and an MPLS echo reply are User Datagram Protocol (UDP) packets with source and destination ports set to 3503.

The MPLS echo request packet is sent to a target device through the use of the appropriate label stack associated with the LSP to be validated. Use of the label stack causes the packet to be switched inband of the LSP (that is, forwarded over the LSP itself). The destination IP address of the MPLS echo request packet is different from the address used to select the label stack. The destination address of the UDP packet is defined as a 127.x.y.z/8 address. This prevents the IP packet from being IP switched to its destination if the LSP is broken.

An MPLS echo reply is sent in response to an MPLS echo request. It is sent as an IP packet and forwarded using IP, MPLS, or a combination of both types of switching. The source address of the MPLS echo reply packet is an address from the device generating the echo reply. The destination address is the source address of the device in the MPLS echo request packet.

The figure below shows the echo request and echo reply paths for MPLS LSP Ping.
If you initiate an MPLS LSP Ping request at LSR1 to a Forwarding Equivalence Class (FEC), at LSR6, you get the results shown in the table below.

**Table 1: MPLS LSP Ping Example**

<table>
<thead>
<tr>
<th>Step</th>
<th>Device</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>LSR1</td>
<td>Initiates an MPLS LSP Ping request for an FEC at the target device LSR6 and sends an MPLS echo request to LSR2.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR2</td>
<td>Receives and forwards the MPLS echo request packet through transit devices LSR3 and LSR4 to the penultimate device LSR5.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR5</td>
<td>Receives the MPLS echo request, pops the MPLS label, and forwards the packet to LSR6 as an IP packet.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR6</td>
<td>Receives the IP packet, processes the MPLS echo request, and sends an MPLS echo reply to LSR1 through an alternate route.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR7 to LSR10</td>
<td>Receive and forward the MPLS echo reply back toward LSR1, the originating device.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR1</td>
<td>Receives the MPLS echo reply in response to the MPLS echo request.</td>
</tr>
</tbody>
</table>

You can use MPLS LSP Ping to validate IPv4 Label Distribution Protocol (LDP), Any Transport over MPLS (AToM), and IPv4 Resource Reservation Protocol (RSVP) FECs by using appropriate keywords and arguments with the command:

```
ping mpls
  [ipv4
    destination-address destination-mask
    | pseudowire
    ipv4-address
    vc-id
    | traffic-eng
  tunnel-interface tunnel-number ]
```
MPLS LSP Traceroute Operation

MPLS LSP Traceroute also uses Multiprotocol Label Switching (MPLS) echo request and reply packets to validate a label switched path (LSP). The echo request and echo reply are User Datagram Protocol (UDP) packets with source and destination ports set to 3503.

The MPLS LSP Traceroute feature uses time-to-live (TTL) settings to force expiration of the TTL along an LSP. MPLS LSP Traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4, ...) to discover the downstream mapping of each successive hop. The success of the LSP traceroute depends on the transit device processing the MPLS echo request when it receives a labeled packet with a TTL of 1. On Cisco devices, when the TTL expires, the packet is sent to the Route Processor (RP) for processing. The transit device returns an MPLS echo reply containing information about the transit hop in response to the TTL-expired MPLS packet.

The figure below shows an MPLS LSP Traceroute example with an LSP from LSR1 to LSR4.

Figure 2: MPLS LSP Traceroute Example

If you enter an LSP traceroute to a Forwarding Equivalence Class (FEC) at LSR4 from LSR1, you get the results shown in the table below.

Table 2: MPLS LSP Traceroute Example

<table>
<thead>
<tr>
<th>Step</th>
<th>Device</th>
<th>MPLS Packet Type and Description</th>
<th>Device Action</th>
</tr>
</thead>
</table>
| 1.   | LSR1   | MPLS echo request—With a target FEC pointing to LSR4 and to a downstream mapping. | • Sets the TTL of the label stack to 1.  
• Sends the request to LSR2. |
| 1.   | LSR2   | MPLS echo reply. | Receives packet with TTL = 1.  
• Processes the UDP packet as an MPLS echo request.  
• Finds a downstream mapping, replies to LSR1 with its own downstream mapping based on the incoming label, and sends a reply. |
| 1.   | LSR1   | MPLS echo request—With the same target FEC and the downstream mapping received in the echo reply from LSR2. | • Sets the TTL of the label stack to 2.  
• Sends the request to LSR2. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Device</th>
<th>MPLS Packet Type and Description</th>
<th>Device Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>LSR2</td>
<td>MPLS echo request.</td>
<td>Receives packet with TTL = 2.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Decrement the TTL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Forwards the echo request to LSR3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Processes the UDP packet as an MPLS echo request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Finds a downstream mapping and replies to LSR1 with its own downstream mapping based on the incoming label.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR1</td>
<td>MPLS echo request—With the same target FEC and the downstream mapping received in the echo reply from LSR3.</td>
<td>• Sets the TTL of the packet to 3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sends the request to LSR2.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR2</td>
<td>MPLS echo request.</td>
<td>Receives packet with TTL = 3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Decrement the TTL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Forwards the echo request to LSR3.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR3</td>
<td>MPLS echo request.</td>
<td>Receives packet with TTL = 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Decrement the TTL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Forwards the echo request to LSR4.</td>
</tr>
<tr>
<td>1.</td>
<td>LSR4</td>
<td>MPLS echo reply.</td>
<td>Receives packet with TTL = 1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Processes the UDP packet as an MPLS echo request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Finds a downstream mapping and also finds that the device is the egress device for the target FEC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Replies to LSR1.</td>
</tr>
</tbody>
</table>

You can use MPLS LSP Traceroute to validate IPv4 Label Distribution Protocol (LDP) and IPv4 RSVP FECs by using appropriate keywords and arguments with the `trace mpls` command:

```
trace mpls ipv4 {destination-address destination-mask | traffic-eng
tunnel-interface tunnel-number}
```

By default, the TTL is set to 30. Therefore, the traceroute output always contains 30 lines, even if an LSP problem exists. This might mean duplicate entries in the output, should an LSP problem occur. The device address of the last point that the trace reaches is repeated until the output is 30 lines. You can ignore the duplicate entries. The following example shows that the trace encountered an LSP problem at the device that has an IP address of 10.6.1.6:

```
Device# traceroute mpls ipv4 10.6.7.4/32
Tracing MPLS Label Switched Path to 10.6.7.4/32, timeout is 2 seconds
Codes: '!' = success, 'Q' = request not transmitted,
```
'. ' - timeout, 'U' - unreachable, 
'R' - downstream router but not target

Type escape sequence to abort.
0 10.6.1.14 MRU 4470 [Labels: 22 Exp: 0]
R 1 10.6.1.15 MRU 4470 [Labels: 21 Exp: 0] 2 ms
R 2 10.6.1.16 4 ms
R 3 10.6.1.16 1 ms
R 4 10.6.1.16 1 ms
R 5 10.6.1.16 3 ms
R 6 10.6.1.16 4 ms
R 7 10.6.1.16 1 ms
R 8 10.6.1.16 2 ms
R 9 10.6.1.16 3 ms
R 10 10.6.1.16 4 ms
R 11 10.6.1.16 1 ms
R 12 10.6.1.16 2 ms
R 13 10.6.1.16 4 ms
R 14 10.6.1.16 5 ms
R 15 10.6.1.16 2 ms
R 16 10.6.1.16 3 ms
R 17 10.6.1.16 4 ms
R 18 10.6.1.16 2 ms
R 19 10.6.1.16 3 ms
R 20 10.6.1.16 4 ms
R 21 10.6.1.16 1 ms
R 22 10.6.1.16 2 ms
R 23 10.6.1.16 3 ms
R 24 10.6.1.16 4 ms
R 25 10.6.1.16 1 ms
R 26 10.6.1.16 3 ms
R 27 10.6.1.16 4 ms
R 28 10.6.1.16 1 ms
R 29 10.6.1.16 2 ms
R 30 10.6.1.16 3 ms

Any Transport over MPLS Virtual Circuit Connection Verification

AToM Virtual Circuit Connection Verification (AToM VCCV) allows the sending of control packets inband of an AToM pseudowire (PW) from the originating provider edge (PE) device. The transmission is intercepted at the destination PE device, instead of being forwarded to the customer edge (CE) device. This capability allows you to use MPLS LSP Ping to test the PW section of AToM virtual circuits (VCs).

AToM VCCV consists of the following:
• A signaled component in which the AToM VCCV capabilities are advertised during VC label signaling
• A switching component that causes the AToM VC payload to be treated as a control packet

**AToM VCCV Signaling**

One of the steps involved in Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) setup is the signaling of VC labels and AToM Virtual Circuit Connection Verification (VCCV) capabilities between AToM VC endpoints. The device uses an optional parameter, defined in the Internet Draft draft-ieft-pwe3-vccv-01.txt, to communicate the AToM VCCV disposition capabilities of each endpoint.

The AToM VCCV disposition capabilities are categorized as follows:

• Applications—MPLS LSP Ping and Internet Control Message Protocol (ICMP) Ping are applications that AToM VCCV supports to send packets inband of an AToM PW for control purposes.
• Switching modes—Type 1 and Type 2 are switching modes that AToM VCCV uses for differentiating between control and data traffic.

The table below describes AToM VCCV Type 1 and Type 2 switching modes.

**Table 3: Type 1 and Type 2 AToM VCCV Switching Modes**

<table>
<thead>
<tr>
<th>Switching Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>Uses a Protocol ID (PID) field in the AToM control word to identify an AToM VCCV packet.</td>
</tr>
<tr>
<td>Type 2</td>
<td>Uses an MPLS Router Alert Label above the VC label to identify an AToM VCCV packet.</td>
</tr>
</tbody>
</table>

**Selection of AToM VCCV Switching Types**

Cisco devices always use Type 1 switching, if available, when they send MPLS LSP Ping packets over an Any Transport over Multiprotocol Label Switching (AToM) virtual circuit (VC) control channel. Type 2 switching accommodates those VC types and implementations that do not support or interpret the AToM control word.

The table below shows the AToM Virtual Circuit Connection Verification (VCCV) switching mode advertised and the switching mode selected by the AToM VC.

**Table 4: AToM VCCV Switching Mode Advertised and Selected by AToM Virtual Circuit**

<table>
<thead>
<tr>
<th>Type Advertised</th>
<th>Type Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>AToM VCCV not supported</td>
<td>–</td>
</tr>
<tr>
<td>Type 1 AToM VCCV switching</td>
<td>Type 1 AToM VCCV switching</td>
</tr>
<tr>
<td>Type 2 AToM VCCV switching</td>
<td>Type 2 AToM VCCV switching</td>
</tr>
<tr>
<td>Type 1 and Type 2 AToM VCCV switching</td>
<td>Type 1 AToM VCCV switching</td>
</tr>
</tbody>
</table>

An AToM VC advertises its AToM VCCV disposition capabilities in both directions: that is, from the originating device (PE1) to the destination device (PE2), and from PE2 to PE1.
In some instances, AToM VCs might use different switching types if the two endpoints have different AToM VCCV capabilities. If PE1 supports Type 1 and Type 2 AToM VCCV switching and PE2 supports only Type 2 AToM VCCV switching, there are two consequences:

- LSP ping packets sent from PE1 to PE2 are encapsulated with Type 2 switching.
- LSP ping packets sent from PE2 to PE1 use Type 1 switching.

You can determine the AToM VCCV capabilities advertised to and received from the peer by entering the `show mpls l2transport binding` command at the PE device. For example:

```
Device# show mpls l2transport binding
Destination Address: 10.131.191.252, VC ID: 333
  Local Label: 16
      Cbit: 1,  VC Type: FastEthernet,  GroupID: 0
      MTU: 1500,  Interface Desc: n/a
  VCCV Capabilities: Type 1, Type 2
Remote Label: 19
      Cbit: 1,  VC Type: FastEthernet,  GroupID: 0
      MTU: 1500,  Interface Desc: n/a
  VCCV Capabilities: Type 1
```

**Command Options for ping mpls and trace mpls**

MPLS LSP Ping and Traceroute command options are specified as keywords and arguments on the `ping mpls` and `trace mpls` commands.

The `ping mpls` command provides the options displayed in the command syntax below:

```
ping mpls ipv4 {destination-address/destination-mask [destination address-start address-end increment] [ttl time-to-live] | pseudowire ipv4-address vc-id vc-id [destination address-start address-end increment] | traffic-eng tunnel-interface tunnel-number [ttl time-to-live]} [source source-address] [repeat count] [timeout seconds] [[size packet-size] | [sweep minimum maximum size-Increment]] [pad pattern] [reply mode {ipv4 | router-alert}] [interval msec] [exp exp-bits] [verbose]
```

The `trace mpls` command provides the options displayed in the command syntax below:

```
trace mpls {ipv4 destination-address/destination-mask [destination address-start [address-end [address-increment]]] | traffic-eng tunnel tunnel-interface-number} [source source-address] [timeout seconds] [reply mode reply-mode] [ttl maximum-time-to-live] [exp exp-bits]
```

**Selection of FECs for Validation**

A label switched path (LSP) is formed by labels. Devices learn labels through the Label Distribution Protocol (LDP), traffic engineering (TE), Any Transport over Multiprotocol Label Switching (AToM), or other MPLS applications. You can use MPLS LSP Ping and Traceroute to validate an LSP used for forwarding traffic for a given Forwarding Equivalence Class (FEC). The table below lists the keywords and arguments for the `ping mpls` and `traceroute mpls` commands that allow the selection of an LSP for validation.
Table 5: Selection of LSPs for Validation

<table>
<thead>
<tr>
<th>FEC Type</th>
<th>ping mpls Keyword and Argument</th>
<th>traceroute mpls Keyword and Argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDP IPv4 prefix</td>
<td><code>ipv4 destination-address destination-mask</code></td>
<td><code>ipv4 destination-address destination-mask</code></td>
</tr>
<tr>
<td>MPLS TE tunnel</td>
<td><code>traffic-eng tunnel-interface tunnel-number</code></td>
<td><code>traffic-eng tunnel-interface tunnel-number</code></td>
</tr>
<tr>
<td>AToM VC</td>
<td><code>pseudowire ipv4-address vc-id vc-id</code></td>
<td>MPLS LSP Traceroute does not support the AToM tunnel LSP type for this release.</td>
</tr>
</tbody>
</table>

Reply Mode Options for MPLS LSP Ping and Traceroute

The reply mode is used to control how the responding device replies to a Multiprotocol Label Switching (MPLS) echo request sent by an MPLS LSP Ping or MPLS LSP Traceroute command. The table below describes the reply mode options.

Table 6: Reply Mode Options for a Responding Device

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4</code></td>
<td>Reply with an IPv4 User Datagram Protocol (UDP) packet (default). This is the most common reply mode selected for use with an MPLS LSP Ping and Traceroute command when you want to periodically poll the integrity of a label switched path (LSP). With this option, you do not have explicit control over whether the packet traverses IP or MPLS hops to reach the originator of the MPLS echo request. If the headend device fails to receive a reply, select the router-alert option, “Reply with an IPv4 UDP packet with a router alert.” The responding device sets the IP precedence of the reply packet to 6. You implement this option using the <code>reply mode ipv4</code> keywords.</td>
</tr>
<tr>
<td><code>router-alert</code></td>
<td>Reply with an IPv4 UDP packet with a device alert. This reply mode adds the router alert option to the IP header. This forces the packet to be special handled by the Cisco device at each intermediate hop as it moves back to the destination. This reply mode is more expensive, so use the router-alert option only if you are unable to get a reply with the <code>ipv4</code> option, “Reply with an IPv4 UDP packet.” You implement this option using the <code>reply mode router-alert</code> keywords.</td>
</tr>
</tbody>
</table>

The reply with an IPv4 UDP packet implies that the device should send an IPv4 UDP packet in reply to an MPLS echo request. If you select the `ipv4` reply mode, you do not have explicit control over whether the packet uses IP or MPLS hops to reach the originator of the MPLS echo request. This is the mode that you would normally use to test and verify LSPs.

The reply with an IPv4 UDP packet that contains a device alert forces the packet to go back to the destination and be processed by the Route Processor (RP) process switching at each intermediate hop. This bypasses hardware/line card forwarding table inconsistencies. You should select this option when the originating (headend) devices fail to receive a reply to the MPLS echo request.
You can instruct the replying device to send an echo reply with the IP router alert option by using one of the following commands:

```
ping mpls
  {ipv4 destination-address/destination-mask | pseudowire ipv4-address
   vc-id vc-id | traffic-eng tunnel-interface tunnel-number}
reply mode router-alert
```
or

```
trace mpls
  {ipv4 destination-address/destination-mask
   | traffic-eng tunnel-interface tunnel-number
  } reply mode router-alert
```

However, the reply with a router alert adds overhead to the process of getting a reply back to the originating device. This method is more expensive to process than a reply without a router alert and should be used only if there are reply failures. That is, the reply with a router alert label should only be used for MPLS LSP Ping or MPLS LSP Traceroute when the originating (headend) device fails to receive a reply to an MPLS echo request.

**Reply Mode Options for MPLS LSP Ping and Traceroute**

The reply mode is used to control how the responding device replies to a Multiprotocol Label Switching (MPLS) echo request sent by an MPLS LSP Ping or MPLS LSP Traceroute command. The table below describes the reply mode options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>Reply with an IPv4 User Datagram Protocol (UDP) packet (default). This is the most common reply mode selected for use with an MPLS LSP Ping and Traceroute command when you want to periodically poll the integrity of a label switched path (LSP). With this option, you do not have explicit control over whether the packet traverses IP or MPLS hops to reach the originator of the MPLS echo request. If the headend device fails to receive a reply, select the router-alert option, “Reply with an IPv4 UDP packet with a router alert.” The responding device sets the IP precedence of the reply packet to 6. You implement this option using the <code>reply mode ipv4</code> keywords.</td>
</tr>
<tr>
<td>router-alert</td>
<td>Reply with an IPv4 UDP packet with a device alert. This reply mode adds the router alert option to the IP header. This forces the packet to be special handled by the Cisco device at each intermediate hop as it moves back to the destination. This reply mode is more expensive, so use the router-alert option only if you are unable to get a reply with the ipv4 option, “Reply with an IPv4 UDP packet.” You implement this option using the <code>reply mode router-alert</code> keywords.</td>
</tr>
</tbody>
</table>
Packet uses IP or MPLS hops to reach the originator of the MPLS echo request. This is the mode that you would normally use to test and verify LSPs.

The reply with an IPv4 UDP packet that contains a device alert forces the packet to go back to the destination and be processed by the Route Processor (RP) process switching at each intermediate hop. This bypasses hardware/line card forwarding table inconsistencies. You should select this option when the originating (headend) devices fail to receive a reply to the MPLS echo request.

You can instruct the replying device to send an echo reply with the IP router alert option by using one of the following commands:

```
ping mpls
  {ipv4 destination-address/destination-mask | pseudowire ipv4-address
   vc-id vc-id | traffic-eng tunnel-interface tunnel-number}
  reply mode router-alert
```

or

```
trace mpls
  {ipv4 destination-address/destination-mask
   | traffic-eng tunnel-interface tunnel-number}
  reply mode router-alert
```

However, the reply with a router alert adds overhead to the process of getting a reply back to the originating device. This method is more expensive to process than a reply without a router alert and should be used only if there are reply failures. That is, the reply with a router alert label should only be used for MPLS LSP Ping or MPLS LSP Traceroute when the originating (headend) device fails to receive a reply to an MPLS echo request.

### Packet Handling Along Return Path with an IP MPLS Router Alert

When an IP packet that contains an IP router alert option in its IP header or a Multiprotocol Label Switching (MPLS) packet with a router alert label as its outermost label arrives at a device, the device punts (redirects) the packet to the Route Processor (RP) process level for handling. This allows these packets to bypass the forwarding failures in hardware routing tables. The table below describes how IP and MPLS packets with an IP router alert option are handled by the device switching path processes.

#### Table 8: Switching Path Process Handling of IP and MPLS Router Alert Packets

<table>
<thead>
<tr>
<th>Incoming Packet</th>
<th>Normal Switching Action</th>
<th>Process Switching Action</th>
<th>Outgoing Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP packet—Router alert option in IP header</td>
<td>A router alert option in the IP header causes the packet to be punted to the process switching path.</td>
<td>Forwards the packet as is.</td>
<td>IP packet—Router alert option in IP header.</td>
</tr>
<tr>
<td></td>
<td>A router alert option in the IP header causes the packet to be punted to the process switching path.</td>
<td>Adds a router alert as the outermost label and forwards as an MPLS packet.</td>
<td>MPLS packet—Outermost label contains a router alert.</td>
</tr>
</tbody>
</table>
### Other MPLS LSP Ping and Traceroute Command Options

The table below describes other MPLS LSP Ping and Traceroute command options that can be specified as keywords or arguments with the `ping mpls` command, or with both the `ping mpls` and `trace mpls` commands. Options available to use only on the `ping mpls` command are indicated as such.

**Table 9: Other MPLS LSP Ping and Traceroute and AToM VCCV Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datagram size</td>
<td>Size of the packet with the label stack imposed. Specified with the <code>size packet-size</code> keyword and argument. The default size is 100. For use with the MPLS LSP Ping feature only.</td>
</tr>
<tr>
<td>Padding</td>
<td>Padding (the pad time-length-value [TLV]) is used as required to fill the datagram so that the MPLS echo request (User Datagram Protocol [UDP] packet with a label stack) is the size specified. Specify with the <code>pad pattern</code> keyword and argument. For use with the MPLS LSP Ping feature only.</td>
</tr>
<tr>
<td>Sweep size range</td>
<td>Parameter that enables you to send a number of packets of different sizes, ranging from a start size to an end size. This parameter is similar to the Internet Control Message Protocol (ICMP) ping sweep parameter. The lower boundary on the sweep range varies depending on the label switched path (LSP) type. You can specify a sweep size range when you use the <code>ping mpls</code> command. Use the <code>sweep minimum maximum size-increment</code> keyword and arguments. For use with the MPLS LSP Ping feature only.</td>
</tr>
<tr>
<td>Repeat count</td>
<td>Number of times to resend the same packet. The default is 5 times. You can specify a repeat count when you use the <code>ping mpls</code> command. Use the <code>repeat count</code> keyword and argument. For use with the MPLS LSP Ping feature only.</td>
</tr>
<tr>
<td>MPLS echo request source address</td>
<td>Routable address of the sender. The default address is loopback0. This address is used as the destination address in the Multiprotocol Label Switching (MPLS) echo response. Use the <code>source source-address</code> keyword and argument. For use with the MPLS LSP Ping and Traceroute features.</td>
</tr>
</tbody>
</table>
The MPLS echo request destination address in the UDP packet is not used to forward the MPLS packet to the destination device. The label stack that is used to forward the echo request routes the MPLS packet to the destination device. The 127/8 address guarantees that the packets are routed to the localhost (the default loopback address of the device processing the address) if the UDP packet destination address is used for forwarding.

In addition, the destination address is used to affect load balancing when the destination address of the IP payload is used for load balancing.

For use with IPv4 and Any Transport over MPLS (AToM) Forwarding Equivalence Classes (FECs) with the MPLS LSP Ping feature and with IPv4 FECs with the MPLS LSP Traceroute feature.

### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UDP destination address</strong></td>
<td>A valid 127/8 address. You have the option to specify a single x.y.z or a range of numbers between 0.0.0 and x.y.z, where x.y.z are numbers between 0 and 255 and correspond to 127.x.y.z. Use the <code>destination</code> {address | address-start address-end increment} keyword and arguments.</td>
</tr>
<tr>
<td><strong>Time-to-live (TTL)</strong></td>
<td>A parameter you can set that indicates the maximum number of hops a packet should take to reach its destination. The time-to-live (TTL) field in a packet is decremented by 1 each time it travels through a device.</td>
</tr>
<tr>
<td><strong>Timeouts</strong></td>
<td>A parameter you can specify to control the timeout in seconds for an MPLS request packet. The range is from 0 to 3600 seconds. The default is 2.</td>
</tr>
<tr>
<td><strong>Intervals</strong></td>
<td>A parameter you can specify to set the time in milliseconds between successive MPLS echo requests. The default is 0.</td>
</tr>
<tr>
<td><strong>Experimental bits</strong></td>
<td>Three experimental bits in an MPLS header used to specify precedence for the MPLS echo reply. (The bits are commonly called EXP bits.) The range is from 0 to 7, and the default is 0.</td>
</tr>
</tbody>
</table>

For use with MPLS LSP Ping and Traceroute features.
### Option Interactions and Loops

Usage examples for the MPLS LSP Ping and Traceroute and AToM VCCV feature in this and subsequent sections are based on the sample topology shown in the figure below.

**Figure 3: Sample Topology for Configuration Examples**

The interaction of some MPLS LSP Ping and Traceroute and AToM VCCV options can cause loops. See the following topic for a description of the loops you might encounter with the ping mpls and trace mpls commands:

#### Possible Loops with MPLS LSP Ping

With the MPLS LSP Ping feature, loops can occur if you use the repeat count option, the sweep size range option, or the User Datagram Protocol (UDP) destination address range option.
ping mpls
    [ipv4 destination-address/destination-mask]
    [destination address-start address-end increment] | pseudowire ipv4-address
    vc-id vc-id
    [destination address-start address-end increment] |
    traffic-eng tunnel-interface tunnel-number
    [repeat count]
    [sweep minimum maximum size-increment]

Following is an example of how a loop operates if you use the following keywords and arguments on the ping mpls command:

Device# ping mpls
ipv4
   10.131.159.251/32 destination 127.0.0.1 127.0.0.1 0.0.0.1 repeat 2
sweep 1450 1475 25
Sending 2, [1450..1500]-byte MPLS Echos to 10.131.159.251/32,
timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not transmitted,
'.' - timeout, 'U' - unreachable, 'R' - downstream router but not target
Type escape sequence to abort.
Destination address 127.0.0.1
!
!
Destination address 127.0.0.1
!
!
Destination address 127.0.0.1
!
!
Destination address 127.0.0.1
!
!
An mpls ping command is sent for each packet size range for each destination address until the end address is reached. For this example, the loop continues in the same manner until the destination address, 127.0.0.1, is reached. The sequence continues until the number is reached that you specified with the repeat count keyword and argument. For this example, the repeat count is 2. The MPLS LSP Ping loop sequence is as follows:

repeat = 1
    destination address 1 (address-start )
    for (size from sweep
        minimum to maximum , counting by size-increment
    )
        send an lsp ping
        destination address 2 (address-start +
        address-increment )
        for (size from sweep
            minimum to maximum , counting by size-increment
        )
            send an lsp ping
Possible Loop with MPLS LSP Traceroute

With the MPLS LSP Traceroute feature, loops can occur if you use the User Datagram Protocol (UDP) destination address range option and the time-to-live option.

```
trace mpls
  {ipv4
destination-address destination-mask
    |destination
    address-start
    address-end
    address-increment
    | traffic-eng
tunnel-interface
  }
tunnel-number
ttl
  maximum-
time-to-live
}
```

Here is an example of how a loop operates if you use the following keywords and arguments on the `trace mpls` command:

```
Device# trace mpls
ipv4
  10.131.159.251/32 destination 127.0.0.1 127.0.0.1 1 ttl 5
Tracing MPLS Label Switched Path to 10.131.159.251/32, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not transmitted,
    '.' - timeout, 'U' - unreachable,
    'R' - downstream router but not target
Type escape sequence to abort.
Destination address 127.0.0.1
  0 10.131.191.230 MRU 1500 [Labels: 19 Exp: 0]
  R 1 10.131.159.226 MRU 1504 [implicit-null] 40 ms
  ! 2 10.131.159.225 40 ms
```
An mpls trace command is sent for each TTL from 1 to the maximum TTL (\texttt{ttl maximum-time-to-live} keyword and argument) for each destination address until the address specified with the destination \texttt{end-address} argument is reached. For this example, the maximum TTL is 5 and the end destination address is 127.0.0.1. The MPLS LSP Traceroute loop sequence is as follows:

\begin{verbatim}
destination address 1 \{address-start
    for \{ttl
        from 1 to maximum-time-to-live
    \}
    send an lsp trace
destination address 2 \{address-start
    + address-increment
    for \{ttl
        from 1 to maximum-time-to-live
    \}
    send an lsp trace
destination address 3 \{address-start
    + address-increment
    + address-increment
    for \{ttl
        from 1 to maximum-time-to-live
    \}
    send an lsp trace

until destination address = address-end
\end{verbatim}

\section*{MPLS Echo Request Packets Not Forwarded by IP}

Multiprotocol Label Switching (MPLS) echo request packets sent during a label switched path (LSP) ping are never forwarded by IP. The IP header destination address field in an MPLS echo request packet is a 127.x.y.z/8 address. Devices should not forward packets using a 127.x.y.z/8 address. The 127.x.y.z/8 address corresponds to an address for the local host.

The use of a 127.x.y.z address as a destination address of the User Datagram Protocol (UDP) packet is significant in that the MPLS echo request packet fails to make it to the target device if a transit device does not label switch the LSP. This allows for the detection of LSP breakages.

- If an LSP breakage occurs at a transit device, the MPLS echo packet is not forwarded, but consumed by the device.
- If the LSP is intact, the MPLS echo packet reaches the target device and is processed by the terminal point of the LSP.

The figure below shows the path of the MPLS echo request and reply when a transit device fails to label switch a packet in an LSP.
An Any Transport over MPLS (AToM) payload does not contain usable forwarding information at a transit device because the payload might not be an IP packet. An MPLS virtual private network (VPN) packet, although an IP packet, does not contain usable forwarding information at a transit device because the destination IP address is only significant to the virtual routing and forwarding (VRF) instances at the endpoints of the MPLS network.

### Information Provided by the Device Processing LSP Ping or LSP Traceroute

The table below describes the characters that the device processing an LSP ping or LSP traceroute packet returns to the sender about the failure or success of the request.

You can also view the return code for an MPLS LSP Ping operation if you enter the `ping mpls verbose` command.

#### Table 10: LSP Ping and Traceroute Reply Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period “.”</td>
<td>A timeout occurs before the target device can reply.</td>
</tr>
<tr>
<td>U</td>
<td>The target device is unreachable.</td>
</tr>
<tr>
<td>R</td>
<td>The device processing the Multiprotocol Label Switching (MPLS) echo request is a downstream device but is not the destination.</td>
</tr>
<tr>
<td>Exclamation mark “!”</td>
<td>Replying device is an egress for the destination.</td>
</tr>
<tr>
<td>Q</td>
<td>Echo request was not successfully transmitted. This could be returned because of insufficient memory or more probably because no label switched path (LSP) exists that matches the Forwarding Equivalence Class (FEC) information.</td>
</tr>
<tr>
<td>C</td>
<td>Replying device rejected the echo request because it was malformed.</td>
</tr>
</tbody>
</table>
MTU Discovery in an LSP

During an MPLS LSP Ping, Multiprotocol Label Switching (MPLS) echo request packets are sent with the IP packet attribute set do not fragment. That is, the DF bit is set in the IP header of the packet. This allows you to use the MPLS echo request to test for the MTU that can be supported for the packet through the label switched path (LSP) without fragmentation.

The figure below shows a sample network with a single LSP from PE1 to PE2 formed with labels advertised by means of LDP.

Figure 5: Sample Network with LSP—Labels Advertised by LDP

You can determine the maximum receive unit (MRU) at each hop by tracing the LSP using the MPLS Traceroute feature. The MRU is the maximum size of a labeled packet that can be forwarded through an LSP. The following example shows the results of a `trace mpls` command when the LSP is formed with labels created by the Label Distribution Protocol (LDP):

```
Device# trace mpls ipv4 10.131.159.252/32
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
Codes: '!-' - success, 'Q' - request not transmitted,
'.' - timeout, 'U' - unreachable,
'R' - downstream router but not target
Type escape sequence to abort.
0 10.131.191.230 MRU 1496 [Labels: 22/19 Exp: 0/0]
R 1 10.131.159.226 MRU 1500 [Labels: 19 Exp: 0] 40 ms
R 2 10.131.159.229 MRU 1504 [implicit-null] 28 ms
! 3 10.131.159.230 40 ms
```

You can determine the MRU for the LSP at each hop through the use of the `show forwarding detail` command:

```
Device# show mpls forwarding 10.131.159.252 detail
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag or VC or Tunnel Id switched interface
22 19 10.131.159.252/32 0 Tu1 point2point
MAC/Encaps=14/22, MRU=1496, Tag Stack(22 19), via Et0/0
AABBCC00970000ABBCC0098000847 0001600000013000
No output feature configured
```

To determine the maximum sized echo request that will fit on the LSP, you can find the IP MTU by using the `show interface type number` command:

```
Device# show interface e0/0
FastEthernet0/0/0 is up, line protocol is up
    Hardware is Lance, address is aabb.cc00.9800 (bia aabb.cc00.9800)
    Internet address is 10.131.191.230/30
    MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load ½55
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 00:00:01, output 00:00:01, output hang never
```

MPLS LSP Ping, Traceroute, and AToM VCCV

MTU Discovery in an LSP
LSP Network Management

The IP MTU in the show interface type number example is 1500 bytes. Subtract the number of bytes corresponding to the label stack from the MTU number. From the output of the show mpls forwarding command, the Tag stack consists of one label (21). Therefore, the largest MPLS echo request packet that can be sent in the LSP, shown in the figure above, is 1500 - (2 x 4) = 1492.

You can validate this by using the following ping mpls command:

```
Device# ping mpls ipv4 10.131.159.252/32 sweep 1492 1500 1 repeat 1
Sending 1, [1492..1500]-byte MPLS Echos to 10.131.159.252/32, timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not transmitted, '. ' - timeout, 'U' - unreachable, 'R' - downstream router but not target
Type escape sequence to abort.
!QQQQQQQQ
Success rate is 11 percent (1/9), round-trip min/avg/max = 40/40/40 ms
```

In this command, only packets of 1492 bytes are sent successfully, as indicated by the exclamation point (!). Packets of byte sizes 1493 to 1500 are source-quenched, as indicated by the Q.

You can pad an MPLS echo request so that a payload of a given size can be tested. The pad TLV is useful when you use the MPLS echo request to discover the MTU supportable by an LSP. MTU discovery is extremely important for applications like AToM that contain non-IP payloads that cannot be fragmented.

LSP Network Management

To manage a Multiprotocol Label Switching (MPLS) network you must have the ability to monitor label switched paths (LSPs) and quickly isolate MPLS forwarding problems. You need ways to characterize the liveliness of an LSP and reliably detect when a label switched path fails to deliver user traffic.

You can use MPLS LSP Ping to verify the LSP that is used to transport packets destined for IPv4 Label Distribution Protocol (LDP) prefixes, traffic engineering (TE) tunnels, and Any Transport over MPLS pseudowire Forwarding Equivalence Classes (AToM PW FECs). You can use MPLS LSP Traceroute to trace LSPs that are used to carry packets destined for IPv4 LDP prefixes and TE tunnel FECs.

An MPLS echo request is sent through an LSP to validate it. A TTL expiration or LSP breakage causes the transit device to process the echo request before it gets to the intended destination and returns an MPLS echo reply that contains an explanatory reply code to the originator of the echo request.

The successful echo request is processed at the egress of the LSP. The echo reply is sent via an IP path, an MPLS path, or a combination of both back to the originator of the echo request.
**ICMP ping and trace Commands and Troubleshooting**

Internet Control Message Protocol (ICMP) **ping** and **trace** commands are often used to help diagnose the root cause of a failure. When a label switched path (LSP) is broken, the packet might make its way to the target device by way of IP forwarding, thus making ICMP ping and traceroute unreliable for detecting Multiprotocol Label Switching (MPLS) forwarding problems. The MPLS LSP Ping, Traceroute and AToM VCCV feature extends this diagnostic and troubleshooting ability to the MPLS network and handles inconsistencies between the IP and MPLS forwarding tables, inconsistencies in the MPLS control and data plane, and problems with the reply path.

The figure below shows a sample topology with a Label Distribution Protocol (LDP) LSP and traffic engineering (TE) tunnel LSP.

*Figure 6: Sample Topology with LDP and TE Tunnel LSPs*

This section contains the following topics:

**MPLS LSP Ping and Traceroute Discovers LSP Breakage**

**Configuration for Sample Topology**

These are sample topology configurations for the troubleshooting examples in the following sections (see the figure above). There are the six sample device configurations.

**Device CE1 Configuration**

```bash
version 12.0
!
hostname ce1
!
enable password lab
!
interface Loopback0
  ip address 10.131.191.253 255.255.255.255
  no ip directed-broadcast
!
interface GigabitEthernet0/0/0
  ip address 10.0.0.1 255.255.255.255
  no ip directed-broadcast
  no keepalive
  no cdp enable
!
end
```

**Device PE1 Configuration**

```bash
version 12.0
!
hostname pe1
```
Configuration for Sample Topology

!  
ip cef  
mls label protocol ldp  
mls traffic-eng tunnels  
no mpls traffic-eng auto-bw timers frequency 0  
mls ldp discovery targeted-hello accept  
!  
interface Loopback0  
ip address 10.131.191.252 255.255.255.255  
o no ip directed-broadcast  
!  
interface Tunnel1  
ip unnumbered Loopback0  
o no ip directed-broadcast  
mls label protocol ldp  
mls ip  
tunnel destination 10.131.159.255  
tunnel mode mpls traffic-eng  
tunnel mpls traffic-eng autoroute announce  
tunnel mpls traffic-eng priority 2 2  
tunnel mpls traffic-eng bandwidth 512  
tunnel mpls traffic-eng path-option 1 dynamic  
!  
interface Tunnel2  
ip unnumbered Loopback0  
o no ip directed-broadcast  
shutdown  
mls label protocol ldp  
mls ip  
tunnel destination 10.131.159.255  
tunnel mode mpls traffic-eng  
tunnel mpls traffic-eng autoroute announce  
tunnel mpls traffic-eng priority 1 1  
tunnel mpls traffic-eng path-option 1 dynamic  
!  
interface GigabitEthernet0/0/0  
ip address 10.131.191.230 255.255.255.255  
o no ip directed-broadcast  
mpls traffic-eng tunnels  
mpls ip  
ip rsvp bandwidth 1500 1500  
ip rsvp signalling dscp 0  
!  
interface GigabitEthernet0/0/1  
ip address 10.131.159.246 255.255.255.255  
o no ip directed-broadcast  
o shutdown  
mpls ip  
ip rsvp bandwidth 1500 1500  
ip rsvp signalling dscp 0  
!  
interface GigabitEthernet0/0/2  
o ip address  
o no ip directed-broadcast  
o cdp enable  
xconnect 10.131.159.252 333 encapsulation mpls  
!  
interface GigabitEthernet0/0/3  
o ip address  
o no ip directed-broadcast  
shutdown  
!  
router ospf 1
log-adjacency-changes
passive-interface Loopback0
network 10.131.159.244 0.0.0.3 area 0
network 10.131.191.228 0.0.0.3 area 0
network 10.131.191.232 0.0.0.3 area 0
network 10.131.191.252 0.0.0.0 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
!
ip classless
end

Device P1 Configuration

version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname p1
!
enabled password lab
!
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery targeted-hello accept
!
interface Loopback0
  ip address 10.131.191.251 255.255.255.255
no ip directed-broadcast
!
interface GigabitEthernet0/0/0
  ip address 10.131.191.229 255.255.255.255
no ip directed-broadcast
mpls traffic-eng tunnels
mpls ip
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0
!
interface GigabitEthernet0/0/1
  ip address 10.131.159.226 255.255.255.255
no ip directed-broadcast
mpls traffic-eng tunnels
mpls ip
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0
!
routing ospf 1
log-adjacency-changes
passive-interface Loopback0
network 10.131.159.224 0.0.0.3 area 0
network 10.131.191.228 0.0.0.3 area 0
network 10.131.191.232 0.0.0.3 area 0
network 10.131.191.251 0.0.0.0 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
!
end
Device P2 Configuration

```conf
version 12.0
hostname p2

ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery directed-hello accept

! interface Loopback0
  ip address 10.131.159.251 255.255.255.255
no ip directed-broadcast

! interface GigabitEthernet0/0/0
  ip address 10.131.159.229 255.255.255.255
no ip directed-broadcast
mpls traffic-eng tunnels
mpls ip
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0

! interface GigabitEthernet0/0/1
  ip address 10.131.159.225 255.255.255.255
no ip directed-broadcast
mpls traffic-eng tunnels
mpls ip
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0

router ospf 1
  log-adjacency-changes
  passive-interface Loopback0
  network 10.131.159.224 0.0.0.3 area 0
  network 10.131.159.228 0.0.0.3 area 0
  network 10.131.159.251 0.0.0.0 area 0
  mpls traffic-eng router-id Loopback0
  mpls traffic-eng area 0

end
```

Device PE2 Configuration

```conf
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

hostname pe2

logging snmp-authfail
enable password lab

! clock timezone EST -5
ip subnet-zero
ip cef
no ip domain-lookup
mpls label protocol ldp
mpls ldp logging neighbor-changes
```
mpls ldp explicit-null
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
tag-switching tdp discovery directed-hello accept
frame-relay switching
!
interface Loopback0
  ip address 10.131.159.252 255.255.255.255
  no ip directed-broadcast
!
interface Tunnel0
  ip unnumbered Loopback0
  no ip directed-broadcast
tunnel destination 10.131.191.252
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 5 explicit name as1pe-long-path
!
interface GigabitEthernet0/0/0
  ip address 10.131.159.230 255.255.255.255
  no ip directed-broadcast
  mpls traffic-eng tunnels
tag-switching ip
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0
!
interface GigabitEthernet0/0/1
  ip address 10.131.159.245 255.255.255.255
  no ip directed-broadcast
  mpls traffic-eng tunnels
tag-switching ip
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0
!
interface GigabitEthernet0/0/2
  no ip address
  no ip directed-broadcast
  no cdp enable
  xconnect 10.131.191.252 333 encapsulation mpls
!
interface GigabitEthernet0/0/3
  no ip address
  no ip directed-broadcast
  no cdp enable
  xconnect 10.131.191.252 333 encapsulation mpls
!
interface Serial0/0/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial0/0/1
  no ip address
  no ip directed-broadcast
  shutdown
!
router ospf 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
log-adjacency-changes
passive-interface Loopback0
network 10.131.122.0 0.0.0.3 area 0
network 10.131.159.228 0.0.0.3 area 0
network 10.131.159.232 0.0.0.3 area 0
network 10.131.159.244 0.0.0.3 area 0
network 10.131.159.252 0.0.0.0 area 0
Device CE2 Configuration

version 12.0
!
hostname ce2
!
enable password lab
!
interface Loopback0
  ip address 10.131.159.253 255.255.255.255
  no ip directed-broadcast
!
interface GigabitEthernet0/0/2
  ip address 10.0.0.2 255.255.255.255
  no ip directed-broadcast
  no keepalive
  no cdp enable
!
end

Verifying That the LSP Is Set Up Correctly

A show mpls forwarding-table command shows that tunnel 1 is in the Multiprotocol Label Switching (MPLS) forwarding table.

Device# show mpls forwarding-table 10.131.159.252

<table>
<thead>
<tr>
<th>Local tag</th>
<th>Outgoing tag or VC</th>
<th>Prefix</th>
<th>Bytes tag</th>
<th>Outgoing tag or VC</th>
<th>Tunnel Id</th>
<th>switched</th>
<th>interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>[T] 10.131.159.252</td>
<td>32</td>
<td>0</td>
<td>19</td>
<td>Tu1</td>
<td>point2point</td>
<td></td>
</tr>
</tbody>
</table>

Forwarding through a TSP tunnel.
View additional tagging info with the 'detail' option

A show mpls traffic-eng tunnels tunnel 1 command entered at PE1 displays information about tunnel 1 and verifies that it is forwarding packets with an out label of 22.

Device# show mpls traffic-eng tunnels tunnel 1

Name: PE1_t1 (Tunnel1) Destination: 10.131.159.251
Status:
  Admin: up   Oper: up   Path: valid   Signalling: connected
path option 1, type dynamic (Basis for Setup, path weight 20)
Config Parameters:
  Bandwidth: 512 kbps (Global) Priority: 2 2 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled   LockDown: disabled   Loadshare: 512 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: dynamic path option 1 is active
  BandwidthOverride: disabled   LockDown: disabled   Verbatim: disabled
InLabel : -
OutLabel : FastEthernet0/0/0, 22
RSVP Signalling Info:
  Src 10.131.191.252, Dst 10.131.159.251, Tun_Id 1, Tun_Instance 28
RSVP Path Info:
  My Address: 10.131.191.230
  Explicit Route: 10.131.191.229 10.131.159.226 10.131.159.225 10.131.159.251
  Record Route: NONE
  Tspec: ave rate=512 kbits, burst=1000 bytes, peak rate=512 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=512 kbits, burst=1000 bytes, peak rate=512 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.131.191.230 10.131.191.229 10.131.159.226 10.131.159.225 10.131.159.251
History:
  Tunnel:
    Time since created: 9 days, 14 hours, 12 minutes
    Time since path change: 2 minutes, 18 seconds
  Current LSP:
    Uptime: 2 minutes, 18 seconds
  Prior LSP:
    ID: path option 1 [3]
    Removal Trigger: tunnel shutdown

A `trace mpls` command issued at PE1 verifies that packets with 22 as the outermost label and 19 as the end of stack label are forwarded from PE1 to PE2.

```
Device# trace mpls ipv4 10.131.159.252/32
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not transmitted,
  '.' - timeout, 'U' - unreachable,
  'R' - downstream router but not target
Type escape sequence to abort.
  0 10.131.191.230 MRU 1496 [Labels: 22/19
Exp: 0/0]
R 1 10.131.159.226 MRU 1504 [Labels: 19 Exp: 0] 40 ms
R 2 10.131.159.229 MRU 1504 [implicit-null] 28 ms
! 3 10.131.159.251 40 ms
```

The MPLS LSP Traceroute to PE2 is successful, as indicated by the exclamation point (!).

**Discovering LSP Breakage**

A Label Distribution Protocol (LDP) target-session is established between devices PE1 and P2, as shown in the output of the following `show mpls ldp discovery` command:

```
Device# show mpls ldp discovery

Local LDP Identifier:
```
10.131.191.252:0
Discovery Sources:
Interfa...e the following command on the P2 device in global configuration mode:
Device# no mpls ldp discovery targeted-hello accept

The LDP configuration change causes the targeted LDP session between the headend and tailend of the traffic engineering (TE) tunnel to go down. Labels for IPv4 prefixes learned by P2 are not advertised to PE1. Thus, all IP prefixes reachable by P2 are reachable by PE1 only through IP (not MPLS). In other words, packets destined for those prefixes through Tunnel 1 at PE1 will be IP switched at P2 (which is undesirable).

The following **show mpls ldp discovery** command shows that the LDP targeted-session is down:

Device# show mpls ldp discovery

Enter the following **show mpls forwarding-table** command at the PE1 device. The display shows that the outgoing packets are untagged as a result of the LDP configuration changes.

Device# show mpls forwarding-table 10.131.159.252

A **ping mpls** command entered at the PE1 device displays the following:
The `ping mpls` command fails. The R indicates that the sender of the Multiprotocol Label Switching (MPLS) echo reply had a routing entry but no MPLS Forwarding Equivalence Class (FEC). Entering the `ping mpls verbose` command displays the MPLS label switched path (LSP) echo reply sender address and the return code. You should be able to solve the problem by Telneting to the replying device and inspecting its forwarding and label tables. You might need to look at the neighboring upstream device as well, because the breakage might be on the upstream device.

```
Device# ping mpls ipv4 10.131.159.252/32 repeat 1 verbose
Sending 1, 100-byte MPLS Echos to 10.131.159.252/32, timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not transmitted, '.' - timeout, 'U' - unreachable, 'R' - downstream router but not target
Type escape sequence to abort.
R 10.131.159.225, return code 6
Success rate is 0 percent (0/1)
```

Alternatively, use the LSP `traceroute` command to figure out which device caused the breakage. In the following example, for subsequent values of TTL greater than 2, the same device keeps responding (10.131.159.225). This suggests that the MPLS echo request keeps getting processed by the device regardless of the TTL. Inspection of the label stack shows that P1 pops the last label and forwards the packet to P2 as an IP packet. This explains why the packet keeps getting processed by P2. MPLS echo request packets cannot be forwarded by use of the destination address in the IP header because the address is set to a 127/8 address.

```
Device# trace mpls ipv4 10.131.159.252/32 ttl 5
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not transmitted, '.' - timeout, 'U' - unreachable, 'R' - downstream router but not target
Type escape sequence to abort.
0 10.131.191.230 MRU 1500 [Labels: 22 Exp: 0]
R 1 10.131.159.226 MRU 1504 [implicit-null] 40 ms
R 2 10.131.159.225 40 ms
R 3 10.131.159.225 40 ms
R 4 10.131.159.225 40 ms
R 5 10.131.159.225 40 ms
```

### MPLS LSP Traceroute Tracks Untagged Cases

This troubleshooting section contains examples of how to use MPLS LSP Traceroute to determine potential issues with packets that are tagged as implicit null and packets that are untagged.

Untagged output interfaces at a penultimate hop do not impact the forwarding of IP packets through a label switched path (LSP) because the forwarding decision is made at the penultimate hop through use of the incoming label. The untagged case causes Any Transport over Multiprotocol Label Switching (AToM) and MPLS virtual private network (VPN) traffic to be dropped at the penultimate hop.

#### Troubleshooting Implicit Null Cases

In the following example, Tunnel 1 is shut down, and only a label switched path (LSP) formed with Label Distribution Protocol (LDP) labels is established. An implicit null is advertised between the P2 and PE2 devices. Entering an MPLS LSP Traceroute at the PE1 device results in the following display:

```
Device# trace mpls ipv4 10.131.159.252/32
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
Codes: '!' - success, 'Q' - request not transmitted, '.' - timeout, 'U' - unreachable,
```
Troubleshooting Untagged Cases

Untagged cases are valid configurations for Interior Gateway Protocol (IGP) label switched paths (LSPs) that could cause problems for Multiprotocol Label Switching (MPLS) virtual private networks (VPNs).

A `show mpls forwarding-table` command and a `show mpls ldp discovery` command issued at the P2 device show that the Label Distribution Protocol (LDP) is properly set up:

```
Device# show mpls forwarding-table 10.131.159.252
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
19 Pop tag 10.131.159.252/32 864 Et0/0 10.131.159.230
```

The `show mpls ldp discovery` command output shows that GigabitEthernet0/0/0, which connects PE2 to P2, is sending and receiving packets.

If a `no mpls ip` command is entered on GigabitEthernet0/0/0, this could prevent an LDP session between the P2 and PE2 devices from being established. A `show mpls ldp discovery` command entered on the PE device shows that the MPLS LDP session with the PE2 device is down:

```
Device# show mpls ldp discovery
Local LDP Identifier:
  10.131.159.251:0
Discovery Sources:
Interfaces:
  GigabitEthernet0/0/0 (ldp): xmit/recv
    LDP Id: 10.131.159.252:0
  FastEthernet1/0/0 (ldp): xmit/recv
    LDP Id: 10.131.191.251:0
```

If the MPLS LDP session to PE2 goes down, the LSP to 10.131.159.252 becomes untagged, as shown by the `show mpls forwarding-table` command:

```
Device# show mpls forwarding-table 10.131.159.252
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
19 Unagged 10.131.159.252/32 864 Et0/0 10.131.159.230
```
Untagged cases would provide an MPLS LSP Traceroute reply with packets tagged with No Label, as shown in the following display:

Device# trace mpls ipv4 10.131.159.252/32
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
Codes: '!p' - success, 'Q' - request not transmitted,
'.J' - timeout, 'U' - unreachable,
'R' - downstream router but not target
Type escape sequence to abort.
  0 10.131.191.230 MRU 1500 [Labels: 20 Exp: 0]
R 1 10.131.159.226 MRU 1500 [Labels: 19 Exp: 0] 80 ms
R 2 10.131.159.229 MRU 1504 [No Label] 28 ms
! 3 10.131.159.230 40 ms

MPLS LSP Ping and Traceroute Returns a Q

The Q return code always means that the packet could not be transmitted. The problem can be caused by insufficient memory, but it probably results because a label switched path (LSP) could not be found that matches the Forwarding Equivalence Class (FEC), information that was entered on the command line.

The reason that the packet was not forwarded needs to be determined. To do so, look at the Routing Information Base (RIB), the Forwarding Information Base (FIB), the Label Information Base (LIB), and the MPLS Label Forwarding Information Base (LFIB). Lack of an entry for the FEC in any one of these routing/forwarding bases would return a Q.

The table below lists commands that you can use for troubleshooting when the MPLS echo reply returns a Q.

<table>
<thead>
<tr>
<th>Database</th>
<th>Command to View Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Information Base</td>
<td>show ip route</td>
</tr>
<tr>
<td>Label Information Base and MPLS FIB</td>
<td>show mpls forwarding-table detail</td>
</tr>
</tbody>
</table>

The following example shows a ping mpls command where the MPLS echo request is not transmitted, as shown by the returned Qs:

Device# ping mpls ipv4 10.0.0.1/32
Sending 5, 100-byte MPLS Echos to 10.0.0.1/32, timeout is 2 seconds, send interval is 0 msec:
Codes: '!P' - success, 'Q' - request not transmitted,
'.J' - timeout, 'U' - unreachable,
'R' - downstream router but not target
Type escape sequence to abort.
QQQQQ
Success rate is 0 percent (0/5)

A show mpls forwarding-table command and a show ip route command demonstrate that the address is not in either routing table:

Device# show mpls forwarding-table 10.0.0.1
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
Device# show ip route 10.0.0.1
% Subnet not in table
The MPLS echo request is not transmitted because the IPv4 address (10.0.0.1) is not found in either the LFIB or the RIB routing table.

Load Balancing for IPv4 LDP LSPs

An Internet Control Message Protocol (ICMP) ping or trace follows one path from the originating device to the target device. Round robin load balancing of IP packets from a source device is used to discover the various output paths to the target IP address.

For MPLS LSP Ping and Traceroute, Cisco devices use the source and destination addresses in the IP header for load balancing when multiple paths exist through the network to a target device. The Cisco implementation of MPLS might check the destination address of an IP payload to accomplish load balancing (this checking depends on the platform).

To check for load balancing paths, you use the 127.z.y.x /8 destination address in the ping mpls ipvr ip-address address-mask destination address-start address-end address-increment command. The following examples show that different paths are followed to the same destination. This demonstrates that load balancing occurs between the originating device and the target device.

To ensure that the Fast Ethernet interface 1/0/0 on the PE1 device is operational, you enter the following commands on the PE1 device:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface fastethernet 1/0/0
Device(config-if)# no shutdown
Device(config-if)# end

*Dec 31 19:14:10.034: %LINK-3-UPDOWN: Interface FastEthernet1/0/0, changed state to up
*Dec 31 19:14:11.054: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/0, changed state to up
PE1#

*Dec 31 19:14:12.574: %SYS-5-CONFIG_I: Configured from console by console
*Dec 31 19:14:19.334: %OSPF-5-ADJCHG: Process 1, Nbr 10.131.159.252 on FastEthernet1/0/0 from LOADING to FULL, Loading Done
PE1#
```

The following `show mpls forwarding-table` command displays the possible outgoing interfaces and next hops for the prefix 10.131.159.251/32:

```
Device# show mpls forwarding-table 10.131.159.251

Local Outgoing Prefix Bytes tag Outgoing Next Hop
  tag  tag or VC  Prefix  Bytes  tag or Tunnel Id switched interface
1 19  10.131.159.251/32  0  FE0/0/0 10.131.191.229
20 10.131.159.251/32  0  FE1/0/0 10.131.159.245
```

The following `ping mpls` command to 10.131.159.251/32 with a destination UDP address of 127.0.0.1 shows that the path selected has a path index of 0:

```
Device# ping mpls ipv4
10.131.159.251/32 destination 127.0.0.1 repeat 1
Sending 1, 100-byte MPLS Echos to 10.131.159.251/32, timeout is 2 seconds, send interval is 0 msec:
Codes: '!' - success, 'Q' - request not transmitted,
'.' - timeout, 'U' - unreachable,
'R' - downstream router but not target
Type escape sequence to abort.
```
Success rate is 100 percent (1/1), round-trip min/avg/max = 40/40/40 ms

*Dec 29 20:42:40.638: LSPV: Echo Request sent on IPV4 LSP, load_index 2, pathindex 0, size 100
*Dec 29 20:42:40.638: 46 00 00 64 00 00 40 00 FF 11 9D 03 0A 83 BF FC
*Dec 29 20:42:40.638: 7F 00 00 01 94 04 00 00 0D AF 0D AF 0F 04 C 14 70
*Dec 29 20:42:40.638: 00 01 00 00 01 02 00 00 1A 00 00 0C 00 00 00 01
*Dec 29 20:42:40.638: C3 9B 10 40 A3 6C 08 D4 00 00 00 00 00 00 00 00
*Dec 29 20:42:40.638: 00 01 00 09 00 01 00 00 05 OA 83 9F FB 20 00 03 00
*Dec 29 20:42:40.638: 13 01 AB CD AB CD AB CD AB CD AB CD AB CD AB CD
*Dec 29 20:42:40.638: AB CD AB CD
*Dec 29 20:42:40.678: LSPV: Echo packet received: src 10.131.159.225, dst 10.131.191.252, size 74
*Dec 29 20:42:40.678: AA BB CC 00 98 01 AA BB CC 00 FC 01 08 00 45 C0
*Dec 29 20:42:40.678: 00 3C 32 D6 00 00 FD 11 15 37 0A 83 9F E1 0A 83
*Dec 29 20:42:40.678: BF FC 0D AF 0D AF 00 28 D1 85 00 01 00 00 02 02
*Dec 29 20:42:40.678: 01 00 1A 00 00 01 00 00 01 C3 9B 10 40 A3 6C
*Dec 29 20:42:40.678: 00 01 00 09 00 01 00 05 0A 83 9F FC 20 00 03 00
*Dec 29 20:42:40.678: 10 5D 84 B3 9D 01 AB CD AB CD AB CD AB CD AB CD
*Dec 29 20:42:40.678: 00 01 00 00 08 D4 C3 9B 10 40 66 EF C3 C8

The following ping mpls command to 10.131.159.251/32 with a destination UDP address of 127.0.0.1 shows that the path selected has a path index of 1:

```
Device# ping mpls ipv4 10.131.159.251/32 dest 127.0.0.1 repeat 1
Sending 1, 100-byte MPLS Echos to 10.131.159.251/32,
timeout is 2 seconds, send interval is 0 msec:
Codes: '!': success, 'Q': request not transmitted,
'.': timeout, 'U': unreachable,
'R': downstream router but not target
Type escape sequence to abort.
!Success rate is 100 percent (1/1), round-trip min/avg/max = 40/40/40 ms
```

To see the actual path chosen, you use the debug mpls lspv packet data command.

---

**Note**

The hashing algorithm is nondeterministic. Therefore, the selection of the *address-start*, *address-end*, and *address-increment* arguments for the *destination* keyword might not provide the expected results.