MPLS TE - Tunnel-Based Admission Control

The MPLS TE--Tunnel-Based Admission Control (TBAC) feature enables classic Resource Reservation Protocol (RSVP) unicast reservations that are traveling across a Multiprotocol Label Switching traffic engineering (MPLS TE) core to be aggregated over an MPLS TE tunnel.

- Finding Feature Information, page 1
- Prerequisites for MPLS TE - Tunnel-Based Admission Control, page 1
- Restrictions for MPLS TE - Tunnel-Based Admission Control, page 2
- Information About MPLS TE - Tunnel-Based Admission Control, page 2
- How to Configure MPLS TE - Tunnel-Based Admission Control, page 4
- Configuration Examples for MPLS TE - Tunnel-Based Admission Control, page 9
- Additional References, page 14
- Feature Information for MPLS TE - Tunnel-Based Admission Control, page 16
- Glossary, page 16

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MPLS TE - Tunnel-Based Admission Control

- You must configure an MPLS TE tunnel in the network.
- You must configure RSVP on one or more interfaces on at least two neighboring routers that share a link within the network.
Restrictions for MPLS TE - Tunnel-Based Admission Control

- Only IPv4 unicast RSVP flows are supported.
- Primary, one-hop tunnels are not supported. The TE tunnel cannot be a member of a class-based tunnel selection (CBTS) bundle.
- Multitopology Routing (MTR) is not supported.
- Only preestablished aggregates are supported. They can be configured statically or dynamically using command-line interface (CLI) commands.

Information About MPLS TE - Tunnel-Based Admission Control

Feature Overview of MPLS TE - Tunnel-Based Admission Control

TBAC aggregates reservations from multiple, classic RSVP sessions over different forms of tunneling technologies that include MPLS TE tunnels, which act as aggregate reservations in the core. The figure below gives an overview of TBAC.

Figure 1: TBAC Overview

The figure below shows three RSVP end-to-end (E2E) flows that originate at routers on the far left, and terminate on routers at the far right. These flows are classic RSVP unicast flows, meaning that RSVP is maintaining a state for each flow. There is nothing special about these flows, except that along their path, these flows encounter an MPLS-TE core, where there is a desire to avoid creating a per-flow RSVP state.

When the E2E flows reach the edge of the MPLS-TE core, they are aggregated onto a TE tunnel. This means that when transiting through the MPLS-TE core, their state is represented by a single state; the TE tunnel is within the aggregation region, and their packets are forwarded (label-switched) by the TE tunnel. For example,
if 100 E2E flows traverse the same aggregator and deaggregator, rather than creating 100 RSVP states (PATH and RESV messages) within the aggregation region, a single RSVP-TE state is created, that of the aggregate, which is the TE tunnel, to allocate and maintain the resources used by the 100 E2E flows. In particular, the bandwidth consumed by E2E flows within the core is allocated and maintained in aggregate by the TE tunnel. The bandwidth of each E2E flow is normally admitted into the TE tunnel at the headend, just as any E2E flow’s bandwidth is admitted onto an outbound link in the absence of aggregation.

**Benefits of MPLS TE - Tunnel-Based Admission Control**

To understand the benefits of TBAC, you should be familiar with how Call Admission Control (CAC) works for RSVP and Quality of Service (QoS).

**Cost Effective**

Real-time traffic is very sensitive to loss and delay. CAC avoids QoS degradation for real-time traffic because CAC ensures that the accepted load always matches the current network capacity. As a result, you do not have to overprovision the network to compensate for absolute worst peak traffic or for reduced capacity in case of failure.

**Improved Accuracy**

CAC uses RSVP signaling, which follows the same path as the real-time flow, and routers make a CAC decision at every hop. This ensures that the CAC decision is very accurate and dynamically adjusts to the current conditions such as a reroute or an additional link. Also, RSVP provides an explicit CAC response (admitted or rejected) to the application, so that the application can react appropriately and fast; for example, sending a busy signal for a voice call, rerouting the voice call on an alternate VoIP route, or displaying a message for video on demand.

**RSVP and MPLS TE Combined**

TBAC allows you to combine the benefits of RSVP with those of MPLS TE. Specifically, you can use MPLS TE inside the network to ensure that the transported traffic can take advantage of Fast Reroute protection (50-millisecond restoration), Constraint Based Routing (CBR), and aggregate bandwidth reservation.

**Seamless Deployment**

TBAC allows you to deploy IPv4 RSVP without any impact on the MPLS part of the network because IPv4 RSVP is effectively tunneled inside MPLS TE tunnels that operate unchanged as per regular RSVP TE. No upgrade or additional protocol is needed in the MPLS core.

**Enhanced Scaling Capability**

TBAC aggregates multiple IPv4 RSVP reservations ingressing from the same MPLS TE headend router into a single MPLS TE tunnel and egressing from the same MPLS TE tailend router.
How to Configure MPLS TE - Tunnel-Based Admission Control

Enabling RSVP QoS

Perform this task to enable RSVP QoS globally on a device.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip rsvp qos
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>ip rsvp qos</td>
<td>Enables RSVP QoS globally on a device.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# ip rsvp qos</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Command or Action</strong></td>
</tr>
<tr>
<td>end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Device(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Enabling MPLS TE

Perform this task to enable MPLS TE. This task enables MPLS TE globally on a router that is running RSVP QoS.
SUMMARY STEPS

1. enable
2. configure terminal
3. mpls traffic-eng tunnels
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>mpls traffic-eng tunnels</td>
<td>Enables MPLS TE globally on a router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# mpls traffic-eng tunnels</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

Configuring an MPLS TE Tunnel Interface

Before You Begin

You must configure an MPLS-TE tunnel in your network before you can proceed. For detailed information, see the "MPLS Traffic Engineering (TE)--Automatic Bandwidth Adjustment for TE Tunnels" module.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel number
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
  Example:  
  Router> enable |
| Step 2 | configure terminal | Enters global configuration mode.  
  Example:  
  Router# configure terminal |
| Step 3 | interface tunnel number  
  Example:  
  Router(config)# interface tunnel 1 | Specifies a tunnel interface and enters interface configuration mode. |
| Step 4 | end  
  Example:  
  Router(config-if)# end | (Optional) Returns to privileged EXEC mode. |

Configuring RSVP Bandwidth on an MPLS TE Tunnel Interface

Perform this task to configure RSVP bandwidth on the MPLS TE tunnel interface that you are using for the aggregation.
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel *number*
4. ip rsvp bandwidth [*interface-kbps*] [*single-flow-kbps*]
5. end

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface tunnel <em>number</em></td>
<td>Specifies a tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface tunnel 1</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>ip rsvp bandwidth [<em>interface-kbps</em>] [<em>single-flow-kbps</em>]</td>
<td>Enables RSVP bandwidth on an interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# ip rsvp bandwidth 7500</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You must enter a value for the <em>interface-kbps</em> argument on a tunnel interface.</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>end</td>
<td>(Optional) Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# end</td>
<td></td>
</tr>
</tbody>
</table>
Verifying the TBAC Configuration

Note: You can use the following `show` commands in user EXEC or privileged EXEC mode, in any order.

### SUMMARY STEPS

1. `enable`
2. `show ip rsvp`
3. `show ip rsvp reservation [detail] [filter [destination {ip-address | hostname}] [dst-port port-number] [source {ip-address | hostname}] [src-port port-number]]`
4. `show ip rsvp sender [detail] [filter [destination ip-address | hostname] [dst-port port-number] [source ip-address | hostname] [src-port port-number]]`
5. `show mpls traffic-eng link-management bandwidth-allocation [summary] [interface-type interface-number]`
6. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | (Optional) Enables privileged EXEC mode.  
- Enter your password if prompted.  
**Note** Omit this step if you are using the `show` commands in user EXEC mode. |
| `enable` |  
**Example:**  
Router> enable |
| **Step 2** | Displays specific information for RSVP categories. |
| `show ip rsvp` |  
**Example:**  
Router# show ip rsvp |
| **Step 3** | Displays RSVP-related receiver information currently in the database. |
| `show ip rsvp reservation [detail] [filter [destination {ip-address | hostname}] [dst-port port-number] [source {ip-address | hostname}] [src-port port-number]]` |  
**Example:**  
Router# show ip rsvp reservation detail |
| **Step 4** | Displays RSVP PATH-related sender information currently in the database. |
| `show ip rsvp sender [detail] [filter [destination ip-address | hostname] [dst-port port-number] [source ip-address | hostname] [src-port port-number]]` |
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
</tr>
</thead>
</table>
| Displays current local link information. | **Example:**
Router# show ip rsvp sender detail |
| Displays current local link information. | **Step 5** show mpls traffic-eng link-management bandwidth-allocation [summary] [interface-type interface-number]
**Example:**
Router# show mpls traffic-eng link-management bandwidth-allocation |
| (Optional) Exits privileged EXEC mode and returns to user EXEC mode. | **Step 6** exit
**Example:**
Router# exit |

### Configuration Examples for MPLS TE - Tunnel-Based Admission Control

#### Example Configuring TBAC

You must have an MPLS TE tunnel already configured in your network. For detailed information, see the "MPLS Traffic Engineering (TE)--Automatic Bandwidth Adjustment for TE Tunnels" module.

The following example enables RSVP and MPLS TE globally on a router and then configures a tunnel interface and bandwidth of 7500 kbps on the tunnel interface traversed by the RSVP flows:

```bash
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip rsvp qos
Router(config)# mpls traffic-eng tunnels
Router(config)# interface tunnel 1
Router(config-if)# ip rsvp bandwidth 7500
Router(config-if)# end
```
Example Configuring RSVP Local Policy on a Tunnel Interface

The following example configures an RSVP default local policy on a tunnel interface:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# interface tunnel 1
Router(config-if)# ip rsvp policy local default
Router(config-rsvp-local-if-policy)# max bandwidth single 10
Router(config-rsvp-local-if-policy)# forward all
Router(config-rsvp-local-if-policy)# end
```

Example Verifying the TBAC Configuration

The figure below shows a network in which TBAC is configured.

Figure 2: Sample TBAC Network

```
<table>
<thead>
<tr>
<th>IP address</th>
<th>IP address</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>10.0.0.2</td>
<td>10.0.0.3</td>
</tr>
</tbody>
</table>

IPv4 RSVP sender
TE tunnel (headend)
TE tunnel (tailend)
IPv4 RSVP Receiver
```

The following example verifies that RSVP and MPLS TE are enabled and coexist on the headend router (10.0.0.2 in the figure above):

```
Router# show ip rsvp
RSVP: enabled (on 3 interface(s))
  RSVP QoS enabled <-------
  MPLS/TE signalling enabled <------
  Signalling:
    Refresh interval (msec): 30000
    Refresh misses: 4
```

The following example verifies that RSVP and MPLS TE are enabled and coexist on the tailend router (10.0.0.3 in the figure above):

```
Router# show ip rsvp
RSVP: enabled (on 3 interface(s))
  RSVP QoS enabled <------
  MPLS/TE signalling enabled <------
  Signalling:
    Refresh interval (msec): 30000
    Refresh misses: 4
```
The following examples verify that an IPv4 flow is traveling through a TE tunnel (a label-switched path [LSP]) on the headend router (10.0.0.2 in the figure above):

Router# `show ip rsvp sender`
To From Pro DPort Sport Prev Hop I/F BPS
10.0.0.3 10.0.0.1 UDP 2 2 10.0.0.1 Et0/0 10K <-- IPv4 flow
10.0.0.3 10.0.0.2 0 1 11 none none 100K <-- TE tunnel

Router# `show ip rsvp reservation`
To From Pro DPort Sport Next Hop I/F Fi Serv BPS
10.0.0.3 10.0.0.1 UDP 2 2 10.0.0.3 Tu1 SE RATE 10K <-- IPv4 flow
10.0.0.3 10.0.0.2 0 1 11 10.1.0.2 Et1/0 SE LOAD 100K <-- TE tunnel

The following examples verify that an IPv4 flow is traveling through a TE tunnel (LSP) on the tailend router (10.0.0.3 in the figure above):

Router# `show ip rsvp sender`
To From Pro DPort Sport Prev Hop I/F BPS
10.0.0.3 10.0.0.1 UDP 2 2 10.0.0.2 Et1/0 10K <-- IPv4 flow
10.0.0.3 10.0.0.2 0 1 11 10.1.0.1 Et1/0 100K <-- TE tunnel

Router# `show ip rsvp reservation`
To From Pro DPort Sport Next Hop I/F Fi Serv BPS
10.0.0.3 10.0.0.1 UDP 2 2 none none SE RATE 10K <-- IPv4 flow
10.0.0.3 10.0.0.2 0 1 11 none none SE LOAD 100K <-- TE tunnel

The following examples display detailed information about the IPv4 flow and the TE tunnel (LSP) on the headend router (10.0.0.2 in the figure above):

Router# `show ip rsvp sender detail`
PATH: <----------------------------------------------- IPv4 flow information begins here.
Destination 10.0.0.3, Protocol_Id 17, Don't Police, DstPort 2
Sender address: 10.0.0.1, port: 2
Path refreshes:
  arriving: from PHOP 10.0.0.10 on Et0/0 every 30000 msecs. Timeout in 189 sec
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
Path ID handle: 02000412.
Incoming policy: Accepted. Policy source(s): Default
Status:
Output on Tunnel1, out of band. Policy status: Forwarding. Handle: 0800040E <---- TE tunnel verified
Policy source(s): Default
Path FLR: Never repaired
PATH: <----------------------------------------------- TE tunnel information begins here.
  Tun Dest: 10.0.0.3 Tun ID: 1 Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2 LSP ID: 11
Path refreshes:
  sent: to NHOP 10.1.0.2 on GigabitEthernet1/0/0

Router# `show ip rsvp reservation detail`
RSVP Reservation. Destination is 10.0.0.3, Source is 10.0.0.1,<--- IPv4 flow information begins here.
  Protocol is UDP, Destination port is 2, Source port is 2
  Next Hop: 10.0.0.3 on Tunnel1, out of band <----------------------- TE tunnel verified
  Reservation Style is Shared-Explicit, QoS Service is Guaranteed-Rate
  ... Reservation: <----------------------------- TE Tunnel information begins here.
  Tun Dest: 10.0.0.3 Tun ID: 1 Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2 LSP ID: 11
  Next Hop: 10.1.0.2 on GigabitEthernet1/0/0
  Label: 0 (outgoing)
Reservation Style is Shared-Explicit, QoS Service is Controlled-Load

Router# show ip rsvp installed detail

RSVP: GigabitEthernet0/0/0 has no installed reservations

RSVP: GigabitEthernet1/0/0 has the following installed reservations
RSVP Reservation. Destination is 10.0.0.3. Source is 10.0.0.2,
  Protocol is 0 , Destination port is 1, Source port is 11
  Traffic Control ID handle: 03000405
  Created: 04:46:55 EST Fri Oct 26 2007 <------ IPv4 flow information
  Admitted flowspec:
    Reserved bandwidth: 100K bits/sec, Maximum burst: 1K bytes, Peak rate: 100K bits/sec
    Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
  Resource provider for this flow: None

RSVP: Tunnel1 has the following installed reservations <------ TE tunnel verified
RSVP Reservation. Destination is 10.0.0.3. Source is 10.0.0.1,
  Protocol is UDP, Destination port is 2, Source port is 2
  Traffic Control ID handle: 01000415
  Created: 04:57:07 EST Fri Oct 26 2007 <------ IPv4 flow information
  Admitted flowspec:
    Reserved bandwidth: 10K bits/sec, Maximum burst: 10K bytes, Peak rate: 10K bits/sec
    Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Resource provider for this flow: None

Router# show ip rsvp interface detail

Et0/0:
  RSVP: Enabled
  Interface State: Up
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 3M bits/sec
    Max. allowed (per flow): 3M bits/sec

Et1/0:
  RSVP: Enabled
  Interface State: Up
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 3M bits/sec
    Max. allowed (per flow): 3M bits/sec

Tu1: <-------------------------- TE tunnel information begins here.
  RSVP: Enabled
  RSVP aggregation over MPLS TE: Enabled
  Interface State: Up
  Bandwidth:
    Curr allocated: 20K bits/sec
    Max. allowed (total): 3M bits/sec
    Max. allowed (per flow): 3M bits/sec

Example Verifying the TBAC Configuration
The following examples display detailed information about the IPv4 flow and the TE tunnel (LSP) on the tailend router (10.0.0.3 in the figure above):

Router# show ip rsvp sender detail
PATH: <----------------------------------------------- IPv4 flow information begins here.
  Destination 10.0.0.3, Protocol_Id 17, Don't Police , DatPort 2
  Sender address: 10.0.0.1, port: 2
  Path refreshes:
    arriving: from PHOP 10.0.0.2 on Et1/0 every 30000 msecs, out of band. Timeout in 188 sec
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes

PATH: <------------------------------------------------ TE tunnel information begins here.
  Tun Dest: 10.0.0.3 Tun ID: 1 Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2 LSP ID: 11
  Path refreshes:
    arriving: from PHOP 10.1.0.1 on Et1/0 every 30000 msecs. Timeout in 202 sec

Router# show ip rsvp reservation detail
RSVP Reservation. Destination is 10.0.0.3, Source is 10.0.0.1, <--- IPv4 flow information begins here.
  Protocol is UDP, Destination port is 2, Source port is 2
  Next Hop: none
  Reservation Style is Shared-Explicit, QoS Service is Guaranteed-Rate

Reservation: <--------------------------------------- TE tunnel information begins here.
  Tun Dest: 10.0.0.3 Tun ID: 1 Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2 LSP ID: 11
  Next Hop: none
  Label: 1 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load

Router# show ip rsvp request detail
RSVP Reservation. Destination is 10.0.0.3, Source is 10.0.0.1,
  Protocol is UDP, Destination port is 2, Source port is 2
  Prev Hop: 10.0.0.2 on GigabitEthernet1/0/0, out of band <---------- TE tunnel verified

 Reservation Style is Shared-Explicit, QoS Service is Guaranteed-Rate
 Average Bitrate is 10K bits/sec, Maximum Burst is 10K bytes

Request: <------------------------------------ TE tunnel information begins here.
  Tun Dest: 10.0.0.3 Tun ID: 1 Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2 LSP ID: 11
  Prev Hop: 10.1.0.1 on GigabitEthernet1/0/0
  Label: 0 (incoming)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
Example Verifying the RSVP Local Policy Configuration

The following example verifies that a default local policy has been configured on tunnel interface 1:

```
Device# show run interface tunnnel 1
Building configuration...

Current configuration : 419 bytes
!
interface Tunnel1
 bandwidth 3000
 ip unnumbered Loopback0
 tunnel destination 10.0.0.3
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autordute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng fast-reroute
 ip rsvp policy local default ----------------- Local policy information begins here.
  max bandwidth single 10
  forward all
 ip rsvp bandwidth 3000
end
```

The following example provides additional information about the default local policy configured on tunnel interface 1:

```
Device# show ip rsvp policy local detail
Tunnel1:
 Default policy:
  Preemption Scope: Unrestricted.
  Local Override: Disabled.
  Fast ReRoute: Accept.
  Handle: BC000413.

<table>
<thead>
<tr>
<th>Path:</th>
<th>Accept</th>
<th>Forward</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resv:</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PathError:</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ResvError:</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Setup Priority</th>
<th>Hold Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>TE: N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Non-TE: N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senders: 0</td>
</tr>
<tr>
<td>Receivers: 1</td>
</tr>
<tr>
<td>Conversations: 1</td>
</tr>
<tr>
<td>Group bandwidth (bps): 10K</td>
</tr>
<tr>
<td>Per-flow b/w (bps): N/A</td>
</tr>
</tbody>
</table>

Generic policy settings:
  Default policy: Accept all
  Preemption: Disabled
```

Additional References

The following sections provide references related to the RSVP--VRF Lite Admission Control feature.
### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples</td>
<td><em>Cisco IOS Quality of Service Solutions Command Reference</em></td>
</tr>
<tr>
<td>VRF-related internet draft</td>
<td><em>Support for RSVP in Layer 3 VPNs, Internet draft, November 19, 2007 [draft-davie-tsvwg-rsvp-l3vpn-01.txt]</em></td>
</tr>
<tr>
<td>Cisco IOS commands</td>
<td><em>Cisco IOS Master Commands List, All Releases</em></td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for MPLS TE - Tunnel-Based Admission Control

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for MPLS TE--Tunnel-Based Admission Control (TBAC)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS TE Tunnel-Based Admission Control</td>
<td>Cisco IOS XE Release 2.6</td>
<td>The MPLS TE--Tunnel-Based Admission Control feature enables classic Resource Reservation Protocol (RSVP) unicast reservations that are traveling across an MPLS TE core to be aggregated over an MPLS TE tunnel. The following commands were introduced or modified: ip rsvp qos, show ip rsvp, show ip rsvp reservation, show ip rsvp sender, show mpls traffic-eng link-management bandwidth-allocation.</td>
</tr>
</tbody>
</table>

Glossary

admission control --The process by which an RSVP reservation is accepted or rejected on the basis of end-to-end available network resources.
**QoS** -- quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability. Quality of service focuses on achieving appropriate network performance for networked applications; it is superior to best effort performance.

**RSVP** -- Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications that run on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams that they want to receive.

**VRF** -- virtual routing and forwarding. An extension of IP routing that provides multiple routing instances. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) device.