Contents

Configuring RSVP

Overview

The Resource Reservation Protocol (RSVP) is a signaling protocol that reserves resources on a network. Extended RSVP supports MPLS label distribution and allows resource reservation information to be transmitted with label bindings. This extended RSVP is called RSVP-TE. RSVP-TE is a label distribution protocol for MPLS TE. It distributes MPLS labels and reserves resources on the nodes of a specific path to establish a CRLSP.

RSVP messages

RSVP uses the following types of messages:

- **Path messages**—Sent by the sender downstream along the data transmission path to save path state information on each node along the path.
- **Resv messages**—Sent by the receiver upstream towards the sender to request resource reservation and to create and maintain reservation state on each node along the reverse data transmission path.
- **PathTear messages**—Sent downstream by the sender or a transit node to remove the path state and related reservation state on each node along the path.
- **ResvTear messages**—Sent upstream by the receiver or a transit node to remove the reservation state on each node along the path.
- **PathErr messages**—Sent upstream by the receiver or a transit node to report Path message processing errors to the sender. They do not affect the state of the nodes along the path.
- **ResvErr messages**—Sent downstream by the sender or a transit node to notify the downstream nodes of an Resv message processing error or of a reservation error caused by preemption.
- **ResvConf messages**—Sent to the receiver to confirm Resv messages.
- **Hello messages**—Sent between any two directly connected RSVP neighbors to set up and maintain the neighbor relationship. Hello messages are sent only when the RSVP hello extension has been enabled.

RSVP-TE extends RSVP by adding new objects to Path and Resv messages. In addition to label bindings, these objects also carry routing constraints to support CRLSP and FRR.

New objects added to the Path message:

- **LABEL_REQUEST**—Requests the downstream node to allocate a label.
- **EXPLICIT_ROUTE**—Carries the path information calculated by the ingress node, making sure the CRLSP is set up along that path.
- **RECORD_ROUTE**—Records the path that the CRLSP actually traverses and the label allocated by each node on the path.
- **SESSION_ATTRIBUTE**—Carries the MPLS TE tunnel attributes, such as the setup priority, holding priority, and affinity.

New objects added to the Resv message:

- **LABEL**—Advertises the label allocated by the downstream node to the upstream node.
- **RECORD_ROUTE**—Records the path that the CRLSP actually traverses and the label allocated by each node on the path.

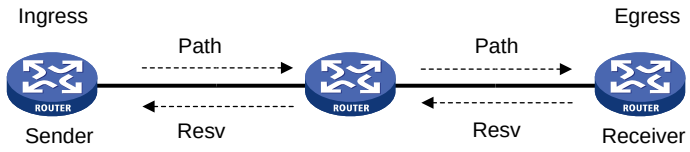
CRLSP setup procedure

As shown in Figure 1, a CRLSP is set up by using the following steps:

1. The ingress LSR generates a Path message that carries LABEL_REQUEST, and then forwards the message along the path calculated by CSPF hop-by-hop towards the egress LSR.
2. After receiving the Path message, the egress LSR generates a Resv message carrying the reservation information and the LABEL object. It forwards the Resv message to the ingress LSR along the reverse direction of the path that the Path message traveled.

   The Resv message advertises labels, reserves resources, and creates a reserve state on each LSR it passes, so QoS can be guaranteed for services transmitted on the CRLSP.
3. When the ingress LSR receives the Resv message, the CRLSP is established.

Figure 1 Setting up a CRLSP



RSVP refresh mechanism

Refresh messages

RSVP maintains resource reservation states on a node by periodically sending messages.

The resource reservation states include path states and reservation states. A path state is saved in a path state block (PSB), and a reservation state is saved in a reservation state block (RSB). A PSB is created by a Path message and saves the LABEL_REQUEST object. A RSB is created by a Resv message and saves the LABEL object.

The path states and reservation states are refreshed periodically by Path and Resv messages. A state is removed if no refresh messages for the state are received in a certain interval, and the CRLSP established based on this state is also removed.

The Path and Resv messages for refreshing the resource reservation states are collectively referred to as refresh messages. Refresh messages can also be used to recover from lost RSVP messages.

When multiple RSVP sessions exist on a network, a short refresh interval can cause network degradation, but a long refresh interval cannot meet the requirements of delay sensitive applications. To find an appropriate balance, you can use the summary refresh (Srefresh) and the reliable RSVP message delivery features.

Srefresh

Srefresh is implemented by adding a Message_ID object to a Path or Resv message to uniquely identify the message. To refresh Path and Resv states, RSVP does not need to send standard Path and Resv messages. Instead, it sends an Srefresh message carrying a set of Message_ID objects that identify the Path and Resv states to be refreshed. The Srefresh feature reduces the number of refresh messages on the network and speeds up refresh message processing.

Reliable RSVP message delivery

An RSVP sender cannot know or retransmit lost RSVP messages. The reliable RSVP message delivery mechanism is designed to ensure reliable transmission.

This mechanism requires the peer device to acknowledge each RSVP message received from the local device. If no acknowledgment is received, the local device retransmits the message.

To implement reliable RSVP message delivery, a node sends an RSVP message that includes a Message_ID object in which the ACK_Desired flag is set. The receiver needs to confirm the delivery

by sending back a message that includes the Message_ID_ACK object. If the sender does not receive a Message_ID_ACK within the retransmission interval (Rf), it performs the following tasks:

- Retransmits the message when Rf expires.
- Sets the next transmission interval to (1 + delta) × Rf.

The sender repeats this process until it receives the Message_ID_ACK before the retransmission time expires or it has transmitted the message three times.

RSVP authentication

RSVP authentication ensures integrity of RSVP messages, and prevents false resource reservation requests from occupying network resources.

With RSVP authentication, the sender uses the MD5 algorithm and the authentication key to calculate a message digest for an RSVP message, and inserts the digest to the RSVP message. When the receiver receives the message, it performs the same calculation and compares the result with the message digest. If they match, the receiver accepts the message. Otherwise, it drops the message.

By carrying a sequence number in a message, RSVP authentication can also prevent packet replay attacks. The device records the sequence number of a received RSVP message, and determines whether the subsequent messages are valid according to the recorded sequence number. If the sequence number of a subsequent message is within the valid range, the device accepts the message. Otherwise, it drops the message.

RSVP GR

RSVP Graceful Restart (GR) preserves soft state and label forwarding information when the signaling protocol or control plane fails, so that LSRs can still forward packets according to forwarding entries.

RSVP GR defines the following roles:

- **GR restarter**—Router that gracefully restarts due to a manually configured command or a fault. It must be GR-capable.
- **GR helper**—Neighbor of the GR restarter. A GR helper maintains the neighbor relationship with the GR restarter and helps the GR restarter restore its LFIB information. A GR helper must be GR-capable.

The device can act only as a RSVP GR helper.

The RSVP GR feature depends on the extended hello capability of RSVP. A GR-capable device advertises its GR capability and relevant time parameters to its neighbors in RSVP hello packets. If a device and all its neighbors have the RSVP GR capability and have exchanged GR parameters, each of them can function as the GR helper of another device.

A GR helper considers that a GR restarter is rebooting when the number of consecutive lost hellos or erroneous hellos reaches the value configured by the **hello lost** command. When a GR restarter is rebooting, the GR helpers perform the following operations:

- Retain soft state information about the GR restarter.
- Continue sending hello packets periodically to the GR restarter until the restart timer expires.

If a GR helper receives a hello message from the GR restarter before the restart timer expires, the recovery timer is started and signaling packet exchange is triggered to restore the original soft state. Otherwise, all RSVP soft state information and forwarding entries relevant to the neighbor are removed. When the recovery timer expires, soft state information and forwarding entries that are not restored are removed.

Protocols and standards

- RFC 2205, *Resource ReSerVation Protocol*
- RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*
- RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

Configuration restrictions and guidelines

To configure RSVP, you must set the VXLAN hardware resource mode to Layer 2 gateway mode. In Layer 2 gateway mode, MPLS shares hardware resources with VXLAN. In any other mode than Layer 2 gateway mode, MPLS features are not available because no hardware resources can be used for MPLS. For more information about VXLAN hardware resource modes, see *VXLAN Configuration Guide*.

RSVP configuration task list

Tasks at a glance
(Required.) Enabling RSVP
(Optional.) Perform the following tasks on each node of an MPLS TE tunnel according to your network requirements: • Configuring RSVP refresh • Configuring RSVP Srefresh and reliable RSVP message delivery • Configuring RSVP hello extension • Configuring RSVP authentication • Setting a DSCP value for outgoing RSVP packets • Configuring RSVP GR • Enabling BFD for RSVP

Enabling RSVP

Step	**Command**	**Remarks**
1. Enter system view.	**system-view**	N/A
2. Enable global RSVP and enter RSVP view.	**rsvp**	By default, global RSVP is disabled.
3. Return to system view.	**quit**	N/A
4. Enter interface view.	**interface** *interface-type interface-number*	N/A
5. Enable RSVP on the interface.	**rsvp enable**	By default, RSVP is disabled on the interface.

Configuring RSVP refresh

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RSVP view.	**rsvp**	N/A
3. Set the refresh interval for Path and Resv messages.	**refresh interval** *interval*	By default, the refresh interval is 30 seconds for both path and Resv messages.
4. Set the PSB and RSB timeout multiplier.	**keep-multiplier** *number*	By default, the PSB and RSB timeout multiplier is 3.

Configuring RSVP Srefresh and reliable RSVP message delivery

After Srefresh is enabled, RSVP maintains the path and reservation states by sending Srefresh messages rather than standard refresh messages.

To configure Srefresh and reliable RSVP message delivery:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable Srefresh and reliable RSVP message delivery.	**rsvp reduction srefresh** [**reliability**]	By default, Srefresh and reliable RSVP message delivery are disabled.
4. Set the retransmission increment value for reliable RSVP message delivery.	**rsvp reduction retransmit increment** *increment-value*	By default, the RSVP message retransmission increment is 1. This command takes effect after reliable RSVP message delivery is enabled by using the **rsvp reduction srefresh reliability** command.
5. Set the retransmission interval for reliable RSVP message delivery.	**rsvp reduction retransmit interval** *interval*	By default, the RSVP message retransmission interval is 500 milliseconds. This command takes effect after reliable RSVP message delivery is enabled by using the **rsvp reduction srefresh reliability** command.

Configuring RSVP hello extension

When RSVP hello extension is enabled on an interface, the device receives and sends hello messages through the interface to detect the neighbor's status.

If the device receives a hello request from the neighbor, the device replies with a hello ACK message. If the device receives no hello request from the neighbor within the interval specified by the **hello interval** command, the device sends hello requests to the neighbor.

When the number of consecutive lost hellos or erroneous hellos from the neighbor reaches the maximum (specified by the **hello lost** command), the device determines the neighbor is in fault. If GR is configured, the device acts as a GR helper to help the neighbor to restart. If FRR is configured, the device performs an FRR. For more information about FRR, see "Configuring MPLS TE."

To configure RSVP hello extension:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RSVP view.	**rsvp**	N/A
3. Set the maximum number of consecutive lost or erroneous hellos.	**hello lost** *times*	By default, the maximum number is 4.
4. Set the interval for sending hello requests.	**hello interval** *interval*	By default, hello requests are sent every 5 seconds.
5. Return to system view.	**quit**	N/A
6. Enter interface view.	**interface** *interface-type interface-number*	N/A
7. Enable RSVP hello extension.	**rsvp hello enable**	By default, RSVP hello extension is disabled.

Configuring RSVP authentication

RSVP adopts hop-by-hop authentication to prevent fake resource reservation requests from occupying network resources. The interfaces at the two ends of a link must use the same authentication key.

RSVP authentication can be configured in the following views:

- **RSVP view**—Configuration applies to all RSVP security associations.
- **RSVP neighbor view**—Configuration applies only to RSVP security associations with the specified RSVP neighbor.
- **Interface view**—Configuration applies only to RSVP security associations established on the current interface.

Configurations in RSVP neighbor view, interface view, and RSVP view are in descending order of priority.

To configure RSVP authentication in RSVP neighbor view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RSVP view.	**rsvp**	N/A
3. Create an RSVP authentication neighbor and enter RSVP neighbor view.	**peer** *ip-address*	By default, no RSVP authentication neighbors exist.
4. Enable RSVP authentication for the RSVP neighbor and specify the authentication	**authentication key** { **cipher** | **plain** } *string*	By default, RSVP authentication is disabled.

Step	Command	Remarks
key.		
5. Enable challenge-response handshake for the RSVP neighbor.	**authentication challenge**	By default, the challenge-response handshake feature is disabled.
6. Set the idle timeout for the RSVP security associations with the RSVP neighbor.	**authentication lifetime** *life-time*	By default, the idle timeout is 1800 seconds (30 minutes).
7. Set the maximum number of out-of-sequence RSVP authentication messages that can be received from the RSVP neighbor.	**authentication window-size** *number*	By default, only one RSVP authenticated message can be received out of sequence.

To configure RSVP authentication in interface view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	N/A
3. Enable RSVP authentication on the interface and configure the authentication key.	**rsvp authentication key** { **cipher** | **plain** } *string*	By default, RSVP authentication is disabled. Do not enable both RSVP authentication and FRR on the same interface.
4. Enable challenge-response handshake on the interface.	**rsvp authentication challenge**	By default, the challenge-response handshake feature is disabled.
5. Set the idle timeout for RSVP security associations on the interface.	**rsvp authentication lifetime** *life-time*	By default, the idle timeout is 1800 seconds (30 minutes).
6. Set the maximum number of out-of-sequence RSVP authentication messages that can be received on the interface.	**rsvp authentication window-size** *number*	By default, only one RSVP authenticated message can be received out of sequence.

To configure RSVP authentication in RSVP view:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RSVP view.	**rsvp**	N/A
3. Enable RSVP authentication globally and configure the authentication key.	**authentication key** { **cipher** | **plain** } *string*	By default, RSVP authentication is disabled.
4. Enable challenge-response handshake globally.	**authentication challenge**	By default, the challenge-response handshake feature is disabled.
5. Set the global idle timeout for RSVP security associations.	**authentication lifetime** *life-time*	By default, the idle timeout is 1800 seconds (30 minutes).
6. Set the global RSVP	**authentication window-size**	By default, only one RSVP

Step	Command	Remarks
authentication window size (the maximum number of RSVP authenticated messages that can be received out of sequence).	*number*	authenticated message can be received out of sequence.

Setting a DSCP value for outgoing RSVP packets

The DSCP value of an IP packet specifies the priority level of the packet and affects the transmission priority of the packet.

To set a DSCP value for outgoing RSVP packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RSVP view.	**rsvp**	N/A
3. Set a DSCP value for outgoing RSVP packets.	**dscp** *dscp-value*	By default, the DSCP value is 48.

Configuring RSVP GR

RSVP GR depends on the RSVP hello extension feature. When configuring RSVP GR, you must enable RSVP hello extension.

Perform this task on GR-capable devices.

To configure RSVP GR:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter RSVP view.	**rsvp**	N/A
3. Enable GR for RSVP.	**graceful-restart enable**	By default, RSVP GR is disabled.
4. Return to system view.	**quit**	N/A
5. Enter interface view.	**interface** *interface-type interface-number*	N/A
6. Enable RSVP hello extension.	**rsvp hello enable**	By default, RSVP hello extension is disabled.

Enabling BFD for RSVP

If a link fails, MPLS TE tunnels over the link fail to forward packets. MPLS TE cannot quickly detect a link failure. To address this issue, you can enable BFD for RSVP so MPLS TE can quickly switch data from the primary path to the backup path upon a link failure.

To enable BFD for RSVP:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter interface view.	**interface** *interface-type interface-number*	You must enable RSVP on the interface.
3. Enable BFD for the RSVP neighbor on the interface.	**rsvp bfd enable**	By default, RSVP BFD is disabled.

Displaying and maintaining RSVP

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display RSVP information.	**display rsvp** [**interface** [*interface-type interface-number*]]
Display information about the security associations established with RSVP neighbors.	**display rsvp authentication** [**from** *ip-address*] [**to** *ip-address*] [**verbose**]
Display information about CRLSPs established through RSVP.	**display rsvp lsp** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**verbose**]
Display information about RSVP neighbors.	**display rsvp peer** [**interface** *interface-type interface-number*] [**ip** *ip-address*] [**verbose**]
Display information about RSVP resource reservation requests sent to upstream devices.	**display rsvp request** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**prevhop** *ip-address*] [**verbose**]
Display information about RSVP resource reservation states.	**display rsvp reservation** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**nexthop** *ip-address*] [**verbose**]
Display information about RSVP path states.	**display rsvp sender** [**destination** *ip-address*] [**source** *ip-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**verbose**]
Display RSVP statistics.	**display rsvp statistics** [**interface** [*interface-type interface-number*]]
Clear RSVP security associations.	**reset rsvp authentication** [**from** *ip-address* **to** *ip-address*]
Clear RSVP statistics.	**reset rsvp statistics** [**interface** [*interface-type interface-number*]

RSVP configuration examples

Establishing an MPLS TE tunnel with RSVP-TE

Network requirements

Switch A, Switch B, Switch C, and Switch D run IS-IS and all of them are Layer 2 switches.

Use RSVP-TE to establish an MPLS TE tunnel from Switch A to Switch D to transmit data between the two IP networks. The MPLS TE tunnel requires a bandwidth of 2000 kbps.

The maximum bandwidth of the link that the tunnel traverses is 10000 kbps and the maximum reservable bandwidth of the link is 5000 kbps.

Figure 2 Network diagram

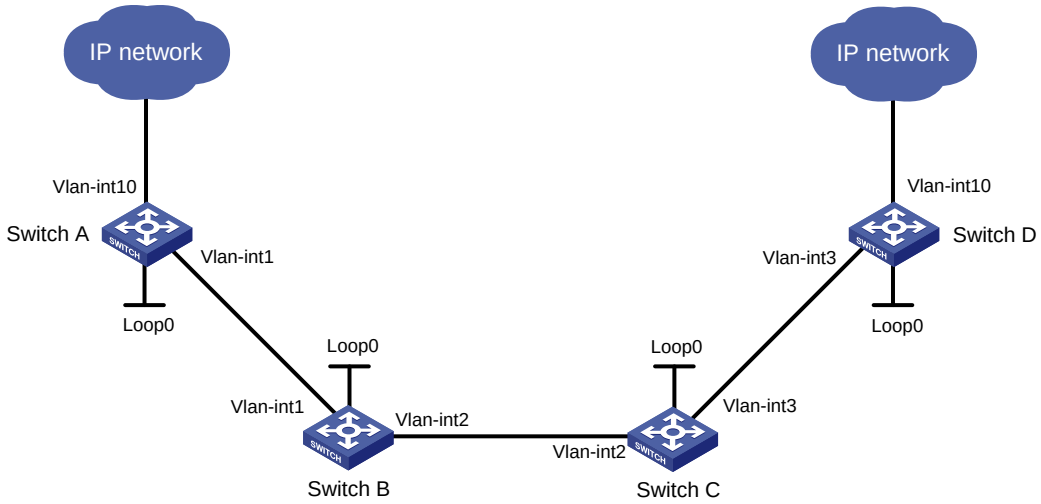


Table 1 Interface and IP address assignment

Device	Interface	IP address	Device	Interface	IP address
Switch A	Loop0	1.1.1.9/32	Switch D	Loop0	4.4.4.9/32
	Vlan-int1	10.1.1.1/24		Vlan-int3	30.1.1.2/24
	Vlan-int10	100.1.1.1/24		Vlan-int10	100.1.2.1/24
Switch B	Loop0	2.2.2.9/32	Switch C	Loop0	3.3.3.9/32
	Vlan-int1	10.1.1.2/24		Vlan-int3	30.1.1.1/24
	Vlan-int2	20.1.1.1/24		Vlan-int2	20.1.1.2/24

Configuration procedure

1. Configure IP addresses and masks for interfaces. (Details not shown.)
2. Configure IS-IS to advertise interface addresses, including the loopback interface address:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] network-entity 00.0005.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] isis enable 1
[SwitchA-Vlan-interface1] isis circuit-level level-2
[SwitchA-Vlan-interface1] quit
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] isis enable 1
[SwitchA-LoopBack0] isis circuit-level level-2
[SwitchA-LoopBack0] quit
```

   # Configure Switch B.

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 00.0005.0000.0000.0002.00
```

```
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] isis enable 1
[SwitchB-Vlan-interface1] isis circuit-level level-2
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] isis enable 1
[SwitchB-Vlan-interface2] isis circuit-level level-2
[SwitchB-Vlan-interface2] quit
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] isis enable 1
[SwitchB-LoopBack0] isis circuit-level level-2
[SwitchB-LoopBack0] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 00.0005.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] isis enable 1
[SwitchC-Vlan-interface3] isis circuit-level level-2
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] isis enable 1
[SwitchC-Vlan-interface2] isis circuit-level level-2
[SwitchC-Vlan-interface2] quit
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] isis enable 1
[SwitchC-LoopBack0] isis circuit-level level-2
[SwitchC-LoopBack0] quit
```

Configure Switch D.

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] network-entity 00.0005.0000.0000.0004.00
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 3
[SwitchD-Vlan-interface3] isis enable 1
[SwitchD-Vlan-interface3] isis circuit-level level-2
[SwitchD-Vlan-interface3] quit
[SwitchD] interface loopback 0
[SwitchD-LoopBack0] isis enable 1
[SwitchD-LoopBack0] isis circuit-level level-2
[SwitchD-LoopBack0] quit
```

Execute the **display ip routing-table** command on each switch to verify that the switches have learned the routes to one another, including the routes to the loopback interfaces. (Details not shown.)

3. Configure an LSR ID, and enable MPLS, MPLS TE, and RSVP:

Configure Switch A.

```
[SwitchA] mpls lsr-id 1.1.1.9
[SwitchA] mpls te
[SwitchA-te] quit
[SwitchA] rsvp
[SwitchA-rsvp] quit
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] mpls enable
[SwitchA-Vlan-interface1] mpls te enable
[SwitchA-Vlan-interface1] rsvp enable
[SwitchA-Vlan-interface1] quit
```

Configure Switch B.

```
[SwitchB] mpls lsr-id 2.2.2.9
[SwitchB] mpls te
[SwitchB-te] quit
[SwitchB] rsvp
[SwitchB-rsvp] quit
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] mpls enable
[SwitchB-Vlan-interface1] mpls te enable
[SwitchB-Vlan-interface1] rsvp enable
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] mpls enable
[SwitchB-Vlan-interface2] mpls te enable
[SwitchB-Vlan-interface2] rsvp enable
[SwitchB-Vlan-interface2] quit
```

Configure Switch C.

```
[SwitchC] mpls lsr-id 3.3.3.9
[SwitchC] mpls te
[SwitchC-te] quit
[SwitchC] rsvp
[SwitchC-rsvp] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] mpls enable
[SwitchC-Vlan-interface3] mpls te enable
[SwitchC-Vlan-interface3] rsvp enable
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] mpls enable
[SwitchC-Vlan-interface2] mpls te enable
[SwitchC-Vlan-interface2] rsvp enable
[SwitchC-Vlan-interface2] quit
```

Configure Switch D.

```
[SwitchD] mpls lsr-id 4.4.4.9
[SwitchD] mpls te
[SwitchD-te] quit
[SwitchD] rsvp
[SwitchD-rsvp] quit
```

```
[SwitchD] interface vlan-interface 3
[SwitchD-Vlan-interface3] mpls enable
[SwitchD-Vlan-interface3] mpls te enable
[SwitchD-Vlan-interface3] rsvp enable
[SwitchD-Vlan-interface3] quit
```

4. Configure IS-IS TE:

Configure Switch A.

```
[SwitchA] isis 1
[SwitchA-isis-1] cost-style wide
[SwitchA-isis-1] mpls te enable level-2
[SwitchA-isis-1] quit
```

Configure Switch B.

```
[SwitchB] isis 1
[SwitchB-isis-1] cost-style wide
[SwitchB-isis-1] mpls te enable level-2
[SwitchB-isis-1] quit
```

Configure Switch C.

```
[SwitchC] isis 1
[SwitchC-isis-1] cost-style wide
[SwitchC-isis-1] mpls te enable level-2
[SwitchC-isis-1] quit
```

Configure Switch D.

```
[SwitchD] isis 1
[SwitchD-isis-1] cost-style wide
[SwitchD-isis-1] mpls te enable level-2
[SwitchD-isis-1] quit
```

5. Configure MPLS TE attributes of links:

Set the maximum link bandwidth and maximum reservable bandwidth on Switch A.

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] mpls te max-link-bandwidth 10000
[SwitchA-Vlan-interface1] mpls te max-reservable-bandwidth 5000
[SwitchA-Vlan-interface1] quit
```

Set the maximum link bandwidth and maximum reservable bandwidth on Switch B.

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] mpls te max-link-bandwidth 10000
[SwitchB-Vlan-interface1] mpls te max-reservable-bandwidth 5000
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] mpls te max-link-bandwidth 10000
[SwitchB-Vlan-interface2] mpls te max-reservable-bandwidth 5000
[SwitchB-Vlan-interface2] quit
```

Set the maximum link bandwidth and maximum reservable bandwidth on Switch C.

```
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] mpls te max-link-bandwidth 10000
[SwitchC-Vlan-interface3] mpls te max-reservable-bandwidth 5000
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 2
```

```
[SwitchC-Vlan-interface2] mpls te max-link-bandwidth 10000
[SwitchC-Vlan-interface2] mpls te max-reservable-bandwidth 5000
[SwitchC-Vlan-interface2] quit
```

Set the maximum link bandwidth and maximum reservable bandwidth on Switch D.

```
[SwitchD] interface vlan-interface 3
[SwitchD-Vlan-interface3] mpls te max-link-bandwidth 10000
[SwitchD-Vlan-interface3] mpls te max-reservable-bandwidth 5000
[SwitchD-Vlan-interface3] quit
```

6. Configure an MPLS tunnel on Switch A:

Configure MPLS TE tunnel interface Tunnel 1.

```
[SwitchA] interface tunnel 1 mode mpls-te
[SwitchA-Tunnel1] ip address 7.1.1.1 255.255.255.0
```

Specify the tunnel destination address as the LSR ID of Switch D.

```
[SwitchA-Tunnel1] destination 4.4.4.9
```

Configure MPLS TE to use RSVP-TE to establish the tunnel.

```
[SwitchA-Tunnel1] mpls te signaling rsvp-te
```

Assign 2000 kbps bandwidth to the tunnel.

```
[SwitchA-Tunnel1] mpls te bandwidth 2000
[SwitchA-Tunnel1] quit
```

7. Configure a static route on Switch A to direct the traffic destined for subnet 100.1.2.0/24 to the MPLS TE tunnel 1 for forwarding.

```
[SwitchA] ip route-static 100.1.2.0 24 tunnel 1 preference 1
```

Verifying the configuration

Verify that the tunnel interface is up on Switch A.

```
[SwitchA] display interface tunnel
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64kbps
Maximum transmission unit: 64000
Internet address: 7.1.1.1/24 (primary)
Tunnel source unknown, destination 4.4.4.9
Tunnel TTL 255
Tunnel protocol/transport CR_LSP
Last clearing of counters: Never
    Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate: 6 bytes/sec, 48 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 177 packets, 11428 bytes, 0 drops
```

Display detailed information about the MPLS TE tunnel on Switch A.

```
[SwitchA] display mpls te tunnel-interface
Tunnel Name            : Tunnel 1
Tunnel State            : Up (Main CRLSP up, Shared-resource CRLSP down)
Tunnel Attributes      :
  LSP ID               : 23331           Tunnel ID           : 1
  Admin State          : Normal
```

```
Ingress LSR ID       : 1.1.1.9          Egress LSR ID        : 4.4.4.9
Signaling            : RSVP-TE          Static CRLSP Name    : -
Resv Style           : SE
Tunnel mode          : -
Reverse-LSP name     : -
Reverse-LSP LSR ID   : -                Reverse-LSP Tunnel ID: -
Class Type           : CT0              Tunnel Bandwidth     : 2000 kbps
Reserved Bandwidth   : 2000 kbps
Setup Priority       : 7                Holding Priority     : 7
Affinity Attr/Mask   : 0/0
Explicit Path        : -
Backup Explicit Path : -
Metric Type          : TE
Record Route         : Disabled         Record Label         : Disabled
FRR Flag             : Disabled         Backup Bandwidth Flag: Disabled
Backup Bandwidth Type: -                Backup Bandwidth     : -
Route Pinning        : Disabled
Retry Limit          : 10               Retry Interval       : 2 sec
Reoptimization       : Disabled         Reoptimization Freq  : -
Backup Type          : None             Backup LSP ID        : -
Auto Bandwidth       : Disabled         Auto Bandwidth Freq  : -
Min Bandwidth        : -                Max Bandwidth        : -
Collected Bandwidth  : -
```

Execute the **display ip routing-table** command on Switch A to verify that a static route entry with interface Tunnel 1 as the output interface exists. (Details not shown.)

RSVP GR configuration example

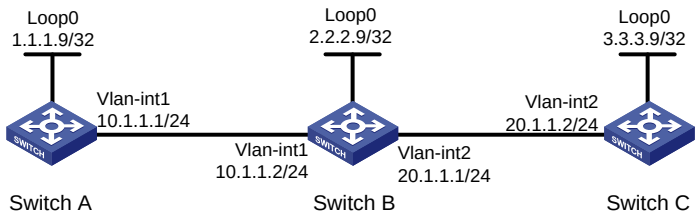
Network requirements

Switch A, Switch B, and Switch C run IS-IS, and all of them are Layer 2 switches.

Use RSVP-TE to establish a TE tunnel from Switch A to Switch C.

Configure RSVP GR on the switches to ensure continuous forwarding when a switch reboots.

Figure 3 Network diagram



Configuration procedure

1. Configure IP addresses and masks for interfaces. (Details not shown.)
2. Configure IS-IS to advertise interface addresses, including the loopback interface address. (Details not shown.)
3. Configure an LSR ID, enable MPLS, MPLS TE, RSVP, and RSVP hello extension:

   # Configure Switch A.

```
<SwitchA> system-view
[SwitchA] mpls lsr-id 1.1.1.9
[SwitchA] mpls te
[SwitchA-te] quit
[SwitchA] rsvp
[SwitchA-rsvp] quit
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] mpls enable
[SwitchA-Vlan-interface1] mpls te enable
[SwitchA-Vlan-interface1] rsvp enable
[SwitchA-Vlan-interface1] rsvp hello enable
[SwitchA-Vlan-interface1] quit
```

Configure Switch B.

```
<SwitchB> system-view
[SwitchB] mpls lsr-id 2.2.2.9
[SwitchB] mpls te
[SwitchB-te] quit
[SwitchB] rsvp
[SwitchB-rsvp] quit
[SwitchB-mpls] interface vlan-interface 1
[SwitchB-Vlan-interface1] mpls enable
[SwitchB-Vlan-interface1] mpls te enable
[SwitchB-Vlan-interface1] rsvp enable
[SwitchB-Vlan-interface1] rsvp hello enable
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] mpls enable
[SwitchB-Vlan-interface2] mpls te enable
[SwitchB-Vlan-interface2] rsvp enable
[SwitchB-Vlan-interface2] rsvp hello enable
[SwitchB-Vlan-interface2] quit
```

Configure Switch C.

```
<SwitchC> system-view
[SwitchC] mpls lsr-id 3.3.3.9
[SwitchC] mpls te
[SwitchC-te] quit
[SwitchC] rsvp
[SwitchC-rsvp] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] mpls enable
[SwitchC-Vlan-interface2] mpls te enable
[SwitchC-Vlan-interface2] rsvp enable
[SwitchC-Vlan-interface2] rsvp hello enable
[SwitchC-Vlan-interface2] quit
```

4. Configure IS-IS TE. (Details not shown.)
5. Configure an MPLS TE tunnel. (Details not shown.)
6. Configure RSVP GR:

   # Configure Switch A.

```
[SwitchA] rsvp
[SwitchA-rsvp] graceful-restart enable
```

Configure Switch B.

```
[SwitchB] rsvp
[SwitchB-rsvp] graceful-restart enable
```

Configure Switch C.

```
[SwitchC] rsvp
[SwitchC-rsvp] graceful-restart enable
```

Verifying the configuration

After a tunnel is established from Switch A and Switch C, display detailed RSVP neighbor information on Switch A.

```
<SwitchA> display rsvp peer verbose
Peer: 10.1.1.2                          Interface: Vlan1
Hello state: Up                         Hello type: Active
P2P PSB count: 0                        P2P RSB count: 1
P2MP PSB count: 0                       P2MP RSB count: 0
Src instance: 0x1f08                    Dst instance: 0x22
Summary refresh: Disabled               Graceful Restart state: Ready
Peer GR restart time: 120000 ms         Peer GR recovery time: 0 ms
```

The output shows that the neighbor's GR state is **Ready**.