MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

First Published: January 16, 2003
Last Updated: December 19, 2006

The MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection feature provides link protection (backup tunnels that bypass only a single link of the label-switched path (LSP)), node protection (backup tunnels that bypass next-hop nodes along LSPs), and the following FRR features:

- Backup tunnel support
- Backup bandwidth protection
- Resource Reservation Protocol (RSVP) Hellos

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection" section on page 107.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

Cisco Systems

Corporate Headquarters
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

Your network must support the following Cisco IOS features:

- IP Cisco Express Forwarding
- Multiprotocol Label Switching (MPLS)

Your network must support at least one of the following protocols:

- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

Before configuring FRR link and node protection, it is assumed that you have done the following tasks but you do not have to already have configured MPLS TE tunnels:

- Enabled MPLS TE on all relevant routers and interfaces
- Configured MPLS TE tunnels

Restrictions for MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

- Interfaces must use MPLS Global Label Allocation.
- Backup tunnel headend and tailend routers must implement FRR as described in draft-pan-rsvp-fastreroute-00.txt.
- Backup tunnels are not protected. If an LSP is actively using a backup tunnel and the backup tunnel fails, the LSP is torn down.
- LSPs that are actively using backup tunnels are not considered for promotion. If an LSP is actively using a backup tunnel and a better backup tunnel becomes available, the active LSP is not switched to the better backup tunnel.
- You cannot enable FRR Hellos on a router that also has Resource Reservation Protocol (RSVP) Graceful Restart enabled.

- (Applicable only to Release 12.2.) You cannot enable primary one-hop autotunnels, backup autotunnels, or autotunnel mesh groups on a router that is also configured with stateful switchover (SSO) redundancy. This restriction does not prevent an MPLS TE tunnel that is automatically configured by TE autotunnel from being successfully recovered of any midpoint router along the LSP's path of the router experiences an SSO switchover.
- MPLS TE LSPs that are fast reroutable cannot be successfully recovered if the LSPs are FRR active and the Point of Local Repair (PLR) router experiences an SSO.

Information About MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

To configure MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection, you need to understand the following concepts:

- Fast Reroute, page 3
- Link Protection, page 3
- Node Protection, page 4
- Bandwidth Protection, page 5
- RSVP Hello, page 5
- Features of MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection, page 6
- Fast Reroute Operation, page 8

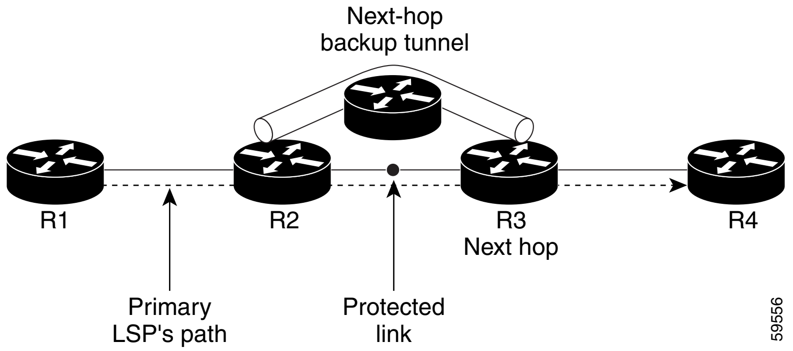
Fast Reroute

Fast Reroute (FRR) is a mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or node.

Link Protection

Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure. Figure 1 illustrates an NHOP backup tunnel.

Figure 1 NHOP Backup Tunnel

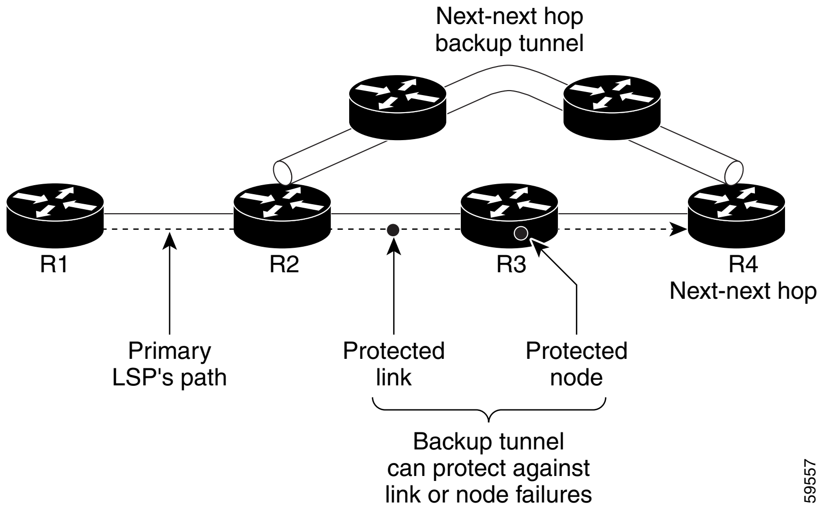


Node Protection

FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link and the node.

Figure 2 illustrates an NNHOP backup tunnel.

Figure 2 NNHOP Backup Tunnel



If an LSP is using a backup tunnel and something changes so that the LSP is no longer appropriate for the backup tunnel, the LSP is torn down. Such changes are the following:

- Backup bandwidth of the backup tunnel is reduced.
- Backup bandwidth type of backup tunnel is changed to a type that is incompatible with the primary LSP.

- Primary LSP is modified so that FRR is disabled. (The **no mpls traffic-eng fast-reroute** command is entered.)

Bandwidth Protection

NHOP and NNHOP backup tunnels can be used to provide bandwidth protection for rerouted LSPs. This is referred to as backup bandwidth. You can associate backup bandwidth with NHOP or NNHOP backup tunnels. This informs the router of the amount of backup bandwidth a particular backup tunnel can protect. When a router maps LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given backup tunnel only if there is sufficient backup bandwidth. The router selects which LSPs use which backup tunnels in order to provide maximum bandwidth protection. That is, the router determines the best way to map LSPs onto backup tunnels in order to maximize the number of LSPs that can be protected. For information about mapping tunnels and assigning backup bandwidth, see the "Backup Tunnel Selection Procedure" section on page 10.

LSPs that have the "bandwidth protection desired" bit set have a higher right to select backup tunnels that provide bandwidth protection; that is, those LSPs can preempt other LSPs that do not have that bit set. For more information, see the "Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection" section on page 8.

RSVP Hello

RSVP Hello Operation

RSVP Hello enables RSVP nodes to detect when a neighboring node is not reachable. This provides node-to-node failure detection. When such a failure is detected, it is handled in a similar manner as a link-layer communication failure.

RSVP Hello can be used by FRR when notification of link-layer failures is not available (for example, with Ethernet), or when the failure detection mechanisms provided by the link layer are not sufficient for the timely detection of node failures.

A node running Hello sends a Hello Request to a neighboring node every interval. If the receiving node is running Hello, it responds with Hello Ack. If four intervals pass and the sending node has not received an Ack or it receives a bad message, the sending node declares that the neighbor is down and notifies FRR.

There are two configurable parameters:

- Hello interval—Use the **ip rsvp signalling hello refresh interval** command.
- Number of acknowledgment messages that are missed before the sending node declares that the neighbor is down—Use the **ip rsvp signalling hello refresh misses** command

Hello Instance

A Hello instance implements RSVP Hello for a given router interface address and remote IP address. A large number of Hello requests are sent; this puts a strain on the router resources. Therefore, create a Hello instance only when it is necessary and delete it when it is no longer needed.

There are two types of Hello instances:

- Active Hello Instances

- Passive Hello Instances

Active Hello Instances

If a neighbor is unreachable when an LSP is ready to be fast rerouted, an active Hello instance is needed. Create an active Hello instance for each neighbor with at least one LSP in this state.

Active Hello instances periodically send Hello Request messages, and expect Hello Ack messages in response. If the expected Ack message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (lost). LSPs traversing that neighbor may be fast rerouted.

If there is a Hello instance with no LSPs for an unreachable neighbor, do not delete the Hello instance. Convert the active Hello instance to a passive Hello instance because there may be an active instance on the neighboring router that is sending Hello requests to this instance.

Passive Hello Instances

Passive Hello instances respond to Hello Request messages (sending Ack messages), but do not initiate Hello Request messages and do not cause LSPs to be fast rerouted. A router with multiple interfaces can run multiple Hello instances to different neighbors or to the same neighbor.

A passive Hello instance is created when a Hello Request is received from a neighbor with a source IP address/destination IP address pair in the IP header for which a Hello instance does not exist.

Delete passive instances if no Hello messages are received for this instance within 10 minutes.

Features of MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection has the following features:

- Backup Tunnel Support, page 6
- Backup Bandwidth Protection, page 7
- RSVP Hello, page 8

Backup Tunnel Support

Backup tunnel support has the following capabilities:

- Backup Tunnels Can Terminate at the Next-Next Hop to Support FRR, page 6
- Multiple Backup Tunnels Can Protect the Same Interface, page 7
- Backup Tunnels Provide Scalability, page 7

Backup Tunnels Can Terminate at the Next-Next Hop to Support FRR

Backup tunnels that terminate at the next-next hop protect both the downstream link and node. This provides protection for link and node failures. For more detailed information, see the “Node Protection” section on page 4.

Multiple Backup Tunnels Can Protect the Same Interface

There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. In many topologies, support for node protection requires supporting multiple backup tunnels per protected interface. These backup tunnels can terminate at the same destination or at different destinations. That is, for a given protected interface, you can configure multiple NHOP or NNHOP backup tunnels. This allows redundancy and load balancing.

In addition to being required for node protection, the protection of an interface by multiple backup tunnels provides the following benefits:

- Redundancy—If one backup tunnel is down, other backup tunnels protect LSPs.
- Increased backup capacity—If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels). For a more detailed explanation, see the "Backup Tunnel Selection Procedure" section on page 10.

Examples are shown in the "Backup Tunnels Terminating at Different Destinations" section on page 9 and the "Backup Tunnels Terminating at the Same Destination" section on page 10.

Backup Tunnels Provide Scalability

A backup tunnel can protect multiple LSPs. Furthermore, a backup tunnel can protect multiple interfaces. This is called many-to-one (N:1) protection. Example of N:1 protection: When one backup tunnel protects 5000 LSPs, each router along the backup path maintains one additional tunnel.

One-to-one protection is when a separate backup tunnel must be used for each LSP needing protection. N:1 protection has significant scalability advantages over one-to-one (1:1) protection. Example of 1:1 protection: When 5000 backup tunnels protect 5000 LSPs, each router along the backup path must maintain state for an additional 5000 tunnels.

Backup Bandwidth Protection

Backup bandwidth protection allows you to give LSPs carrying certain kinds of data (such as voice) priority for using backup tunnels. Backup bandwidth protection has the following capabilities:

- Bandwidth Protection on Backup Tunnels, page 7
- Bandwidth Pool Specifications for Backup Tunnels, page 7
- Semidynamic Backup Tunnel Paths, page 8
- Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection, page 8

Bandwidth Protection on Backup Tunnels

Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained.

Bandwidth Pool Specifications for Backup Tunnels

You can restrict the types of LSPs that can use a given backup tunnel. Backup tunnels can be restricted so that only LSPs using subpool bandwidth can use them or only LSPs that use global-pool bandwidth can use them. This allows different backup tunnels to be used for voice and data. Example: The backup tunnel used for voice could provide bandwidth protection, and the backup tunnel used for data could not provide bandwidth protection.

Semidynamic Backup Tunnel Paths

The path of a backup tunnel can be configured to be determined dynamically. This can be done by using the IP explicit address exclusion feature that was added in Release 12.0(14)ST. If you use this feature, semidynamic NHOP backup tunnel paths can be specified simply by excluding the protected link; semidynamic NNHOP backup tunnel paths can be configured simply by excluding the protected node.

Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection

In case there are not enough NHOP or NNHOP backup tunnels or they do not have enough backup bandwidth to protect all LSPs, you can give an LSP priority in obtaining backup tunnels with bandwidth protection. This is especially useful if you want to give LSPs carrying voice a higher priority than those carrying data.

To activate this feature, enter the **tunnel mpls traffic-eng fast-reroute bw-protect** command to set the “bandwidth protection desired” bit. See the “Enabling Fast Reroute on LSPs” section on page 17.

The LSPs do not necessarily *receive* bandwidth protection. They have a higher *chance* of receiving bandwidth protection if they need it.

LSPs that do not have the bandwidth protection bit set can be demoted. Demotion is when one or more LSPs are removed from their assigned backup tunnel to provide backup to an LSP that has its bandwidth protection bit set. Demotion occurs only when there is a scarcity of backup bandwidth.

When an LSP is demoted, it becomes unprotected (that is, it no longer has a backup tunnel). During the next periodic promotion cycle, an attempt is made to find the best possible backup tunnels for all LSPs that do not currently have protection, including the LSP that was demoted. The LSP may get protection at the same level or a lower level, or it may get no protection.

For information about how routers determine which LSPs to demote, see the “Backup Protection Preemption Algorithms” section on page 14.

RSVP Hello

RSVP Hello enables a router to detect when a neighboring node has gone down but its interface to that neighbor is still operational. This feature is useful when next-hop node failure is not detectable by link layer mechanisms, or when notification of link-layer failures is not available (for example, Gigabit Ethernet). This allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

For a more detailed description of RSVP Hello, see the “RSVP Hello” section on page 5.

Fast Reroute Operation

This section describes the following:

- Tunnel Selection Priorities, page 12
- Bandwidth Protection Considerations, page 14

Fast Reroute Activation

Two mechanisms cause routers to switch LSPs onto their backup tunnels:

- Interface down notification
- RSVP Hello neighbor down notification

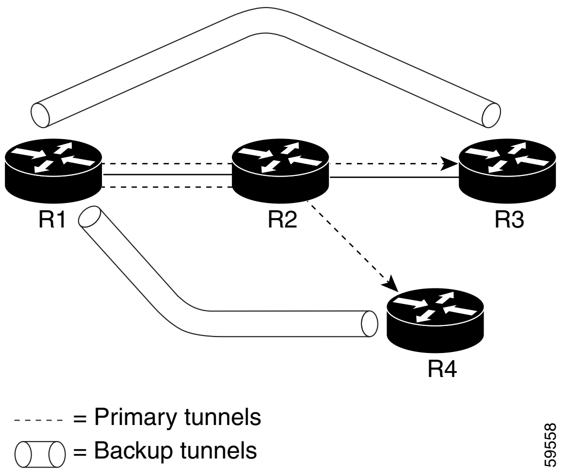
When a router’s link or neighboring node fails, the router often detects this failure by an interface down notification. On a GSR Packet over SONET (PoS) interface, this notification is very fast. When a router notices that an interface has gone down, it switches LPSs going out that interface onto their respective backup tunnels (if any).

RSVP Hellos can also be used to trigger FRR. If RSVP Hellos are configured on an interface, messages are periodically sent to the neighboring router. If no response is received, Hellos declare that the neighbor is down. This causes any LSPs going out that interface to be switched to their respective backup tunnels.

Backup Tunnels Terminating at Different Destinations

Figure 3 illustrates an interface that has multiple backup tunnels terminating at different destinations and demonstrates why, in many topologies, support for node protection requires supporting multiple backup tunnels per protected interface.

Figure 3 Backup Tunnels That Terminate at Different Destinations



In this illustration, a single interface on R1 requires multiple backup tunnels. LSPs traverse the following routes:

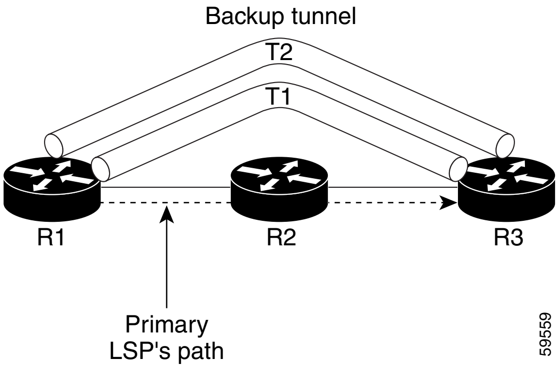
- R1, R2, R3
- R1, R2, R4

To provide protection if node R2 fails, two NNHOP backup tunnels are required: one terminating at R3 and one terminating at R4.

Backup Tunnels Terminating at the Same Destination

Figure 4 shows how backup tunnels terminating at the same location can be used for redundancy and load balancing. Redundancy and load balancing work for both NHOP and NNHOP backup tunnels.

Figure 4 Backup Tunnels That Terminate at the Same Destination



In this illustration, there are three routers: R1, R2, and R3. At R1 two NNHOP backup tunnels (T1 and T2) go from R1 to R3 without traversing R2.

Redundancy—If R2 fails or the link from R1 to R2 fails, either backup tunnel can be used. If one backup tunnel is down, the other can be used. LSPs are assigned to backup tunnels when the LSPs are first established. This is done before a failure.

Load balancing—If neither backup tunnel has enough bandwidth to back up all LSPs, both tunnels can be used. Some LSPs will use one backup tunnel, other LSPs will use the other backup tunnel. The router decides the best way to fit the LSPs onto the backup tunnels.

Backup Tunnel Selection Procedure

When an LSP is signaled, each node along the LSP path that provides FRR protection for the LSP selects a backup tunnel for the LSP to use if either of the following events occurs:

- The link to the next hop fails.
- The next hop fails.

By having the node select the backup tunnel for an LSP before a failure occurs, the LSP can be rerouted onto the backup tunnel quickly if there is a failure.

For an LSP to be mapped to a backup tunnel, all of the following conditions must exist:

- The LSP is protected by FRR; that is, the LSP is configured with the **tunnel mpls traffic-eng fast-reroute** command.
- The backup tunnel is up.
- The backup tunnel is configured to have an IP address, typically a loopback address.
- The backup tunnel is configured to protect this LSP’s outgoing interface; that is, the interface is configured with the **mpls traffic-eng backup-path** command.
- The backup tunnel does not traverse the LSP’s protected interface.
- The backup tunnel terminates at the LSP’s NHOP or NNHOP. If it is an NNHOP tunnel, it does not traverse the LSP’s NHOP.

- The bandwidth protection requirements and constraints, if any, for the LSP and backup tunnel are met. For information about bandwidth protection considerations, see the "Bandwidth Protection" section on page 11.

Bandwidth Protection

A backup tunnel can be configured to protect two types of backup bandwidth:

- Limited backup bandwidth—A backup tunnel provides bandwidth protection. The sum of the bandwidth of all LSPs using this backup tunnel cannot exceed the backup tunnel's backup bandwidth. When you assign LSPs to this type of backup tunnel, sufficient backup bandwidth must exist.
- Unlimited backup bandwidth—The backup tunnel does not provide any bandwidth protection (that is, best-effort protection exists). There is no limit to the amount of bandwidth used by the LSPs that are mapped to this backup tunnel. LSPs that allocate zero bandwidth can use only backup tunnels that have unlimited backup bandwidth.

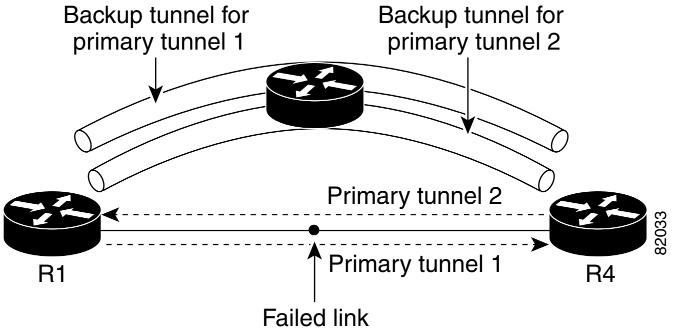
Load Balancing on Limited-Bandwidth Backup Tunnels

There may be more than one backup tunnel that has sufficient backup bandwidth to protect a given LSP. In this case, the router chooses the one that has the least amount of backup bandwidth available. This algorithm limits fragmentation, maintaining the largest amount of backup bandwidth available.

Specifying limited backup bandwidth does not "guarantee" bandwidth protection if there is a link or node failure. For example, the set of NHOP and NNHOP backup tunnels that gets triggered when an interface fails may all share some link on the network topology, and this link may not have sufficient bandwidth to support all LSPs using this set of backup tunnels.

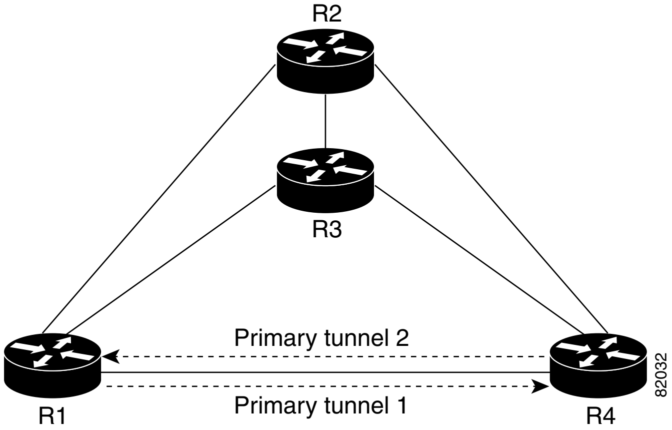
In Figure 5, both backup tunnels traverse the same links and hop. When the link between routers R1 and R4 fails, backup tunnels for primary tunnel 1 and primary tunnel 2 are triggered simultaneously. The two backup tunnels may share a link in the network.

Figure 5 Backup Tunnels Share a Link


Backup tunnel for primary tunnel 1
Backup tunnel for primary tunnel 2
Primary tunnel 2
Primary tunnel 1
R1
R4
Failed link
82033

In Figure 6, the backup tunnel for primary tunnel 1 may traverse routers R1-R2-R3-R4, and the backup tunnel for primary tunnel 2 may traverse routers R4-R2-R3-R1. In this case, the link R2-R3 may get overloaded if R1-R4 fails.

Figure 6 Overloaded Link



Load Balancing on Unlimited-Bandwidth Backup Tunnels

More than one backup tunnel, each having unlimited backup bandwidth, can protect a given interface. In this case, when choosing a backup tunnel for a given LSP, the router chooses the backup tunnel that has the least amount of backup bandwidth in use. This algorithm evenly distributes the LSPs across backup tunnels based on an LSP's bandwidth. If an LSP is requesting zero bandwidth, the router chooses the backup tunnel that is protecting the fewest LSPs.

Pool Type and Backup Tunnels

By default, a backup tunnel provides protection for LSPs that allocate from any pool (that is, global or subpool). However, a backup tunnel can be configured to protect only LSPs that use global-pool bandwidth, or only those that use subpool bandwidth.

Tunnel Selection Priorities

This section describes the following:

- NHOP Versus NNHOP Backup Tunnels, page 12
- Promotion, page 14
- Backup Protection Preemption Algorithms, page 14

NHOP Versus NNHOP Backup Tunnels

More than one backup tunnel can protect a given LSP, where one backup tunnel terminates at the LSP's NNHOP, and the other terminates at the LSP's NHOP. In this case, the router chooses the backup tunnel that terminates at the NNHOP (that is, FRR prefers NNHOP over NHOP backup tunnels).

Table 1 lists the tunnel selection priorities. The first choice is an NNHOP backup tunnel that acquires its bandwidth from a subpool or global pool, and has limited bandwidth. If there is no such backup tunnel, the next choice (2) is a next-next hop backup tunnel that acquires a limited amount of bandwidth from any pool. The preferences go from 1 (best) to 8 (worst), where choice 3 is for an NNHOP backup tunnel with an unlimited amount of subpool or global-pool bandwidth.

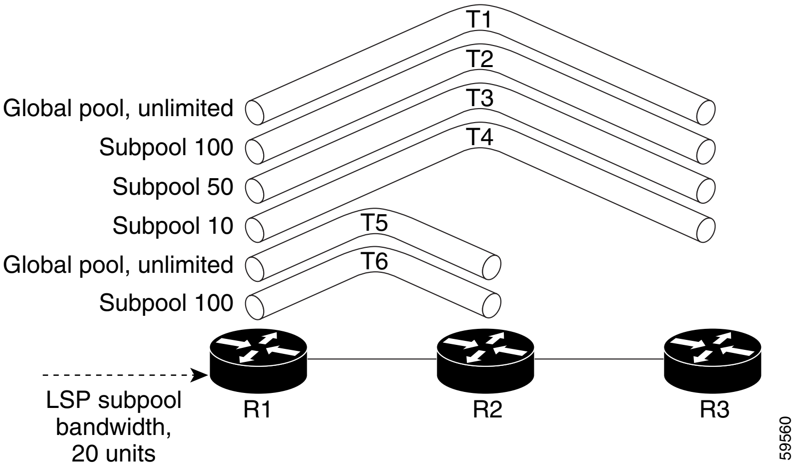
Table 1 Tunnel Selection Priorities

Preference	Backup Tunnel Destination	Bandwidth Pool	Bandwidth Amount
1 (Best)	NNHOP	Subpool or global pool	Limited
2	NNHOP	Any	Limited
3	NNHOP	Subpool or global pool	Unlimited
4	NNHOP	Any	Unlimited
5	NHOP	Subpool or global pool	Limited
6	NHOP	Any	Limited
7	NHOP	Subpool or global pool	Unlimited
8 (Worst)	NHOP	Any	Unlimited

Figure 7 shows an example of the backup tunnel selection procedure based on the designated amount of global pool and subpool bandwidth currently available.

Note If NHOP and NNHOP backup tunnels do not have sufficient backup bandwidth, no consideration is given to the type of data that the LSP is carrying. For example, a voice LSP may not be protected unless it is signaled before a data LSP. To prioritize backup tunnel usage, see the "Backup Protection Preemption Algorithms" section on page 14.

Figure 7 Choosing from Among Multiple Backup Tunnels



In this example, an LSP requires 20 units (kilobits per second) of sub-pool backup bandwidth. The best backup tunnel is selected as follows:

1. Backup tunnels T1 through T4 are considered first because they terminate at the NNHOP.
2. Tunnel T4 is eliminated because it has only ten units of sub-pool backup bandwidth.
3. Tunnel T1 is eliminated because it protects only LSPs using global-pool bandwidth.

4. Tunnel T3 is chosen over T2 because, although both have sufficient backup bandwidth, T3 has the least backup bandwidth available (leaving the most backup bandwidth available on T2).
5. Tunnels T5 and T6 need not be considered because they terminate at an NHOP, and therefore are less desirable than T3, which terminates at an NNHOP.

Promotion

After a backup tunnel has been chosen for an LSP, conditions may change that will cause us to reevaluate this choice. This reevaluation, if successful, is called promotion. Such conditions may include:

1. A new backup tunnel comes up.
2. The currently chosen backup tunnel for this LSP goes down.
3. A backup tunnel's available backup bandwidth increases. For example, an LSP protected by the tunnel has been reoptimized by the headend to use another path.

For cases 1 and 2, the LSP's backup tunnel is evaluated immediately. Case 3 is addressed by periodically reevaluating LSP-to-backup tunnel mappings. By default, background reevaluation is performed every 5 minutes. This interval is configurable via the **mpls traffic-eng fast-reroute timers** command.

Backup Protection Preemption Algorithms

When you set the "bandwidth protection desired" bit for an LSP, the LSP has a higher right to select backup tunnels that provide bandwidth protection and it can preempt other LSPs that do not have that bit set.

If there is insufficient backup bandwidth on NNHOP backup tunnels but not on NHOP backup tunnels, the bandwidth-protected LSP does not preempt NNHOP LSPs; it uses NHOP protection.

If there are multiple LSPs using a given backup tunnel and one or more must be demoted to provide bandwidth, there are two user-configurable methods (algorithms) that the router can use to determine which LSPs are demoted:

- Minimize amount of bandwidth that is wasted.
- Minimize the number of LSPs that are demoted.

For example, If you need ten units of backup bandwidth on a backup tunnel, you can demote one of the following:

- A single LSP using 100 units of bandwidth—Makes available more bandwidth than needed, but results in lots of waste
- Ten LSPs, each using one unit of bandwidth—Results in no wasted bandwidth, but affects more LSPs

The default algorithm is to minimize the number of LSPs that are demoted. To change the algorithm to minimize the amount of bandwidth that is wasted, enter the **mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw** command.

Bandwidth Protection Considerations

There are numerous ways in which bandwidth protection can be ensured. Table 2 describes the advantages and disadvantages of three methods.

Table 2 Bandwidth Protection Methods

Method	Advantages	Disadvantages
Reserve bandwidth for backup tunnels explicitly.	It is simple.	It is a challenge to allow bandwidth sharing of backup tunnels protecting against independent failures.
Use backup tunnels that are signaled with zero bandwidth.	It provides a way to share bandwidth used for protection against independent failures, so it ensures more economical bandwidth usage.	It may be complicated to determine the proper placement of zero bandwidth tunnels.
Backup bandwidth protection.	It ensures bandwidth protection for voice traffic.	An LSP that does not have backup bandwidth protection can be demoted at any time if there is not enough backup bandwidth and an LSP that has backup bandwidth protection needs bandwidth.

Cisco implementation of FRR does not mandate a particular approach, and it provides the flexibility to use any of the above approaches. However, given a range of configuration choices, be sure that the choices are constant with a particular bandwidth protection strategy.

The following sections describe some important issues in choosing an appropriate configuration:

- Using Backup Tunnels with Explicitly Signaled Bandwidth, page 15
- Using Backup Tunnels Signaled with Zero Bandwidth, page 16

Using Backup Tunnels with Explicitly Signaled Bandwidth

Two bandwidth parameters must be set for a backup tunnel:

- Actual signaled bandwidth
- Backup bandwidth

To signal bandwidth requirements of a backup tunnel, configure the bandwidth of the backup tunnel by using the **tunnel mpls traffic-eng bandwidth** command.

To configure the backup bandwidth of the backup tunnel, use the **tunnel mpls traffic-eng backup-bw** command.

The signaled bandwidth is used by the LSRs on the path of the backup tunnel to perform admission control and do appropriate bandwidth accounting.

The backup bandwidth is used by the point of local repair (PLR) (that is, the headend of the backup tunnel) to decide how much primary traffic can be rerouted to this backup tunnel if there is a failure.

Both parameters need to be set to ensure proper operation. The numerical value of the signaled bandwidth and the backup bandwidth should be the same.

Protected Bandwidth Pools and the Bandwidth Pool from Which the Backup Tunnel Reserves Its Bandwidth

The **tunnel mpls traffic-eng bandwidth** command allows you to configure the following:

- Amount of bandwidth a backup tunnel reserves

- The DS-TE bandwidth pool from which the bandwidth needs to be reserved

Note Only one pool can be selected (that is, the backup tunnel can explicitly reserve bandwidth from either the global pool or the subpool, but not both).

The **tunnel mpls traffic-eng backup-bw** command allows you to specify the bandwidth pool to which the traffic must belong for the traffic to use this backup tunnel. Multiple pools are allowed.

There is no direct correspondence between the bandwidth pool that is protected and the bandwidth pool from which the bandwidth of the backup tunnel draws its bandwidth.

Bandwidth protection for 10 Kbps of subpool traffic on a given link can be achieved by configuring any of the following command combinations:

- **tunnel mpls traffic-eng bandwidth sub-pool 10**

  tunnel mpls traffic-eng backup-bw sub-pool 10
- **tunnel mpls traffic-eng bandwidth global-pool 10**

  tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool unlimited
- **tunnel mpls traffic-eng bandwidth global-pool 40**

  tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool 30

Using Backup Tunnels Signaled with Zero Bandwidth

Frequently it is desirable to use backup tunnels with zero signaled bandwidth, even when bandwidth protection is required. It may seem that if no bandwidth is explicitly reserved, no bandwidth guarantees can be provided. However, that is not necessarily true.

In the following situation:

- Only link protection is desired.
- Bandwidth protection is desired only for sub-pool traffic.

For each protected link AB with a maximum reservable subpool value of *n*, there may be a path from node A to node B such that the difference between the maximum reservable global and the maximum reservable subpool is at least the value of *n*. If it is possible to find such paths for each link in the network, you can establish all the backup tunnels along such paths without any bandwidth reservations. If there is a single link failure, only one backup tunnel will use any link on its path. Because that path has at least *n* available bandwidth (in the global pool), assuming that marking and scheduling is configured to classify the subpool traffic into a priority queue, the subpool bandwidth is guaranteed.

This approach allows sharing of the global pool bandwidth between backup tunnels protecting independent link failures. The backup tunnels are expected to be used for only a short period of time after a failure (until the headends of affected LSPs reroute those LSPs to other paths with available subpool bandwidth). The probability of multiple unrelated link failures is very small (in the absence of node or shared risk link group (SRLG) failures, which result in multiple link failures). Therefore, it is reasonable to assume that link failures are in practice independent with high probability. This “independent failure assumption” in combination with backup tunnels signaled without explicit bandwidth reservation enables efficient bandwidth sharing that yields substantial bandwidth savings.

Backup tunnels protecting the subpool traffic do now draw bandwidth from any pool. Primary traffic using the global pool can use the entire global pool, and primary traffic using the subpool can use the entire subpool. Yet, subpool traffic has a complete bandwidth guarantee if there is a single link failure.

A similar approach can be used for node and SRLG protection. However, the decision of where to put the backup tunnels is more complicated because both node and SRLG failures effectively result in the simultaneous failure of several links. Therefore, the backup tunnels protecting traffic traversing all affected links cannot be computed independently of each other. The backup tunnels protecting groups of links corresponding to different failures can still be computed independently of each other, which results in similar bandwidth savings.

Signaled Bandwidth Versus Backup Bandwidth

Backup bandwidth is used locally (by the router that is the headend of the backup tunnel) to determine which, and how many, primary LSPs can be rerouted on a particular backup tunnel. The router ensures that the combined bandwidth requirement of these LSPs does not exceed the backup bandwidth.

Therefore, even when the backup tunnel is signaled with zero bandwidth, the backup bandwidth must be configured with the value corresponding to the actual bandwidth requirement of the traffic protected by this backup tunnel. Unlike the case when bandwidth requirements of the backup tunnels are explicitly signaled, the value of the signaled bandwidth (which is zero) is not the same value as the backup bandwidth.

How to Configure MPLS Traffic Engineering—Fast Reroute (FRR) Link and Node Protection

This section assumes that you want to add FRR protection to a network in which MPLS TE LSPs are configured.

This section contains the following procedures:

- Enabling Fast Reroute on LSPs (required)
- Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop (required)
- Assigning Backup Tunnels to a Protected Interface (required)
- Associating Backup Bandwidth and Pool Type with a Backup Tunnel (optional)
- Configuring Backup Bandwidth Protection (optional)
- Configuring an Interface for Fast Link and Node Failure Detection (optional)
- Verifying That Fast Reroute Is Configured (optional)

Enabling Fast Reroute on LSPs

LSPs can use backup tunnels only if they have been configured as fast reroutable. To do this, enter the following commands at the headend of each LSP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng fast-reroute** [**bw-protect**]

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		- Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface tunnel`** *`number`*
	Example:
	`Router(config)# interface tunnel 1000`
		Enters interface configuration mode for the specified tunnel.

Step 4	**`tunnel mpls traffic-eng fast-reroute`** `[`**`bw-protect`**`]`
	Example:
	`Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect`
		Enables an MPLS TE tunnel to use an established backup tunnel if there is a link or node failure.

Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop

Creating a backup tunnel is basically no different from creating any other tunnel. To create a backup tunnel to the next hop or to the next-next hop, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the "Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images" section on page 1.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *interface-type interface-number*
5. **tunnel destination** *A.B.C.D*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng path-option** [**protect**] *number* {**dynamic** | **explicit** | {**name** *path-name* | *path-number*}} [**lockdown**]
8. **ip explicit-path name** *word*
9. **exclude-address** *address*

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface tunnel`** *`number`*
	Example:
	`Router(config)# interface tunnel 1`
		Creates a new tunnel interface and enters interface configuration mode.

Step 4	**`ip unnumbered`** *`interface-type interface-number`*
	Example:
	`Router(config-if)# ip unnumbered loopback0`
		Gives the tunnel interface an IP address that is the same as that of interface Loopback0.
		Note This command is not effective until Lookback0 has been configured with an IP address.

Step 5	**`tunnel destination`** *`A.B.C.D`*
	Example:
	`Router(config-if)# tunnel destination 10.3.3.3`
		Specifies the IP address of the device where the tunnel will terminate. This address should be the router-id of the device that is the NHOP or NNHOP of LSPs to be protected.

Step 6	**`tunnel mode mpls traffic-eng`**
	Example:
	`Router(config-if)# tunnel mode mpls traffic-eng`
		Sets the encapsulation mode of the tunnel to MPLS TE.

Step 7	**`tunnel mpls traffic-eng path-option`** [**`protect`**] *`number`* {**`dynamic`** | **`explicit`** | {**`name`** *`path-name`* | *`path-number`*}}[**`lockdown`**] **Example:** `Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link`	Configures a path option for an MPLS TE tunnel. Enters router configuration mode.

	Command	Purpose
Step 8	**ip explicit-path name** *word* **Example:** `Router(config-router)# ip explicit-path name avoid-protected-link`	Enters the command mode for IP explicit paths and creates the specified path. Enters explicit path command mode.
Step 9	**exclude-address** *address* **Example:** `Router(config-ip-expl-path)# exclude-address 3.3.3.3`	For link protection, specify the IP address of the link to be protected. For node protection, specify the router-ID of the node to be protected. **Note** Backup tunnel paths can be dynamic or explicit and they do not have to use exclude-address. Because backup tunnels must avoid the protected link or node, it is convenient to use the **exclude-address** command. **Note** When using the **exclude-address** command to specify the path for a backup tunnel, you must exclude an interface address to avoid a link (for creating an NHOP backup tunnel), or a router ID address to avoid a node (for creating an NNHOP backup tunnel).

Assigning Backup Tunnels to a Protected Interface

To assign one or more backup tunnels to a protected interface, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the "Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images" section on page 1.

Note You must configure the interface to have an IP address and to enable the MPLS TE tunnel feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot***/***port*
4. **mpls traffic-eng backup-path tunnel** *interface*

DETAILED STEPS

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. - Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot***/***port* **Example:** `Router(config)# interface POS 5/0`	Moves configuration to the physical interface level, directing subsequent configuration commands to the specific physical interface identified by the *type* value. The *slot* and *port* identify the slot and port being configured. The interface must be a supported interface. See the "Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images" section on page 1. Enters interface configuration mode.
Step 4	**mpls traffic-eng backup-path tunnel** *interface* **Example:** `Router(config-if)# mpls traffic-eng backup-path tunnel 2`	Allows LSPs going out this interface to use this backup tunnel if there is a link or node failure. **Note** You can enter this command multiple times to associate multiple backup tunnels with the same protected interface.

Associating Backup Bandwidth and Pool Type with a Backup Tunnel

To associate backup bandwidth with a backup tunnel and designate the type of LSP that can use a backup tunnel, enter the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng backup-bw** {*bandwidth* | [**sub-pool** {*bandwidth* | **Unlimited**}] [**global-pool** {*bandwidth* | **Unlimited**}]

DETAILED STEPS

	Command	Purpose

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	**`interface tunnel`** *`number`*
	Example:
	`Router(config)# interface tunnel 2`
		Enters interface configuration mode for the specified tunnel.

Step 4	**`tunnel mpls traffic-eng backup-bw`** `{`*`bandwidth`* `|` `[`**`sub-pool`** `{`*`bandwidth`* `|` **`Unlimited`**`}]` `[`**`global-pool`** `{`*`bandwidth`* `|` **`Unlimited`**`}]`
	Example:
	`Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000`
		Associates bandwidth with a backup tunnel and designates whether LSPs that allocate bandwidth from the specified pool can use the tunnel.

Configuring Backup Bandwidth Protection

To configure backup bandwidth protection, enter the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tunnel mpls traffic-eng-fast-reroute** [**bw-protect**]
4. **mpls traffic-eng fast-reroute backup-prot-preemption** [**optimize-bw**]

DETAILED STEPS

Step 1	**`enable`**
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	**`configure terminal`**
	Example:
	`Router# configure terminal`
		Enters interface configuration mode.

Step 3	**tunnel mpls traffic-eng fast-reroute** [**bw-protect**] Example: `Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect`	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure. The **bw-protect** keyword gives an LSP priority for using backup tunnels with bandwidth protection. Enters global configuration mode.
Step 4	**mpls traffic-eng fast-reroute backup-prot-preemption** [**optimize-bw**] **Example:** `Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw`	Changes the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.

Configuring an Interface for Fast Link and Node Failure Detection

To configure an interface for fast link and node failure detection, enter the following commands.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **pos ais-shut**
5. **pos report** {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}

DETAILED STEPS

Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type slot/port* **Example:** `Router(config)# interface pos0/0`	Configures an interface type and enters interface configuration mode.

Step 4	**pos ais-shut** **Example:** `Router(config-if)# pos ais-shut`	Sends the line alarm indication signal (LAIS) when the POS interface is placed in any administrative shutdown state.

Step 5	**pos report** {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}
	Example:
	`Router(config-if)# pos report lrdi`
		Permits selected SONET alarms to be logged to the console for a POS interface.

Verifying That Fast Reroute Is Configured

To verify that FRR can function, perform the following steps.

SUMMARY STEPS

Note To determine if FRR has been configured correctly, perform Steps 1 and 2.

Note If you created LSPs and performed the required configuration tasks but do not have operational backup tunnels (that is, the backup tunnels are not up or the LSPs are not associated with those backup tunnels), perform Step 3.

1. **show mpls traffic-eng tunnels brief**
2. **show ip rsvp sender detail**
3. **show mpls traffic-eng fast-reroute database**
4. **show mpls traffic-eng tunnels backup**
5. **show mpls traffic-eng fast-reroute database**
6. **show ip rsvp reservation**

DETAILED STEPS

Step 1 **show mpls traffic-eng tunnels brief**

Use this command to verify that backup tunnels are up:

```
Router# show mpls traffic-eng tunnels brief
```

Following is sample output from the **show mpls traffic-eng tunnels brief** command:

```
Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         PO4/0/1   up/up
```

```
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Step 2 **show ip rsvp sender detail**

Use this command to verify that LSPs are protected by the appropriate backup tunnels.

Following is sample output from the **show ip rsvp sender detail** command when the command is entered at the PLR before a failure.

```
Router# show ip rsvp sender detail

PATH:
 Tun Dest:   10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
 Tun Sender: 10.10.0.1  LSP ID: 31
 Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
 Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
 ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
 RRO:
   10.10.7.1/32, Flags:0x0 (No Local Protection)
   10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
   10.10.1.1/32, Flags:0x0 (No Local Protection)
 Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
 Fast-Reroute Backup info:
   Inbound  FRR: Not active
   Outbound FRR: No backup tunnel selected
 Path ID handle: 50000416.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxy-terminated
```

Step 3 **show mpls traffic-eng fast-reroute database**

Enter the **clear ip rsvp hello instance counters** command to verify the following:

- MPLS TE FRR node protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

```
Router# show mpls traffic-eng fast-reroute database

Tunnel head end item frr information:
Protected Tunnel      In-label   intf/label       FRR intf/label     Status
Tunne110              Tun        pos5/0:Untagged  Tu0:12304          ready

Prefix item frr information:
Prefix        Tunnel  In-label   Out intf/label   FRR intf/label     Status
10.0.0.11/32  Tu110   Tun hd     pos5/0:Untagged  Tu0:12304          ready

LSP midpoint frr information:
LSP identifier        In-label   Out intf/label   FRR intf/label     Status
10.0.0.12 1 [459]     16         pos0/1:17        Tu2000:19          ready
```

If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the **show mpls forwarding-table** *ip-address* **detail** command. The final line of the display will tell whether that prefix is protected:

```
Router# show mpls forwarding-table 10.0.0.11 detail

Local    Outgoing    Prefix         Bytes tag    Outgoing     Next Hop
tag      tag or VC   or Tunnel Id   switched     interface
Tun hd   Untagged    10.0.0.11/32   48           pos5/0       point2point
          MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
          48D18847 00016000
          No output feature configured
          Fast Reroute Protection via (Tu0, outgoing label 12304)
```

Step 4 **show mpls traffic-eng tunnels backup**

For backup tunnels to be operational, the LSP must be reroutable. At the headend of the LSP, enter the **show run int tunnel** *tunnel-number* command. The output should include the **tunnel mpls traffic-eng fast-reroute** command. If it does not, enter this command for the tunnel.

On the router where the backup tunnels originate, enter the **show mpls traffic-eng tunnels backup** command. Following is sample command output:

```
Router# show mpls traffic-eng tunnels backup

Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin up, Oper: up
  Src 10.55.55.55,, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

The command output will allow you to verify the following:

- Backup tunnel exists—Verify that there is a backup tunnel that terminates at this LSP's NHOP or NNHOP. Look for the LSP's NHOP or NNHOP in the Dest field.
- Backup tunnel is up—To verify that the backup tunnel is up, look for "Up" in the State field.
- Backup tunnel is associated with LSP's interface—Verify that the interface for the LSP is allowed to use this backup tunnel. Look for the LSP's output interface in the "protects" field list.
- Backup tunnel has sufficient bandwidth—If you restricted the amount of bandwidth a backup tunnel can hold, verify that the backup tunnel has sufficient bandwidth to hold the LSPs that would use this backup tunnel if there is a failure. The bandwidth of an LSP is defined by the line **tunnel mpls traffic-eng bandwidth** at the headend of the LSP. To determine the available bandwidth on a backup tunnel, look at the "cfg" and "inuse" fields. If there is insufficient backup bandwidth to

accommodate the LSPs that would use this backup tunnel in the event of a failure, create an additional backup tunnel or increase the backup bandwidth of the existing tunnel by using the **tunnel mpls traffic-eng bandwidth** command.

Note To determine the sufficient amount of bandwidth, offline capacity planning may be required.

- Backup tunnel has appropriate bandwidth type—If you restricted the type of LSPs (subpool or global pool) that can use this backup tunnel, verify that the LSP is the appropriate type for the backup tunnel. The type of the LSP is defined by the line **tunnel mpls traffic-eng bandwidth** at the headend of this LSP. If this line contains the word “subpool”, then it uses sub-pool bandwidth; otherwise, it uses global pool bandwidth. Verify that the type matches the type the backup tunnel can hold by looking in the output of the **tunnel mpls traffic-eng bandwidth** command.

You also can enable debug by entering the **debug ip rsvp fast-reroute** command and the **debug mpls traffic-eng fast-reroute** command on the router that is the headend of the backup tunnel. Then do the following:

1. Enter the **shutdown** command for the primary tunnel.
2. Enter the **no shutdown** command for the primary tunnel.
3. View the debug output.

Step 5 **show mpls traffic-eng fast-reroute database**

Enter the **clear ip rsvp hello instance counters** command to verify the following:

- MPLS TE FRR node protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

```
Router# show mpls traffic-eng fast-reroute database

Tunnel head end item frr information:
Protected Tunnel   In-label   intf/label       FRR intf/label      Status
Tunnel10           Tun        pos5/0:Untagged  Tu0:12304           ready

Prefix item frr information:
Prefix        Tunnel  In-label    Out intf/label   FRR intf/label Status
10.0.0.11/32  Tu110   Tun hd      pos5/0:Untagged  Tu0:12304      ready

LSP midpoint frr information:
LSP identifier       In-label Out intf/label   FRR intf/label   Status
10.0.0.12 1 [459]    16       pos0/1:17        Tu2000:19        ready
```

Note If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the **show mpls forwarding-table** *ip-address* **detail** command. The final line of the display will tell whether that prefix is protected:

```
    Router# show mpls forwarding-table 10.0.0.11 detail

    Local    Outgoing    Prefix         Bytes tag    Outgoing     Next Hop
    tag      tag or VC   or Tunnel Id   switched     interface
    Tun hd   Untagged    10.0.0.11/32   48           pos5/0       point2point
              MAC/Encaps=4/8, MTU=1520, Tag Stack{22}
              48D18847 00016000
              No output feature configured
```

```
                  Fast Reroute Protection via (Tu0, outgoing label 12304)
```

Step 6 **show ip rsvp reservation**

Following is sample output from the **show ip rsvp reservation** command entered at the headend of a primary LSP. Entering the command at the headend of the primary LSP shows, among other things, the status of FRR (that is, local protection) at each hop this LSP traverses. The per-hop information is collected in the Record Route Object (RRO) that travels with the Resv message from the tail to the head.

```
Router# show ip rsvp reservation detail

Reservation:
  Tun Dest: 10.1.1.1  Tun ID: 1  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 104
  Next Hop: 172.17.1.2 on POS1/0
  Label: 18 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  RRO:
    172.18.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 18
    172.19.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
      Label subobject: Flags 0x1, C-Type 1, Label 16
    172.19.1.2/32, Flags:0x0 (No Local Protection)
      Label subobject: Flags 0x1, C-Type 1, Label 0
  Resv ID handle: CD000404.
  Policy: Accepted. Policy source(s): MPLS/TE
```

Notice the following about the primary LSP:

- It has protection that uses a NHOP backup tunnel at its first hop.
- It has protection and is actively using an NHOP backup tunnel at its second hop.
- It has no local protection at its third hop.

The RRO display shows the following information for each hop:

- Whether local protection is available (that is, whether the LSP has selected a backup tunnel)
- Whether local protection is in use (that is, whether the LSP is currently using its selected backup tunnel)
- Whether the selected backup tunnel is an NHOP or NNHOP backup tunnel
- Whether the backup tunnel used at this hop provides bandwidth protection

Troubleshooting Tips

This section describes the following:

- LSPs Do Not Become Active; They Remain Ready
- Primary Tunnel Does Not Select Backup Tunnel That Is Up
- Enhanced RSVP Commands Display Useful Information
- RSVP Hello Detects When a Neighboring Node Is Not Reachable
- Hello Instances Have Not Been Created
- "No entry at index" (error may self-correct, RRO may not yet have propagated from downstream node of interest)" Error Message Is Printed at the Point of Local Repair

- "Couldn't get rsbs" (error may self-correct when Resv arrives)" Error Message Is Printed at the Point of Local Repair

LSPs Do Not Become Active; They Remain Ready

At a PLR, LSPs transition from Ready to Active if one of the following events occurs:

- Primary interface goes down—If the primary interface (LSP's outbound interface) goes down and the LSP is ready to use a backup tunnel, the LSP will transition to the active state causing its data to flow over the backup tunnel. On some platforms and interface types (for example, GSR POS interfaces), there is fast interface-down logic that detects this event very quickly. On other platforms where this logic does not exist, detection time is slower. On such platforms, it may be desirable to enable RSVP Hello (see the next bulleted item, "Hellos detect next hop is down").
- Hellos detect next hop is down—If Hellos are enabled on the primary interface (LSP's outbound interface), and the LSP's next hop is no longer reachable, the next hop is declared down. This event will cause the LSP to begin actively using its backup tunnel. Notice that a next hop will be declared down even if the primary interface does not go down. For example, if the next hop stops responding due to a reboot or software orr hardware problem, Hellos will trigger the LSPs using this next hop to switch to their backup tunnels. Hellos can also help trigger FRR on interfaces such as Gigabit Ethernet where the interface remains up but is unusable (due to lack of link-layer liveness detection mechanisms).

Primary Tunnel Does Not Select Backup Tunnel That Is Up

If a backup tunnel is up, but it is not selected as a backup tunnel by the primary tunnel (LSP), enter the following commands for the backup tunnel:

- **shutdown**
- **no shutdown**

Note If you change the status of a backup tunnel, the backup tunnel selection algorithm is rerun for the backup tunnel. LSPs that have currently selected (that is, are ready to use) that backup tunnel will be disassociated from it, and then reassociated with that backup tunnel or another backup tunnel. This is generally harmless and usually results in mapping the same LSPs to that backup tunnel. However, if any LSPs are actively using that backup tunnel, shutting down the backup tunnel will tear down those LSPs.

Enhanced RSVP Commands Display Useful Information

The following RSVP commands have been enhanced to display information that can be helpful when you are examining the FRR state or troubleshooting FRR:

- **show ip rsvp request**—Displays upstream reservation state (that is, information related to the Resv messages that this node will send upstream).
- **show ip rsvp reservation**—Displays information about Resv messages received.
- **show ip rsvp sender**—Displays information about path messages being received.

These commands show control plane state; they do not show data state. That is, they show information about RSVP messages (Path and Resv) used to signal LSPs. For information about the data packets being forwarded along LSPs, use the **show mpls forwarding** command.

RSVP Hello Detects When a Neighboring Node Is Not Reachable

The RSVP Hello feature enables RSVP nodes to detect when a neighboring node is not reachable. Use this feature when notification of link-layer failures is not available and unnumbered links are not used, or when the failure detection mechanisms provided by the link layer are not sufficient for timely node failure detection. Hello must be configured both globally on the router and on the specific interface to be operational.

Hello Instances Have Not Been Created

If Hello instances have not been created, do the following:

- Determine if RSVP Hello has been enabled globally on the router. Enter the **ip rsvp signalling hello** (configuration) command.
- Determine if RSVP Hello has been enabled on an interface that the LSPs traverse. Enter the **ip rsvp signalling hello** (interface) command.
- Verify that at least one LSP has a backup tunnel by displaying the output of the **show ip rsvp sender** command. A value of “Ready” indicates that a backup tunnel has been selected.

“No entry at index” (error may self-correct, RRO may not yet have propagated from downstream node of interest)” Error Message Is Printed at the Point of Local Repair

FRR relies on a RRO in Resv messages arriving from downstream. Routers receiving path messages with the SESSION_ATTRIBUTE bit indicating that the LSP is fast-reroutable should include an RRO in the corresponding Resv messages.

If an LSP is configured for FRR, but the Resv arriving from a downstream router contains an incomplete RRO, the “No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)” message is printed. An incomplete RRO is one in which the NHOP or the NNHOP did not include an entry in the RRO.

This error typically means that backup tunnels to the NHOP or the NNHOP cannot be selected for this LSP because there is insufficient information about the NHOP or NNHOP due to the lack of an RRO entry.

Occasionally there are valid circumstances in which this situation occurs temporarily and the problem is self-corrected. If subsequent Resv messages arrive with a complete RRO, ignore the error message.

To determine whether the error has been corrected, display the RRO in Resv messages by entering the **clear ip rsvp hello instance counters** command. Use an output filter keyword to display only the LSP of interest.

“Couldn’t get rsbs” (error may self-correct when Resv arrives)” Error Message Is Printed at the Point of Local Repair

The PLR cannot select a backup tunnel for an LSP until a Resv message has arrived from downstream.

When this error occurs, it typically means that something is wrong. For example, no reservation exists for this LSP. You can troubleshoot this problem by using the **debug ip rsvp reservation** command to enable debug.

Occasionally there are valid circumstances in which this error message occurs and there is no need for concern. One such circumstance is when an LSP experiences a change before any Resv message has arrived from downstream. Changes can cause a PLR to try to select a backup tunnel for an LSP, and the selection will fail (causing this error message) if no Resv message has arrived for this LSP.

Configuration Examples for MPLS Traffic Engineering—Fast Reroute (FRR) Link and Node Protection

This section provides the following configuration examples:

- Enabling Fast Reroute for all Tunnels: Example, page 31
- Creating an NHOP Backup Tunnel: Example, page 32
- Creating an NNHOP Backup Tunnel: Example, page 32
- Assigning Backup Tunnels to a Protected Interface: Example, page 32
- Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example, page 33
- Configuring Backup Bandwidth Protection: Example, page 33
- Configuring an Interface for Fast Link and Node Failure Detection: Example, page 33
- Configuring RSVP Hello and POS Signals: Example, page 33

The examples relate to the illustration shown in Figure 8.

Figure 8 Backup Tunnels

Enabling Fast Reroute for all Tunnels: Example

On router R1, enter interface configuration mode for each tunnel to be protected (Tunnel 1000 and Tunnel 2000). Enable these tunnels to use a backup tunnel in case of a link or node failure along their paths.

Tunnel 1000 will use 10 units of bandwidth from the subpool.

Tunnel 2000 will use five units of bandwidth from the global pool. The "bandwidth protection desired" bit has been set by specifying **bw-prot** in the **tunnel mpls traffic-eng fast-reroute** command.

```
Router(config)# interface Tunnel 1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10

Router(config)# interface Tunnel2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-prot
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
```

Creating an NHOP Backup Tunnel: Example

On router R2, create an NHOP backup tunnel to R3. This backup tunnel should avoid using the link 172.1.1.2.

```
Router(config)# ip explicit-path name avoid-protected-link
Router(cfg-ip-expl-path)# exclude-address 172.1.1.2
Explicit Path name avoid-protected-link:
____1: exclude-address 172.1.1.2
Router(cfg-ip_expl-path)# end

Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.3.3.3
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link
```

Creating an NNHOP Backup Tunnel: Example

On router R2, create an NNHOP backup tunnel to R4. This backup tunnel should avoid R3.

```
Router(config)# ip explicit-path name avoid-protected-node
Router(cfg-ip-expl-path)# exclude-address 10.3.3.3
Explicit Path name avoid-protected-node:
____1: exclude-address 10.3.3.3
Router(cfg-ip_expl-path)# end

Router(config)# interface Tunnel 2
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.4.4.4
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-node
```

Assigning Backup Tunnels to a Protected Interface: Example

On router R2, associate both backup tunnels with interface POS 5/0:

```
Router(config)# interface POS 5/0
Router(config-if)# mpls traffic-eng backup-path tunnel 1
Router(config-if)# mpls traffic-eng backup-path tunnel 2
```

Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example

Backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. It does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
Router(config)# interface Tunnel 1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited

Router(config)# interface Tunnel 2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
```

Configuring Backup Bandwidth Protection: Example

In the following example, backup bandwidth protection is configured:

Note This global configuration is required only to change the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

Configuring an Interface for Fast Link and Node Failure Detection: Example

In the following example, pos ais-shut is configured:

```
Router(config)# interface pos 0/0
Router(config-if)# pos ais-shut
```

In the following example, report lrdi is configured on OS interfaces:

```
Router(config)# interface pos 0/0
Router(config-if)# pos report lrdi
```

Configuring RSVP Hello and POS Signals: Example

Hello must be configured both globally on the router and on the specific interface on which you need FRR protection. To configure Hello, use the following configuration commands:

- **ip rsvp signalling hello** (configuration)—Enables Hello globally on the router.
- **ip rsvp signalling hello** (interface)—Enables Hello on an interface where you need FRR protection.

The following configuration commands are optional:

- **ip rsvp signalling hello dscp**—Sets the Differentiated Services Code Point (DSCP) value that is in the IP header of the Hello message.
- **ip rsvp signalling hello refresh misses**—Specifies how many acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
- **ip rsvp signalling hello refresh interval**—Configures the Hello request interval.
- **ip rsvp signalling hello statistics**—Enables Hello statistics on the router.

For configuration examples, see the Hello command descriptions in the "Command Reference" section of *MPLS Traffic Engineering (TE): Link and Node Protection, with RSVP Hellos Support*, Release 12.0(24)S.

To configure POS signaling for detecting FRR failures, enter the **pos report all** command or enter the following commands to request individual reports:

```
pos ais-shut
pos report rdool
pos report lais
pos report lrdi
pos report pais
pos report prdi
pos report sd-ber
```

Additional References

The following sections provide references related to the MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection feature.

Related Documents

Related Topic	Document Title
IS-IS	• *Cisco IOS Network Protocols Command Reference, Part 1*, Release 12.0 • *Cisco IOS Network Protocols Configuration Guide, Part 1*, Release 12.0
Link protection	*MPLS Traffic Engineering Fast ReRoute Link Protection*, Release 12.0(16)ST
Shared risk link groups	• *MPLS Traffic Engineering: Shared Risk Link Groups* (*SRLG*) • *MPLS Traffic Engineering—Inter-AS TE*
FRR protection of TE LSPs from SRLG failure	*MPLS Traffic Engineering: Shared Risk Link Groups* (*SRLG*)
MPLS traffic engineering	• *Cisco IOS Switching Services Command Reference*, Release 12.4 • *Cisco IOS Switching Services Configuration Guide*, Release 12.4
Configuration of MPLS TE tunnels	*Cisco IOS Switching Services Configuration Guide*, Release 12.4
OSPF	• *Cisco IOS IP Routing Protocols Command Reference,* Release 12.4 • *Cisco IOS IP Routing Protocols Command Reference,* Release 12.4
RSVP	• *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4 • *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4

Standards

Standards	Title
draft-ietf-mpls-rsvp-lsp-fastreroute-04.txt	*Fast ReRoute Extensions to RSVP-TE for LSP Tunnels*

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
draft-ietf-mpls-rsvp-lsp-fastreroute-06.txt.	*Fast Reroute Extensions for RSVP-TE for LSP Tunnels*

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents modified commands.

- clear ip rsvp hello instance counters
- clear ip rsvp hello instance statistics
- clear ip rsvp hello statistics
- debug ip rsvp hello
- ip rsvp signalling hello (configuration)
- ip rsvp signalling hello (interface)
- ip rsvp signalling hello dscp
- ip rsvp signalling hello refresh interval
- ip rsvp signalling hello refresh misses

- ip rsvp signalling hello statistics
- mpls traffic-eng backup-path tunnel
- mpls traffic-eng fast-reroute backup-prot-preemption
- mpls traffic-eng fast-reroute timers
- show ip rsvp fast bw-protect
- show ip rsvp fast detail
- show ip rsvp hello
- show ip rsvp hello instance detail
- show ip rsvp hello instance summary
- show ip rsvp hello statistics
- show ip rsvp interface detail
- show ip rsvp request
- show ip rsvp reservation
- show ip rsvp sender
- show mpls traffic tunnel backup
- show mpls traffic-eng fast-reroute database
- show mpls traffic-eng tunnels
- show mpls traffic-eng tunnels summary
- tunnel mpls traffic-eng backup-bw
- tunnel mpls traffic-eng fast-reroute

clear ip rsvp hello instance counters

To clear (refresh) the values for Hello instance counters, use the **clear ip rsvp hello instance counters** command in privileged EXEC mode.

clear ip rsvp hello instance counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

Following is sample output from the **show ip rsvp hello instance detail** command and then the **clear ip rsvp hello instance counters** command. Notice that the “Statistics” fields have been cleared to zero.

```
Router# show ip rsvp hello instance detail

Neighbor 10.0.0.2  Source  10.0.0.1
    State: UP      (for 2d18h)
    Type: PASSIVE  (responding to requests)
    I/F: Et1/1
    LSPs protecting: 0
    Refresh Interval (msec) (used when ACTIVE)
      Configured: 100
      Statistics: (from 2398195 samples)
        Min:      100
        Max:      132
        Average:  100
        Waverage: 100 (Weight = 0.8)
        Current:  100
    Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
    Counters:
      Communication with neighbor lost:
        Num times: 0
        Reasons:
          Missed acks:             0
          Bad Src_Inst received:   0
          Bad Dst_Inst received:   0
          I/F went down:           0
          Neighbor disabled Hello: 0
      Msgs Received:   2398194
           Sent:       2398195
           Suppressed: 0
```

```
Router# clear ip rsvp hello instance counters

Neighbor 10.0.0.2  Source  10.0.0.1
    State: UP      (for 2d18h)
    Type: PASSIVE  (responding to requests)
    I/F: Et1/1
    LSPs protecting: 0
    Refresh Interval (msec) (used when ACTIVE)
      Configured: 100
      Statistics:
        Min:        0
        Max:        0
        Average:    0
        Waverage:   0
        Current:    0
    Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
    Counters:
      Communication with neighbor lost:
        Num times: 0
        Reasons:
          Missed acks:             0
          Bad Src_Inst received:   0
          Bad Dst_Inst received:   0
          I/F went down:           0
          Neighbor disabled Hello: 0
      Msgs Received:   2398194
           Sent:       2398195
           Suppressed: 0
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

clear ip rsvp hello instance statistics

To clear Hello statistics for an instance, use the **clear ip rsvp hello instance statistics** command in privileged EXEC mode.

clear ip rsvp hello instance statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not cleared for an instance.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows sample output from the **show ip rsvp hello statistics** command and the values in those fields after you enter the **clear ip rsvp hello instance statistics** command.

```
Router# show ip rsvp hello statistics

  Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525


Router# clear ip rsvp hello instance statistics

Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:0
    Current length: 0 (max:500)
  Number of samples taken: 0
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

clear ip rsvp hello statistics

To globally clear Hello statistics, use the **clear ip rsvp hello statistics** command in privileged EXEC mode.

clear ip rsvp hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Hello statistics are not globally cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to remove all information about how long Hello packets have been in the Hello input queue.

Examples

Following is sample output from the **show ip rsvp hello statistics** command and the **clear ip rsvp hello statistics** command. Notice that the values in the “Packet arrival queue” fields have been cleared.

```
Router# show ip rsvp hello statistics

  Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525

Router# clear ip rsvp hello statistics

  Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:0
    Current length: 0 (max:500)
  Number of samples taken: 16
```

Related Commands

Command	Description
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

debug ip rsvp hello

To verify that a Hello instance has been created, a Hello instance has been deleted, or that communication with a neighbor has been lost, use the **debug ip rsvp hello** command in privileged EXEC mode.

debug ip rsvp hello [**stats**]

Syntax Description

stats	(Optional) Indicates whether statistics are enabled or disabled.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enter the **debug ip rsvp hello** command, Resource Reservation Protocol (RSVP) signaling messages are shown, but RSVP hello messages are excluded because of the large number of hello messages that are sent.

Examples

Following is sample output from the **debug ip rsvp hello** command. The first portion of the output is for interface Se2/0 when Hello is created:

```
Router# debug ip rsvp hello

00:22:03: RSVP-HELLO: rsvp_hello_inst_init: Initializing ACTIVE hello inst
12.0.0.2->12.0.0.3
00:22:03: RSVP-HELLO: rsvp_hello_create_instance_from_psb: Next hop Se2/0 is adjacent
00:22:03: RSVP-HELLO: rsvp_hello_create_instance_from_psb: Create hello instance for
12.0.0.2->12.0.0.3 on Se2/0 (psb=61BC5F60)
00:22:03: RSVP-HELLO: rsvp_hello_find_instance: psb_cnt=2 for hello inst
12.0.0.2->12.0.0.3
00:22:03: RSVP-HELLO: rsvp_hello_incoming_message: Neighbor 10.0.0.3 state changed to UP
00:22:05: %LINK-3-UPDOWN: Interface Tunnel1, changed state to up
00:22:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
rsvp-3640-2(config-if)#
rsvp-3640-2(config-if)# shut
rsvp-3640-2(config-if)#
```

The following output shows that Hello has been deleted:

```
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: psb for hello inst 10.0.0.2->10.0.0.3 exited
READY state (psb_cnt=1)
```

```
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: psb for hello inst 10.0.0.2->10.0.0.3 exited
READY state (psb_cnt=0)
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: Last psb deleted, hello inst for
12.0.0.2->12.0.0.3 ACTIVE->PASSIVE
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: psb for hello inst 10.0.0.2->10.0.0.3 exited
READY state (psb_cnt=0)
00:25:19: RSVP-HELLO: rsvp_hello_path_delete: Last psb deleted, hello inst for
13.0.0.2->13.0.0.3 ACTIVE->PASSIVE
00:25:21: %LINK-5-CHANGED: Interface Tunnel1, changed state to administratively down
00:25:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1,
changed state to down

00:05:51: RSVP-HELLO: Communication lost with 10.0.0.2
00:05:51: RSVP-HELLO: rsvp_hello_communication_lost: Neighbor 10.0.0.2 was reset
(src_inst)
```

Following is sample output from the **debug ip rsvp hello stats** command:

```
Router(config)# ip rsvp signalling hello stat
Router(config)# end
Router#
00:32:28: RSVP-HELLO: rsvp_hello_stats_init: Hello stats is being configured
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the Hello message sent out from an interface.
ip rsvp signalling hello refresh misses	Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.
ip rsvp signalling hello statisticsc	Enables Hello statistics on the router.

ip rsvp signalling hello (configuration)

To enable Hello globally on the router, use the **ip rsvp signalling hello** command in global configuration mode.

ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

To enable Hello globally on the router, you must enter this command. You also must enable Hello on the interface.

Examples

In the following example, Hello is enabled globally on the router:

```
Router# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

ip rsvp signalling hello (interface)

To enable Hello on an interface where you need Fast Reroute protection, use the **ip rsvp signalling hello** command in interface configuration mode.

ip rsvp signalling hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must configure Hello globally on the router and on the specific interface.

Examples

In the following example, Hello is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello
```

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the Hello messages sent out from the interface.
ip rsvp signalling hello refresh misses	Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.

ip rsvp signalling hello dscp

To set the differentiated services code point (DSCP) value that is in the IP header of the hello message sent out from an interface, use the **ip rsvp signalling hello dscp** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ip rsvp signalling hello dscp [*num*]

no ip rsvp signalling hello dscp

Syntax Description

num	(Optional) DSCP value. Range: 0 to 63. Default: 0.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If a link is congested, it is recommended that you set the DSCP to a value higher than zero (0) to reduce the likelihood that hello messages will be dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to all Resource Reservation Protocol (RSVP) flows installed on a specific interface. You can configure each interface independently for DSCP.

Examples

In the following example, hello messages sent from this interface have a DSCP value of 48:

```
Router(config-if)# ip rsvp signalling hello dscp 48
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.

ip rsvp signalling hello refresh interval

To configure the Hello request interval, use the **ip rsvp signalling hello refresh interval** command in interface configuration mode.

ip rsvp signalling hello refresh interval *milliseconds*

Syntax Description

milliseconds	Frequency, in milliseconds, at which a node sends hello messages to a neighbor. Range: 10 to 30,000. Default: 200.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can configure the Hello request interval on a per-neighbor basis. A node periodically generates a hello message containing a HELLO REQUEST object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the Hello interval.

Examples

In the following example, Hello requests are sent to a neighbor every 50 milliseconds:

```
Router(config-if)# ip rsvp signalling hello refresh interval 50
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello statistics	Displays how long Hello packets have been in the Hello input queue.

ip rsvp signalling hello refresh misses

To specify how many consecutive Hello acknowledgments a node can miss before the node considers its neighbor to be down, use the **ip rsvp signalling hello refresh misses** command in interface configuration mode.

ip rsvp signalling hello refresh misses *num*

Syntax Description

num	The number of sequential Hello acknowledgments that a node can miss. Range: 4 to 10. Default: 4.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Hello comprises a hello message, a HELLO REQUEST object, and a HELLO ACK object. Each request is answered by an acknowledgment. If a link is very congested or has a very heavy load, set the *num* argument to a value higher than the default value to ensure that Hello does not falsely declare that a neighbor is down.

Examples

In the following example, if the node does not receive five consecutive Hello acknowledgments, the node declares that its neighbor is down:

```
Router(config-if)# ip rsvp signalling hello refresh misses 5
```

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Help on an interface.
ip rsvp signalling hello dscp	Sets the DSCP value that is in hello messages sent out from an interface.

ip rsvp signalling hello statistics

To enable Hello statistics on the router, use the **ip rsvp signalling hello statistics** command in privileged EXEC mode.

ip rsvp signalling hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example, Hello statistics are enabled on the router.

```
Router(config)# ip rsvp signalling hello statistics
```

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

mpls traffic-eng backup-path tunnel

To configure the physical interface to use a backup tunnel in the event of a detected failure on that interface, use the **mpls traffic-eng backup-path tunnel** command in interface configuration mode.

mpls traffic-eng backup-path tunnel *interface*

Syntax Description

interface	String that identifies the tunnel interface being created and configured.

Command Default

This command is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(8)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Catalyst 6000 series with the SUP720 processor.
12.2(28)SB	This command was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example specifies the traffic engineering backup tunnel with the identifier 1000:

```
Router(config-if)# mpls traffic-eng backup-path Tunnel1000
```

Related Commands

Command	Description
show mpls traffic-eng fast-reroute database	Displays information about existing Fast Reroute configurations.
tunnel mpls traffic-eng fast-reroute	Enables an MPLS traffic engineering tunnel to use a backup tunnel in the event of a link failure (assuming a backup tunnel exists).

mpls traffic-eng fast-reroute backup-prot-preemption

To change the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted, use the **mpls traffic-eng fast-reroute backup-prot-preemption** command in privileged configuration mode. To use the default algorithm of minimizing the number of label-switched paths (LSPs) that are demoted, use the **no** form of this command.

mpls traffic-eng fast-reroute backup-prot-preemption [**optimize-bw**]

no mpls traffic-eng fast-reroute backup-prot-preemption

Syntax Description

optimize-bw	(Optional) Minimizes the amount of bandwidth wasted.

Command Default

A minimum number of LSPs are preempted.

Command Modes

Privileged configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **mpls traffic-eng fast-reroute backup-prot-preemption** command allows you to determine the criteria the router will use when selecting the LSPs that will be preempted.

If you enter the command with the **optimize-bw** keyword, the router chooses LSPs that will waste the least amount of bandwidth.

If you do not enter the **mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw** command, the router preempts as few LSPs as possible.

Each router in the network does not have to use the same algorithm; that is, you can specify **optimize-bw** for some routers in the network but not for others.

You can enter the **mpls traffic-eng fast-re-route backup-prot-preemption** command at any time. If you change the algorithm, it does not affect LSPs that already are protected. It only affects the placement of new LSPs signaled after you enter this command. The command can affect LSPs during the next periodic promotion cycle.

Examples

In the following examples, a next-next hop (NNHOP) backup tunnel has the following characteristics:

- Total backup capacity: 240 units
- Used backup bandwidth: 220 units
- Available backup bandwidth: 20 units

The backup tunnel currently is protecting LSP1 through LSP5, which have the following bandwidth, and do not have backup bandwidth protection (that is, the “bandwidth protection desired” bit was not set via the **tunnel mpls traffic-eng fast-reroute** command):

- LSP1: 10 units
- LSP2: 20 units
- LSP3: 30 units
- LSP4: 60 units
- LSP5: 100 units

As shown, LSP1 through LSP5 use 220 units of bandwidth.

LSP6 has backup bandwidth protection and needs 95 units of bandwidth. Twenty units of bandwidth are available, so 75 more units of bandwidth are needed.

In the following example, backup bandwidth protection is enabled and the amount of wasted bandwidth is minimized:

```
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

LSP2 and LS4 are preempted so that the least amount of bandwidth is wasted.

In the following example, backup protection preemption is enabled and the number of preempted LSPs is minimized:

```
Router(config)# no mpls traffic-eng fast-reroute backup-prot-preemption
```

The router selects the LSP whose bandwidth is next-greater than the required bandwidth. Therefore, the router picks LSP5 because it has the next larger amount of bandwidth over 75. One LSP is demoted. and 25 units of bandwidth are wasted.

Related Commands

Command	Description
show ip rsvp fast bw-protect	Displays information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection.

mpls traffic-eng fast-reroute timers

To specify how often the router considers switching a label-switched path (LSP) to a new (better) backup tunnel if additional backup bandwidth becomes available, use the **mpls traffic-eng fast-reroute timers** command in global configuration mode. To disable this timer, set the seconds value to zero or use the **no** form of this command.

mpls traffic-eng fast-reroute timers [**frequency** *seconds*]

no mpls traffic-eng fast-reroute timers

Syntax Description

frequency *seconds*	(Optional) Interval, in seconds, between scans to determine if an LSP should use a new, better backup tunnel. Valid values: 0 to 604800. A value of 0 disables promotions to a better LSP.

Command Default

The timer is running and is set to a frequency of every 300 seconds (5 minutes). If you enter **no mpls traffic-eng fast-reroute timers**, the router returns to this default behavior.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

In the following example, LSPs are scanned every 2 minutes (120 seconds) to see if they should be promoted to a better backup tunnel:

```
Router(config)# mpls traffic-eng fast-reroute timers frequency 120
```

show ip rsvp fast bw-protect

To display information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection, use the **show ip rsvp fast bw-protect** command in user EXEC or privileged EXEC mode.

show ip rsvp fast bw-protect

Syntax Description

This command has no arguments or keywords.

Command Default

The backup bandwidth protection and backup tunnel status information is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip rsvp fast bw-protect** command:

```
Router# show ip rsvp fast bw-protect

Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
--------------   -------  --------   ----------    -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

Table 3 describes the significant fields shown in the display.

Table 3 show ip rsvp fast bw-protect Field Descriptions

Field	Description
Primary Tunnel	Identification of the tunnel being protected.
Protect I/F	Interface name.
BW BPS:Type	Bandwidth, in bits per second, and type of bandwidth. Possible values are: • S—Subpool • G—Global pool

Table 3 show ip rsvp fast bw-protect Field Descriptions (continued)

Field	Description
Backup Tunnel:Label	Identification of the backup tunnel.
State	Status of backup tunnel. Valid values are: • Ready—Data is passing through the primary tunnel, but the backup tunnel is ready to take over if the primary tunnel goes down. • Active—The primary tunnel is down, so the backup tunnel is used for traffic. • None—There is no backup tunnel.
BW-P	Status of backup bandwidth protection. Possible values are ON and OFF.
Type	Type of backup tunnel. Possible values are: • Nhop—Next hop • NNHOP—Next-next hop

Related Commands

Command	Description
tunnel mpls traffic-eng fast-reroute bw-protect	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

show ip rsvp fast detail

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **show ip rsvp fast detail** command in user EXEC or privileged EXEC mode.

show ip rsvp fast detail

Syntax Description

This command has no arguments or keywords.

Command Default

Specific information for RSVP categories is not displayed.

Command Modes

User EXEC
Privileged EXEC'

Command History

Release	Modification
12.0(24)S	This command was introduced
12.0(29)S	Bandwidth Prot desired was added in the Flag field of the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip rsvp fast detail** command:

```
Router# show ip rsvp fast detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: PRAB-72-5_t500
  ERO: (incoming)
    10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
    555.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    555.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    555.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    555.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: Ready -- backup tunnel selected
      Backup Tunnel: Tu501      (label 19)
      Bkup Sender Template:
        Tun Sender: 555.5.6.5  LSP ID: 8
```

```
     Bkup FilerSpec:
       Tun Sender: 555.5.6.5, LSP ID: 8
 Path ID handle: 04000405.
 Incoming policy: Accepted. Policy source(s): MPLS/TE
 Status: Proxied
 Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

Table 4 describes the significant fields shown in the display.

Table 4 show ip rsvp fast detail Field Descriptions

Field	Description
Tun Dest	IP address of the receiver.
Tun ID	Tunnel identification number.
Ext Tun ID	Extended tunnel identification number.
Tun Sender	IP address of the sender.
LSP ID	Label-switched path identification number.
Setup Prio	Setup priority.
Holding Prio	Holding priority.
Flags	Backup bandwidth protection has been configured for the label-switched path (LSP).
Session Name	Name of the session.
ERO (incoming)	EXPLICIT_ROUTE object of incoming path messages.
ERO (outgoing)	EXPLICIT_ROUTE object of outgoing path messages.
Traffic params Rate	Average rate, in bits per second.
Max. burst	Maximum burst size, in bytes.
Min Policed Unit	Minimum policed units, in bytes.
Max Pkt Size	Maximum packet size, in bytes.
Inbound FRR	Status of inbound Fast Reroute (FRR) backup tunnel. If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active.
Outbound FRR	Status of outbound FRR backup tunnel. If this node is a point of local repair (PLR) for an LSP, there are three possible states: • Active—This LSP is actively using its backup tunnel, presumably because there has been a downstream failure. • No Backup—This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure. • Ready—This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use.

Table 4 show ip rsvp fast detail Field Descriptions (continued)

Field	Description
Backup Tunnel	If the Outbound FRR state is Ready or Active, this field indicates the following: • Which backup tunnel has been selected for this LSP to use in case of a failure. • The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point).
Bkup Sender Template	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Bkup FilerSpec	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Path ID handle	Protection Switch Byte (PSB) identifier.
Incoming policy	Policy decision of the LSP. If RSVP policy was not granted for the incoming path message for the tunnel, the LSP does not come up. Accepted is displayed.
Policy source(s)	For FRR LSPs, this value always is MPLS/TE for the policy source.
Status	For FRR LSPs, valid values are: • Proxied—Headend routers • Proxied Terminated—Tailend routers For midpoint routers, the field always is blank.

Related Commands

Command	Description
mpls traffic-eng fast-reroute backup-prot-preemption	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted.

show ip rsvp hello

To display if Hello is enabled globally on the router and if Hello statistics are enabled, use the **show ip rsvp hello** command in privileged EXEC mode.

show ip rsvp hello

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip rsvp hello** command:

```
Router# show ip rsvp hello

  State: Enabled
  Statistics: Enabled

Default State: Disabled
Default Statistics: Disabled
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip rsvp hello Field Descriptions

Field	Description
State	Status of whether Hello is globally enabled on the router.
Statistics	Status of Hello statistics. Valid values are: • Enabled—Statistics are configured. Hello packets are time-stamped when they arrive in the Hello input queue for the purpose of recording the time it takes until they are processed. • Disabled—Hello statistics are not configured. • Shutdown—Hello statistics are configured but not operational. The input queue is too long (that is, more than 10,000 packets are queued).

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello statistics	Displays how long Hello packets have been in the Hello input queue.

show ip rsvp hello instance detail

To display detailed information about a Hello instance, use the **show ip rsvp hello instance detail** command in privileged EXEC mode.

show ip rsvp hello instance detail [**filter destination** *ip-address*]

Syntax Description

filter destination *ip-address*	(Optional) IP address of the neighbor node.

Command Default

Detailed information about a Hello instance is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip rsvp hello instance detail** command:

```
Router# show ip rsvp hello instance detail

Neighbor 10.0.0.2  Source  10.0.0.1
    State: UP      (for 2d18h)
    Type: PASSIVE  (responding to requests)
    I/F: Et1/1
    LSPs protecting: 0
    Refresh Interval (msec) (used when ACTIVE)
      Configured: 100
      Statistics: (from 2398195 samples)
        Min:      100
        Max:      132
        Average:  100
        Waverage: 100 (Weight = 0.8)
        Current:  100
    Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
    Counters:
      Communication with neighbor lost:
        Num times: 0
        Reasons:
          Missed acks:             0
          Bad Src_Inst received:   0
          Bad Dst_Inst received:   0
          I/F went down:           0
          Neighbor disabled Hello: 0
      Msgs Received:   2398194
           Sent:       2398195
           Suppressed: 0
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip rsvp hello instance detail Field Descriptions

Field	Description
Neighbor	IP address of the adjacent node.
Source	IP address of the node that is sending the hello message.
State	Status of communication. Values are UP (node is communicating with its neighbor) and LOST (communication has been lost or never was established).
Type	Values are ACTIVE (node is sending requests) and PASSIVE (node is responding to a request).
I/F	Interface type.
LSPs protecting	Number of label-switched paths (LSPs) that are being protected.
Refresh Interval Configured	The frequency with which a node generates a hello message containing a HELLO REQUEST object for each neighbor whose status is being tracked. The frequency of these hello messages is determined by the Hello interval specified in the **ip rsvp signalling hello refresh interval** command.
Min	Minimum refresh interval.
Max	Maximum refresh interval.
Average	Average refresh interval.
Waverage	Weighted average refresh interval.
Current	Current refresh interval.
Src_instance	Source instance field value.
Dst_instance	Destination instance field value.
Communication with neighbor lost	Subsequent fields designate the number of times that communication with the neighbor was lost and why.
Num times	Total number of times that communication with the neighbor was lost.
Reasons	Subsequent fields designate why communication with the neighbor was lost.
Missed acks	Number of times that communication was lost due to missed ACKs.
Bad Src_Inst received	Number of times that communication was lost due to bad Bad Src_Inst fields.
Bad Dst_Inst received	Number of times that communication was lost due to bad Dst_Inst fields.

Table 6 show ip rsvp hello instance detail Field Descriptions (continued)

Field	Description
I/F went down	Number of times that the interface became unoperational.
Neighbor disabled Hello	Number of times that neighbor disabled Hello.
Msgs Received	Number of messages that were received.
Sent	Number of messages that were sent.
Suppressed	Number of messages that were suppressed due to optimization.

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.
show ip rsvp hello	Displays if Hello is enabled globally on the router and if Hello statistics are enabled.
show ip rsvp hello instance summary	Displays summary information about a Hello instance.

show ip rsvp hello instance summary

To display summary information about a Hello instance, use the **show ip rsvp hello instance summary** command in privileged EXEC mode.

show ip rsvp hello instance summary

Syntax Description

This command has no arguments or keywords.

Command Default

Summary information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip rsvp hello instance summary** command:

```
Router# show ip rsvp hello instance summary

I/F      Neighbor    Type     State  LostCnt
Et1/1    10.0.0.1    PASSIVE  UP     0
Se2/0    10.0.0.3    ACTIVE   UP     0
Et1/2    10.0.0.3    ACTIVE   UP     0
```

Table 7 describes the significant fields shown in the display.

Table 7 show ip rsvp hello instance summary Field Descriptions

Field	Description
I/F	Interface.
Neighbor	IP address of adjacent node.
Type	Activity. Values are ACTIVE (node is sending requests) and PASSIVE (node is responding to a request).
State	Status of communication. Values are UP (node is communicating with its neighbor) and LOST (communication has been lost or never was established).
LostCnt	Number of times that communication was lost with the neighbor.

Related Commands

Command	Description
ip rsvp signalling hello (configuration)	Enables Hello globally on the router.

ip rsvp signalling hello statistics	Enables Hello statistics on the router.
ip rsvp signalling hello	Displays if Hello is enabled globally on the router and if Hello statistics are enabled.
show ip rsvp hello instance detail	Displays detailed information about a Hello instance.

show ip rsvp hello statistics

To display how long hello packets have been in the Hello input queue, use the **show ip rsvp hello statistics** command in privileged EXEC mode.

show ip rsvp hello statistics

Syntax Description

This command has no arguments or keywords.

Command Default

Information about how long hello packets have been in the Hello input queue is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can use this command to determine if the Hello refresh interval is too small. If the interval is too small, communication may falsely be declared as lost.

Examples

The following is sample output from the **show ip rsvp hello statistics** command:

```
Router# show ip rsvp hello statistics

Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525
```

Table 8 describes the significant fields shown in the display.

Table 8 show ip rsvp hello statistics Field Descriptions

Field	Description
Status	Indicator of whether Hello has been enabled globally on the router.
Current	Amount of time, in milliseconds, that the current hello packet has been in the Hello input queue.

Table 8 show ip rsvp hello statistics Field Descriptions (continued)

Field	Description
Average	Average amount of time, in milliseconds, that hello packets are in the Hello input queue.
Max	Maximum amount of time, in milliseconds, that hello packets have been in the Hello input queue.
Current length	Current amount of time, in milliseconds, that hello packets have been in the Hello input queue.
Number of samples taken	Number of packets for which these statistics were compiled.

Related Commands

Command	Description
clear ip rsvp hello instance statistics	Clears Hello statistics for an instance.
clear ip rsvp hello statistics	Globally clears Hello statistics.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.
ip rsvp signalling hello statistics	Enables Hello statistics on the router.

show ip rsvp interface detail

To display the interface configuration for Hello, use the **show ip rsvp interface detail** command in privileged EXEC mode.

show ip rsvp interface detail [*interface*]

Syntax Description

interface	(Optional) Interface for which you want to show the Hello configuration.

Command Default

The interface configuration for Hello is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show ip rsvp interface detail** command:

```
Router# show ip rsvp interface detail Et1/2

Et1/2:
   Bandwidth:
     Curr allocated: 0G bits/sec
     Max. allowed (total): 7500K bits/sec
     Max. allowed (per flow): 7500K bits/sec
     Max. allowed for LSP tunnels using sub-pools: 0G bits/sec
   Neighbors:
     Using IP encap: 1.  Using UDP encap: 0
     DSCP value used in RSVP msgs: 0x0
   Hello:
     State: Enabled
     Refresh Interval: 500
     Missed Acks: 4
     DSCP value used in HELLO msgs: 0
```

Table 9 describes the significant fields shown in the display.

Table 9 show ip rsvp interface detail Field Descriptions

Field	Description
Curr allocated	Amount of bandwidth currently allocated.
Max. allowed (total)	Total maximum amount of bandwidth allowed.
Max. allowed (per flow)	Maximum amount of bandwidth allowed per flow.

Table 9 show ip rsvp interface detail Field Descriptions (continued)

Field	Description
Max. allowed for LSP tunnels using sub-pools	Maximum amount of bandwidth permitted for label-switched path (LSP) tunnels that obtain their bandwidth from subpools.
Using IP encap	Number of neighbors using IP encapsulation.
Using UDP encap	Number of neighbors using User Data Protocol (UDP) encapsulation.
DSCP value used in RSVP msgs	The differentiated services code point (DSCP) value that is in Resource Reservation Protocol (RSVP) messages.
State	State (Enabled or Disabled) of Hello.
Refresh Interval	Frequency with which a node sends a hello message to its neighbor.
Missed Acks	Number of sequential acknowledgments that the node did not receive.
DSCP value used in HELLO msgs	The DSCP value that is in hello messages.

Related Commands

Command	Description
ip rsvp signalling hello (interface)	Enables Hello on an interface where you need Fast Reroute protection.
ip rsvp signalling hello dscp	Sets the DSCP value that is in the IP header of the hello message sent out from an interface.
ip rsvp signalling hello refresh interval	Configures the Hello request interval.

show ip rsvp request

To display Resource Reservation Protocol (RSVP)-related request information currently in the database, use the **show ip rsvp request** command in privileged EXEC mode.

show ip rsvp reservation [**detail**] [**filter** [**destination** *ip-address* | *host-name*] [**dst-port** *port-number*] [**source** *ip-address* | *host-name*] [**src-port** *port-number*]]

Syntax Description

ip-address	(Optional) Specifies the destination IP address.
host-name	(Optional) Specifies the hostname.
detail	(Optional) Specifies additional receiver information.
filter	(Optional) Specifies a subset of the receivers to display.
destination *ip-address*	(Optional) Specifies the destination IP address of the receiver.
host-name	(Optional) Specifies the hostname of the receiver.
dst-port *port-number*	(Optional) Specifies the destination port number. Valid destination port numbers can be in the range of 0 to 65535.
source *ip-address*	(Optional) Specifies the source IP address of the receiver.
host-name	(Optional) Specifies the host name of the receiver.
src-port *port-number*	(Optional) Specifies the source port number. Valid source port numbers can be in the range of 0 to 65535.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2. The **detail** keyword was added to display additional request information.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. This command was enhanced to show Fast Reroute information when a link-state packet (LSP) is actively using a backup tunnel that terminates at this node (that is, when a node is the merge point [MP].) The command is supported on the Cisco 10000 series Edge Services Router (ESR).
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show ip rsvp request** command to display the RSVP reservations currently being requested upstream for a specified interface or all interfaces. The received reservations may differ from requests because of aggregated or refused reservations. If desired, information for only a single tunnel or a subset of tunnels can be displayed.

Limiting the Display

When hundreds or thousands of tunnels exist and you are interested in only a few, you can display the output for only a single tunnel or a subset of tunnels. To request a limited display, enter the **show ip rsvp request** command with the appropriate keyword (called an output filter): **destination**, **dst-port**, **source**, and **src-port**. You can enter any or all of the output filters, and you can enter them whether or not you specify the **detail** keyword.

Examples

The following is sample output from the **show ip rsvp request** command:

```
Router# show ip rsvp request

To              From            Pro DPort Sport Next Hop        I/F    Fi Serv
172.240.1.49    172.240.4.53    1   0     0     172.240.3.53    Et1    FF LOAD
```

Table 10 describes the significant fields shown in the display.

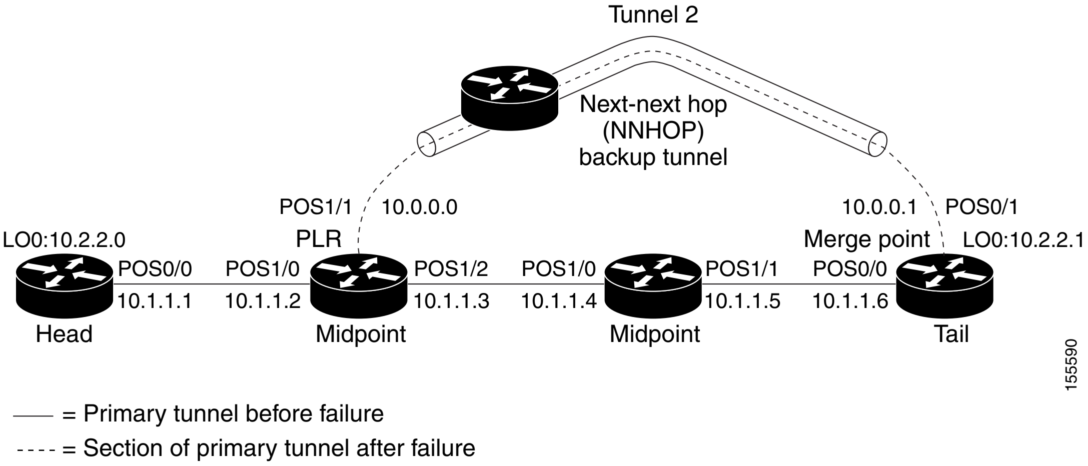
Table 10 show ip rsvp request Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wildcard Filter, Shared Explicit, or Fixed Filter).
Serv	Service (value can be **rate** or **load**).

The following is sample output from the **show ip rsvp request detail** command when the command is entered on the MP before and after a failure.

Figure 9 illustrates the network topology for the RSVP configuration example.

Figure 9 Network Topology for the RSVP Configuration Example



Example 1: The command is entered on the MP before a failure.

```
Router# show ip rsvp request detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.5 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
    Empty
```

Example 2: The command is entered on the MP after a failure.

```
Router# show ip rsvp request detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.5 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     Empty
   FRR is in progress (we are Merge Point)

 RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.0.0.0 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     Empty
   FRR is in progress (we are Merge Point)
```

Notice that after the failure, there are two entries for the rerouted LSP. Information referenced in the following explanation is highlighted.

The first entry continues to show the prefailure information (that is, resv messages are being sent to 10.1.1.5 on Ethernet1). This state is for the resv being sent upstream before the failure, in response to path messages sent before the failure. This state may time out quickly, or it may continue to be refreshed for a few minutes if, for example, an upstream node is unaware of the failure.

The second entry shows the post-failure information (that is, resv messages are being sent to 10.0.0.0 on Ethernet2). This state is for the resv messages being sent upstream after the failure (to the Point of Local Repair [PLR]), and will remain and be refreshed as long as the LSP is rerouted.

In example 2, the MP is also the tail of the LSP. There is no Record Route Object (RRO) information because there are no nodes downstream.

Related Commands

Command	Description
show ip rsvp reservation	Displays RSVP PATH-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP RESV-related receiver information currently in the database.

show ip rsvp reservation

To display Resource Reservation Protocol (RSVP)-related receiver information currently in the database, use the **show ip rsvp reservation** command in user EXEC or privileged EXEC mode.

Syntax for T Releases

show ip rsvp reservation [*ip-address* | *host-name*] [**detail**]

Syntax for 12.0 S and 12.2 S Releases

show ip rsvp reservation [**detail**] [**filter** [**destination** *ip-address* | *host-name*]
[**dst-port** *port-number*] [**source** *ip-address* | *host-name*] [**src-port** *port-number*]]

Syntax Description

ip-address	(Optional) Destination IP address.
host-name	(Optional) Hostname.
detail	(Optional) Specifies additional receiver information.
filter	(Optional) Specifies a subset of the receivers to display.
destination *ip-address*	(Optional) Specifies the destination IP address of the receiver.
host-name	(Optional) Specifies the hostname of the receiver.
dst-port *port-number*	(Optional) Specifies the destination port number. The destination port number range is from 0 to 65535.
source *ip-address*	(Optional) Source IP address of the receiver.
host-name	(Optional) Hostname of the receiver.
src-port *port-number*	(Optional) Source port number. The source port number range is from 0 to 65535.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2. The **detail** keyword was added to display additional reservation information.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S. The command displays Fast Reroute information when a link-state packet (LSP) is actively using a backup tunnel at this node (that is, when a node is the Point of Local Repair [PLR]). If desired, information for only a single tunnel or a subset of tunnels can be displayed. The command is supported on the Cisco 10000 series Edge Services Router (ESR).
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T and its output was modified to display application ID information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show ip rsvp reservation** command to display the current receiver (RESV) information in the database for a specified interface or all interfaces. This information includes reservations aggregated and forwarded from other RSVP routers.

Limiting the Display

When hundreds or thousands of tunnels exist and you are interested in only a few, you can display the output for only a single tunnel or a subset of tunnels. To request a limited display, enter the **show ip rsvp reservation** command with the appropriate keyword (called an output filter): **destination**, **dst-port**, **source,** and **src-port**. You can enter any or all of the output filters, and you can enter them whether or not you specify the **detail** keyword.

Examples

The following is sample output from the **show ip rsvp reservation** command:

```
Router# show ip rsvp reservation

To            From          Pro DPort Sport Next Hop      I/F    Fi Serv
172.240.1.49  172.240.4.53  1   0     0     172.240.1.49  Se1    FF LOAD
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip rsvp reservation Field Descriptions

Field	Descriptions
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates IP protocol such as TCP or User Data Protocol (UDP).
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wildcard Filter, Shared-Explicit, or Fixed-Filter).
Serv	Service (value can be RATE or LOAD).

The following is sample output from the **show ip rsvp reservation detail** command:

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 192.168.104.3, Source is 192.168.104.1,
  Protocol is UDP, Destination port is 4444, Source port is 4444
  Next Hop is 192.168.106.2, Interface is ATM1/0.1
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 0A00040B.
  Created: 12:18:32 UTC Sat Dec 4 2004
  Average Bitrate is 5K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
    Priorities - preempt: 5, defend: 2
    Application ID: 'GUID=www.cisco.com, VER=1.1.1.2, APP=voice, SAPP=h323'
                    '/usr/local/bin/CallManager'
```

Table 12 describes the significant fields shown in the display.

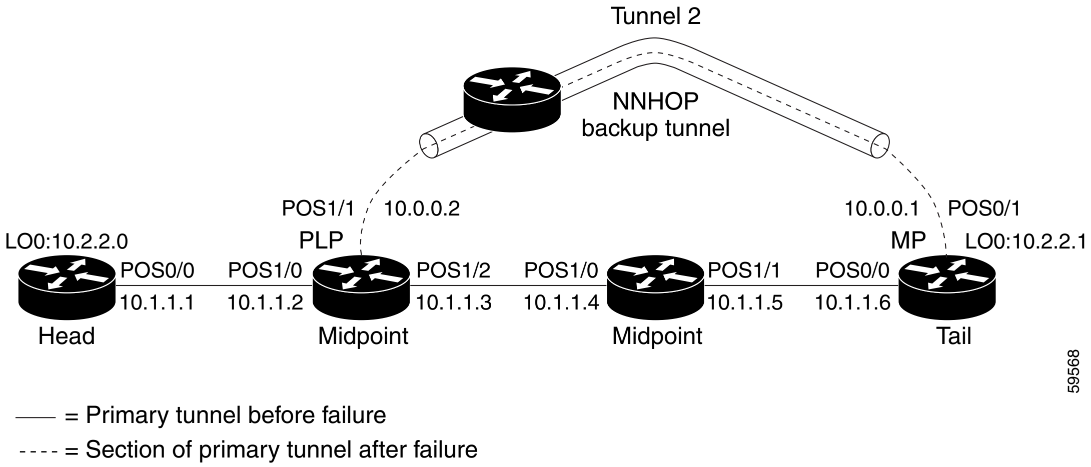
Table 12 show ip rsvp reservation detail Field Descriptions

Field	Descriptions
RSVP Reservation	Destination—Receiver's IP address of the RESV message. Source—Sender's IP address of the RESV message.
Protocol	Protocol—IP protocol used; UDP—User Data Protocol.
Destination port	Receiver's port number.
Source port	Sender's port number.
Next Hop	IP address of the next hop.
Interface	Interface type of the next hop.
Reservation Style	Multireservations sharing of bandwidth; values include Fixed-Filter, Shared-Explicit, and Wildcard-Filter.
QoS Service	Type of QoS Service configured; values include Guaranteed-Rate and Control Load.
Resv ID handle	Internal database ID assigned to the RESV message by RSVP for bookkeeping purposes.
Created	Time and date when the reservation was created.
Average Bitrate	Average rate, in bits per second, for the data.
Maximum Burst	Largest amount of data allowed in kilobytes.
Min Policed Unit	Size of the smallest packet generated by the application in bytes, including the application data and all protocol headers at or above the IP level.
Max Pkt Size	Largest packet allowed in bytes.
Status	Status of the local policy; values are Proxied and Proxy-terminated. **Note** A blank status field means you issued the command on a midpoint for that reservation.
Policy	Policy status: Forwarding—RSVP RESV messages are being accepted and forwarded.
Policy source(s)	Type of local policy in effect; values include default, local, and Multiprotocol Label Switching (MPLS)/Traffic Engineering (TE).
Priorities	Preemption priorities in effect. • preempt: the startup priority; values are 0 to 7 for traffic engineering (TE) reservations with 0 being the highest. Values are 0 to 65535 for non-TE reservations with 0 being the lowest. • defend: the hold priority; values are the same as preempt.
Application ID	A quotable string that identifies the sender application and can be used to match on local policies. The string includes the policy locator in the X.500 Distinguished Name format and the application or filename of the sender application.

The following is sample output from the **show ip rsvp reservation detail** command when the command is entered on the PLR before and after a failure.

Figure 9 illustrates the network topology for the RSVP configuration example.

Figure 10 Network Topology for the RSVP Configuration Example



Example 1: The command is entered on the PLR before a failure

```
Router# show ip rsvp reservation detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.4 on POS1/2
   Label is 18
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     10.1.1.5/32, Flags:0x0 (No Local Protection)
       Label record: Flags 0x1, ctype 1, incoming label 18
     10.1.1.6/32, Flags:0x0 (No Local Protection)
       Label record: Flags 0x1, ctype 1, incoming label 0
```

Example 2: The command is entered on the PLR after a failure

```
Router# show ip rsvp reservation detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   FRR is in progress: (we are PLR)
    Bkup Next Hop is  10.0.0.1 on POS1/1
        Label     is  0
    Orig Next Hop was 10.1.1.4 on POS1/2
        Label     was 18
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
  RRO:
    10.2.2.1/32, Flags:0x0 (No Local Protection)
      Label record: Flags 0x1, ctype 1, incoming label 0
```

Notice the following (see highlighted text) in Examples 1 and 2:

- At the PLR, you see "Fast Reroute (FRR) is in progress (we are PLR)" when an LSP has been rerouted (that is, it is actively using a backup tunnel).
- RESV messages arrive on a different interface and from a different Next Hop after a failure. The prefailure display shows the original NHOP and arriving interface; the postfailure display shows both the original and the new (Bkup) NHOP and arriving interface. The label is also shown.
- The Record Route Object (RRO) in arriving RESV messages changes after the failure, given that the RESV messages will avoid the failure (that is, it will traverse different links or hops).

Related Commands

Command	Description
clear ip rsvp hello instance counters	Clears (refreshes) the values for Hello instance counters.
ip rsvp reservation	Enables a router to simulate RSVP RESV message reception from the sender.
show ip rsvp sender	Displays RSVP RESV-related receiver information currently in the database,

show ip rsvp sender

To display Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **show ip rsvp sender** command in user EXEC or privileged EXEC mode.

Syntax for T Releases

show ip rsvp sender [*ip-address* | *host-name*] [**detail**]

Syntax for 12.0 S and 12.2 S Releases

show ip rsvp sender [**detail**] [**filter** [**destination** *ip-address* | *host-name*]
[**dst-port** *port-number*] [**source** *ip-address* | *host-name*] [**src-port** *port-number*]]

Syntax Description

ip-address	(Optional) Destination IP address.
host-name	(Optional) Hostname.
detail	(Optional) Specifies additional sender information.
filter	(Optional) Specifies a subset of the senders to display.
destination *ip-address*	(Optional) Destination IP address of the sender.
host-name	(Optional) Hostname of the sender.
dst-port *port-number*	(Optional) Destination port number. The range is from 0 to 65535.
source *ip-address*	(Optional) Source IP address of the sender.
host-name	(Optional) Hostname of the sender.
src-port *port-number*	(Optional) Source port number. The range is from 0 to 65535.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.0(22)S	This command was integrated into Cisco IO Release 12.0(22)S. The command output includes additional information that can be helpful when examining Fast Reroute state or when troubleshooting Fast Reroute. If desired, information for only a single tunnel or a subset of tunnels can be displayed. The command is supported on the Cisco 10000 series Edge Services Router (ESR).
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T and its output was modified to display application ID information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show ip rsvp sender** command to display the RSVP sender (PATH) information currently in the database for a specified interface or all interfaces.

The **show ip rsvp sender** is very useful for determining the state of RSVP signaling both before and after a label-switched packet (LSP) has been fast rerouted. The **show ip rsvp sender** command is especially useful when used at the Point of Local Repair (PLR) or at the Merge Point (MP).

Limiting the Display

When hundreds or thousands of tunnels exist and you are interested in only a few, it is useful to display output for only a single tunnel or a subset of tunnels. To request a limited display, enter the **show ip rsvp sender** command with the appropriate keyword (called an output filter): **destination**, **dst-port**, **source**, and **src-port**. You can enter any or all of the output filters, and you can enter them whether or not you specify the **detail** keyword.

Examples

The following is sample output from the **show ip rsvp sender** command:

```
Router# show ip rsvp sender

To              From            Pro DPort Sport Prev Hop        I/F
172.240.1.49    172.240.4.53    1   0     0     172.240.3.53    Et1
172.240.2.51    172.240.5.54    1   0     0     172.240.3.54    Et1
```

Table 13 describes the significant fields shown in the display.

Table 13 show ip rsvp sender Field Descriptions

Field	Descriptions
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates IP protocol such as TCP or User Data Protocol (UDP).
DPort	Destination port number.
Sport	Source port number.
Prev Hop	IP address of the previous hop.
I/F	Interface of the previous hop.

The following is sample output from the **show ip rsvp sender detail** command:

```
Router# show ip rsvp sender detail

PATH Session address: 192.168.104.3, port: 4444. Protocol: UDP
  Sender address: 192.168.104.1, port: 4444
     Inbound from: 192.168.104.1 on interface:
  Traffic params - Rate: 5K bits/sec, Max. burst: 1K bytes
                   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Path ID handle: 09000408.
  Incoming policy: Accepted. Policy source(s): Default
    Priorities - preempt: 5, defend: 2
    Application ID: 'GUID=www.cisco.com, VER=10.1.1.2, APP=voice, SAPP=h323'
                    '/usr/local/bin/CallManager'
```

```
Status: Proxied
Output on ATM1/0.1. Policy status: Forwarding. Handle: 04000409
  Policy source(s): Default
```

Table 14 describes the significant fields shown in the display.

Table 14 show ip rsvp sender detail Field Descriptions

Field	Descriptions
PATH Session address	Destination IP address of the PATH message. • port—number of the destination port. • Protocol—IP protocol used; UDP—User Data Protocol.
Sender address	Source IP address of the PATH message. • port—number of the source port.
Inbound from	IP address of the sender and the interface name. **Note** A blank interface field means the PATH message originated at the router on which the **show** command is being executed (the headend router). A specified interface means the PATH message originated at an upstream router.
Traffic params	• Rate—Speed in kilobits per second. • Max. burst—Largest amount of data allowed in kilobytes. • Min Policed Unit—Size of the smallest packet generated by the application in bytes, including the application data and all protocol headers at or above the IP level. • Max Pkt Size—Largest packet allowed in bytes.
PATH ID handle	Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes.
Incoming policy	State of the incoming policy: • Accepted—RSVP PATH messages are being accepted, but not forwarded. • Not Accepted—RSVP PATH messages are being rejected. Policy source(s)—type of policy in effect. Values are: • default • local • Multiprotocol Label Switching (MPLS)/Traffic Engineering (TE)
Priorities	Preemption priorities in effect. • preempt: the startup priority; values are 0 to 7 for traffic engineering (TE) reservations with 0 being the highest. Values are 0 to 65535 for non-TE reservations with 0 being the lowest. • defend: the hold priority; values are the same as for preempt.
Application ID	A quotable string that identifies the sender application and can be used to match on local policies. The string includes the policy locator in the X.500 Distinguished Name format and the application or filename of the sender application.

Table 14 show ip rsvp sender detail Field Descriptions (continued)

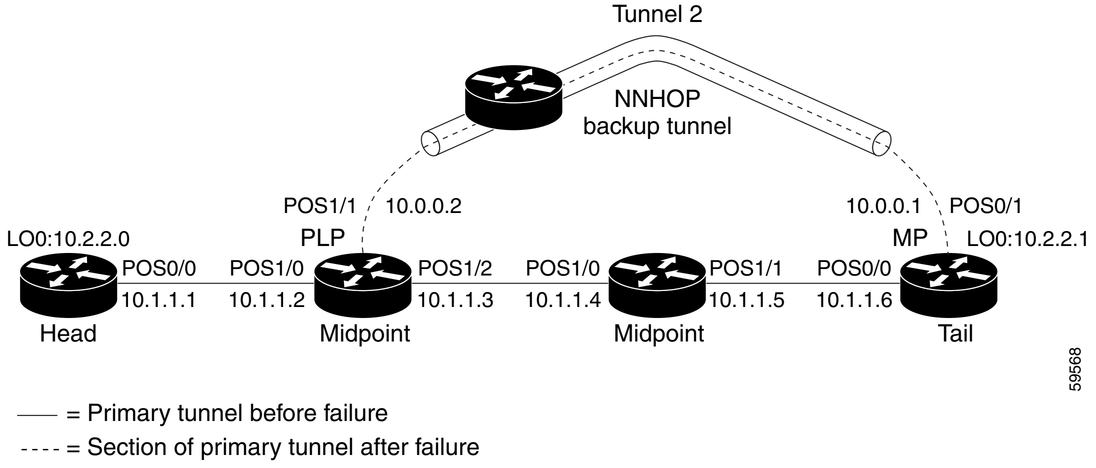
Field	Descriptions
Status	Status of the local policy; values are: • Proxied • Proxy-terminated • Blockaded
Output on *interface*	Policy status (on the outbound interface): • Forwarding—Inbound PATH messages are being forwarded. • Not Forwarding—Outbound PATH messages are being rejected. • Handle—Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes.
Policy source(s)	Type of local (outbound) policy in effect; values are: • default • local • MPLS/TE

The following is sample output from the **show ip rsvp sender detail** command under the following circumstances:

- The command is entered at the PLR before a failure (Example 1).
- The command is entered at the PLR after a failure (Example 2).
- The command is entered at the MP before a failure (Example 3).
- The command is entered at the MP after a failure (Example 4).
- The command output shows all senders (Example 5).
- The command output shows only senders who have a specific destination (Example 6).
- Show more detail about a sender who has a specific destination (Example 7).

Figure 9 illustrates the network topology for the RSVP configuration example.

Figure 11   Network Topology for the RSVP Configuration Example



Example 1: The command is entered at the PLR before a failure

The following is sample output from the **show ip rsvp sender detail** command when it is entered at the PLR before a failure:

```
Router# show ip rsvp sender detail

PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS1/0 from PHOP 10.1.1.1
   Path refreshes being sent to NHOP 10.1.1.4 on POS1/1
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   ERO:
     10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
     10.1.1.5 (Strict IPv4 Prefix, 8 bytes, /32)
     10.1.1.6 (Strict IPv4 Prefix, 8 bytes, /32)
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: Ready -- backup tunnel selected
       Backup Tunnel: Tu2        (label 0)
       Bkup Sender Template:
         Tun Sender: 10.0.0.0, LSP ID: 126
       Bkup FilerSpec:
         Tun Sender: 10.0.0.0, LSP ID 126
```

Table 15 describes the significant fields shown in the display.

Note The Flags field is important for Fast Reroute. For information about flags that must be set, see the Flags field description in Table 15.

Table 15 show ip rsvp sender detail Field Descriptions—on PLR Before Failure

Field	Description
The first five fields provide information that uniquely identifies the LSP. **The first three fields identify the LSP's session (that is, the contents of the SESSION object in arriving PATH messages).**	
Tun Dest	IP address of the destination of the tunnel.
Tun ID	Tunnel identification number.
Ext Tun ID	Extended tunnel identification number.
The next two fields identify the LSP's sender (SENDER_TEMPLATE object of arriving PATH messages).	
Tun Sender	Tunnel sender.
LSP ID	LSP identification number.
The remaining fields indented under PATH provide additional information about this LSP.	
Session Attr—Session attributes. Refers to information included in the SESSION_ATTRIBUTE object of arriving PATH messages, such as the Setup and Holding Priorities, Flags, and the Session Name.	
Setup Prio	Setup priority.
Holding Prio	Holding priority.
Flags	An LSP must have the "Local protection desired" flag of the SESSION_ATTRIBUTE object set for the LSP to use a backup tunnel (that is, in order to receive local protection). If this flag is not set, you have not enabled Fast Reroute for this tunnel at its headend (by entering the **tunnel mpls traffic-eng fast-reroute** command). NNHOP backup tunnels rely on label recording, so LSPs should have the "label recording desired" flag set too. This flag is set if the tunnel was configured for Fast Reroute.
ERO—Refers to the EXPLICIT_ROUTE Object (ERO) of the PATH messages. This field displays the contents of the ERO at this node. As a PATH message travels from the sender (headend) to the receiver (tailend), each node removes its own IP address from the ERO. The displayed value reflects the remainder of hops between this node and the tail.	
Fast-Reroute Backup info—Information that is relevant to Fast Reroute for this LSP.	
Inbound FRR	If this node is downstream from a rerouted LSP (for example, at a Merge Point for this LSP), the state is Active.

Table 15 show ip rsvp sender detail Field Descriptions—on PLR Before Failure (continued)

Field	Description
Outbound FRR	If this node is a PLR for an LSP, there are three possible states: • Active—This LSP is actively using its backup tunnel, presumably because there has been a downstream failure. • No Backup—This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure. • Ready—This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use.
Backup Tunnel	If the Outbound FRR state is Ready or Active, this field indicates the following: • Which backup tunnel has been selected for this LSP to use in case of a failure. • The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the Merge Point).
Bkup Sender Template	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, PATH and PATHTEAR messages will contain the new SENDER_TEMPLATE. RESV and RESVTEAR messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Bkup FilerSpec	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, PATH and PATHTEAR messages will contain the new SENDER_TEMPLATE. RESV and RESVTEAR messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes as shown in Example 2.

Example 2: The command is entered at the PLR after a failure

If the LSP begins actively using the backup tunnel and the command is entered at the PLR after a failure, the display changes as shown below.

Note Highlighted fields are referenced in the explanation that follows the sample display.

```
Router# show ip rsvp sender detail

PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS1/0 from PHOP 10.1.1.1
   Path refreshes being sent to NHOP 10.2.2.1 on Tunnel2
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   ERO:
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: Active -- using backup tunnel
       Backup Tunnel: Tu2        (label 0)
       Bkup Sender Template:
         Tun Sender: 10.0.0.0, LSP ID: 126
       Bkup FilerSpec:
         Tun Sender: 10.0.0.0, LSP ID 126
       Orig Output I/F: Et2
       Orig Output ERO:
         10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
         10.1.1.5 (Strict IPv4 Prefix, 8 bytes, /32)
         10.1.1.6 (Strict IPv4 Prefix, 8 bytes, /32)
         10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
```

Once an LSP is actively using a backup tunnel, the following changes occur:

- PATH refreshes are no longer sent to the original NHOP out the original interface. They are sent through the backup tunnel to the node that is the tail of the backup tunnel (NHOP or NNHOP).
- The ERO is modified so that it will be acceptable upon arrival at the NHOP or NNHOP.
- The display shows both the original ERO and the new one now being used.
- The display shows the original output interface (that is, the interface from which PATH messages were sent for this LSP before the failure).

Example 3: The command is entered at the MP before a failure

If the same **show ip rsvp sender** command is entered at the Merge Point (the backup tunnel tail), the display changes from before to after the failure. The following is sample output before a failure:

```
Router# show ip rsvp sender detail

PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS0/0 from PHOP 10.1.1.5
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: No backup tunnel selected
```

Example 4: The command is entered at the MP after a failure

After a failure, the following changes occur:

- The interface and previous hop (PHOP) from which PATH messages are received will change.
- The inbound FRR becomes Active.
- The original PHOP and the original input interface are displayed as shown below.

The following is sample output after a failure:

```
Router# show ip rsvp sender detail

PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS0/1 from PHOP 10.0.0.0 on Loopback0
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Active
       Orig Input I/F: POS0/0
       Orig PHOP: 10.1.1.5
       Now using Bkup Filterspec w/ sender: 10.0.0.0 LSP ID: 126
     Outbound FRR: No backup tunnel selected
```

Notice the following changes, which are highlighted in the sample command output:

- After a failure, PATH refreshes arrive on a different interface and from a different PHOP.
- The original PHOP and input interface are shown under Fast-Reroute Backup information, along with the FILTERSPEC object that will now be used when sending messages (such as RESV and RESVTEAR).

Example 5: The command output shows all senders

In the following example, information about all senders is displayed.

```
Router# show ip rsvp sender

To              From              Pro DPort Sport Prev Hop        I/F  BPS  Bytes
10.2.2.1        10.2.2.0          0   1     59    10.1.1.1        Et1   0G     1K
10.2.2.1        172.31.255.255    0   2     9                           0G     1K
10.2.2.1        10.2.2.0          0   3     12    10.1.1.1        Et1   0G     1K
10.2.2.1        172.31.255.255    0   3     20                          0G     1K
172.16.0.0      172.31.255.255    0   0     23                          0G     1K
172.16.0.0      172.31.255.255    0   1     22                          0G     1K
172.16.0.0      172.31.255.255    0   1000  22                          0G     1K
```

Table 16 describes the significant fields shown in the display.

Table 16 show ip rsvp sender Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).

Table 16 show ip rsvp sender Field Descriptions (continued)

Field	Description
DPort	Destination port number.
Sport	Source port number.
Prev Hop	IP address of the previous hop.
I/F	Interface of the previous hop.
BPS	Reservation rate, in bits per second, the application is advertising it might achieve.
Bytes	Bytes of burst size the application is advertising it might achieve.

Example 6: The command output shows only senders who have a specific destination.

To show only information about senders who have a specific destination, specify the destination filter as shown below. In this example, the destination is 155.16.6.6.

```
Router# show ip rsvp sender destination 155.16.6.6

To          From         Pro DPort Sport Prev Hop    I/F  BPS  Bytes
155.16.0.0  155.31.255   0   0     23                      0G     1K
155.16.0.0  155.31.255   0   1     22                      0G     1K
155.16.0.0  155.31.255   0   1000  22                      0G     1K
```

Example 7: Show more detail about a sender who has a specific destination.

To show more detail about the sender whose destination port is 1000 (as shown in Example 6), specify the command with the destination port filter:

```
Router# show ip rsvp sender detail dst-port 1000

PATH:
  Tun Dest 155.16.0.0 Tun ID 1000 Ext Tun ID 155.31.255.255
  Tun Sender: 155.31.255.255, LSP ID: 22
  Path refreshes being sent to NHOP 10.1.1.4 on Ethernet2
  Session Attr::
    Setup Prio: 7, Holding Prio: 7
    Flags: SE Style
    Session Name:tagsw4500-25_t1000
  ERO:
    10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
    155.16.0.0 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: No backup tunnel selected
```

Related Commands

Command	Description
ip rsvp sender	Enables a router to simulate RSVP PATH message reception from the sender.
show ip rsvp reservation	Displays RSVP PATH-related receiver information currently in the database.

show mpls traffic tunnel backup

To display information about the backup tunnels that are currently configured, use the **show mpls traffic tunnel backup** command in user EXEC or privileged EXEC mode.

show mpls traffic tunnel backup tunnel*tunnel-id*

Syntax Description

tunnel*tunnel-id*	Tunnel ID of the backup tunnel for which you want to display information.

Command Default

Information about currently configured backup tunnels is not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA

Examples

The following is sample output from the **show mpls traffic tunnel backup** command.

```
Router# show mpls traffic tunnel backup tunnel1000

Tunnel1000          Dest: 10.0.0.9        State: Up
any-pool cfg 100 inuse 0 num_lsps 0
     protects: ATM0.1
```

Table 17 describes the significant fields shown in the display.

Table 17 show mpls traffic tunnel backup Field Descriptions

Field	Description
Tunnel	Tunnel ID of the backup tunnel for which this information is being displayed.
Dest	IP address of the destination of the backup tunnel.
State	State of the backup tunnel. Valid values are Up, Down, or Admin-down.
any-pool	Pool from which bandwidth is acquired. Valid values are any-pool, global-pool, and sub-pool.
cfg	Amount of bandwidth configured for that pool.
inuse	Amount of bandwidth currently being used.

Table 17 show mpls traffic tunnel backup Field Descriptions (continued)

Field	Description
num_lsps	Number of label-switched paths (LSPs) being protected.
protects	The protected interfaces that are using this backup tunnel.

Related Commands

Command	Description
tunnel mpls traffic-eng backup-bw	Specifies what types of LSPs can use a backup tunnel, whether the backup tunnel should provide bandwidth protection, and if so, how much.

show mpls traffic-eng fast-reroute database

To display the contents of the Fast Reroute (FRR) database, use the **show mpls traffic-eng fast-reroute database** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng fast-reroute database [*network* [*mask* | *masklength*] | **labels** *low label* [**-***high label*] | **interface** *ifname* [**backup-interface** *ifname*] | **backup-interface** *ifname*] [**state** {**active** | **ready** | **partial** | **complete**}] [**role** {**head** | **middle**}][**detail**]

Syntax Description

network	IP address of the destination network. This functions as the prefix of the FRR rewrite.
mask	Bit combination indicating the portion of the IP address that is being used for the subnet address.
masklength	Number of bits in mask of destination.
labels	Shows only database entries that possess in-labels (local labels) assigned by this router. You specify either a starting value or a range of values.
low label	Starting label value or lowest value in the range.
-*high label*	(Optional) Highest label value in the range.
interface	Shows only database entries related to the primary outgoing interface.
ifname	Name of the primary outgoing interface.
backup-interface	(Optional) Shows only database entries related to the backup outgoing interface.
ifname	Name of the backup outgoing interface.
state	(Optional) Shows entries that match one of four possible states: active, ready, partial, or complete.
active	The FRR rewrite has been put into the forwarding database (where it can be placed onto appropriate incoming packets).
ready	The FRR rewrite has been created, but has not yet been moved into the forwarding database.
partial	State before the FRR rewrite has been fully created; its backup routing information is still incomplete.
complete	State after the FRR rewrite has been assembled: it is either ready or active.
role	(Optional) Shows entries associated either with the tunnel head or tunnel midpoint.
head	Entry associated with tunnel head.
middle	Entry associated with tunnel midpoint.
detail	(Optional) Shows long-form information: LFIB-FRR total number of clusters, groups, and items in addition to the short-form information of prefix, label and state.

Command Default

The contents of the FRR database are not displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(10)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Catalyst 6000 series with the SUP720 processor.
12.2(28)SB	This command was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows output from the **show mpls traffic-eng fast-reroute database** command at a tunnel head link:

```
Router# show mpls traffic-eng fast-reroute database 10.0.0.0

Tunnel head fast reroute information:

Prefix       Tunnel  In-label  Out intf/label  FRR intf/label  Status
10.0.0.0/16   Tu111   Tun hd    PO0/0:Untagged  Tu4000:16        ready
10.0.0.0/16   Tu449   Tun hd    PO0/0:Untagged  Tu4000:736       ready
10.0.0.0/16   Tu314   Tun hd    PO0/0:Untagged  Tu4000:757       ready
10.0.0.0/16   Tu313   Tun hd    PO0/0:Untagged  Tu4000:756       ready
```

Table 18 describes the significant fields shown in the display.

Table 18 show mpls traffic-eng fast-reroute database Field Descriptions

Field	Description
Prefix	Address to which packets with this label are going.
Tunnel	Tunnel's identifying number.
In-label	Label advertised to other routers to signify a particular prefix. The value "Tun hd" occurs when no such label has been advertised.
Out intf/label	Out interface—short name of the physical interface through which traffic goes to the protected link. Out label: • At a tunnel head, this is the label advertised by the tunnel destination device. The value "*Untagged*" occurs when no such label has been advertised. • At tunnel midpoints, this is the label selected by the next hop device. The "Pop Tag" value occurs when the next hop is the tunnel's final hop.

Table 18 show mpls traffic-eng fast-reroute database Field Descriptions (continued)

Field	Description
FRR intf/label	Fast Reroute interface—the backup tunnel interface. Fast Reroute label: • At a tunnel head, this is the label selected by the tunnel tail to indicate the destination network. The value “`Untagged`” occurs when no such label has been advertised. • At tunnel midpoints, this has the same value as the Out Label.
Status	State of the rewrite: `partial`, `ready`, or `active`. (These terms are defined above, in the “Syntax Description” section).

The following example shows output from the **show mpls traffic-eng fast-reroute database** command with the **labels** keyword specified at a midpoint link:

Router# **show mpls traffic-eng fast-reroute database labels 250 - 255**

```
Tunnel head fast reroute information:
Prefix   Tunnel   In-label   Outintf/label   FRR intf/label   Status

LSP midpoint frr information:

LSP identifier          In-label   Out intf/label  FRR intf/label  Status
10.110.0.10 229 [7334] 255        PO0/0:694       Tu4000:694      active
10.110.0.10 228 [7332] 254        PO0/0:693       Tu4000:693      active
10.110.0.10 227 [7331] 253        PO0/0:692       Tu4000:692      active
10.110.0.10 226 [7334] 252        PO0/0:691       Tu4000:691      active
10.110.0.10 225 [7333] 251        PO0/0:690       Tu4000:690      active
10.110.0.10 224 [7329] 250        PO0/0:689       Tu4000:689      active
```

The following example shows output from the **show mpls traffic-eng fast-reroute database** command with the **detail** keyword included at a tunnel head link:

```
Router# show mpls traffic-eng fast-reroute database 10.0.0.0. detail

LFIB FRR Database Summary:
  Total Clusters:      2
  Total Groups:        2
  Total Items:         789
Link 10:PO5/0 (Down, 1 group)
  Group 51:PO5/0->Tu4000 (Up, 779 members)
    Prefix 10.0.0.0/16, Tu313, active
      Input label Tun hd, Output label PO0/0:773, FRR label Tu4000:773
    Prefix 10.0.0.0/16, Tu392, active
      Input label Tun hd, Output label PO0/0:775, FRR label Tu4000:775
    Prefix 10.0.0.0/16, Tu111, active
      Input label Tun hd, Output label PO0/0:16, FRR label Tu4000:16
    Prefix 10.0.0.0/16, Tu394, active
      Input label Tun hd, Output label PO0/0:774, FRR label Tu4000:774
```

Table 19 describes the significant fields when the **detail** keyword is used.

Table 19 show mpls traffic-eng fast-reroute database with detail Keyword Field Descriptions

Field	Description
Total Clusters	A cluster is the physical interface upon which Fast Reroute link protection has been enabled.
Total Groups	A group is a database record that associates the link-protected physical interface with a backup tunnel. A cluster (physical interface) therefore can have one or more groups. For example, the cluster Ethernet4/0/1 is protected by backup Tunnel1 and backup Tunnel2, and so has two groups.
Total Items	An item is a database record that associates a rewrite with a group. A group therefore can have one or more items.
Link 10:PO5/0 (Down, 1 group)	This describes a cluster (physical interface): • “10” is the interface’s unique IOS-assigned ID number. • “:” is followed by the interface’s short name. • Parentheses contain the operating state of the interface (Up or Down) and the number of groups associated with it.
Group 51:PO5/0->Tu4000 (Up, 779 members)	This describes a group: • “51” is the ID number of the backup interface. • “:” is followed by the group’s physical interface short name. • “->” is followed by the backup tunnel interface short name. • Parentheses contain the operating state of the tunnel interface (Up or Down) and the number of items—also called “members”— associated with it.

Related Commands

Command	Description
show mpls traffic-eng fast-reroute log reroutes	Displays contents of Fast Reroute event log.

show mpls traffic-eng tunnels

To display information about tunnels, use the **show mpls traffic-eng tunnels** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng tunnels
[**destination** *address*]
[**source-id** {*num* | *ipaddress* | *ipaddress num*}]
[**role** {**all** | **head** | **middle** | **tail** | **remote**}]
[**up** | **down**]
[**name** *name*]
[**suboptimal constraints** {**none** | **current** | **max**}]
[**interface in** *phys-intf*] [**interface out** *phys-intf* | [**interface** *phys-intf*
[**property** {**backup** | **fast-reroute**}]
[**brief** | **backup** | **protection**]

Syntax Description

destination *address*	(Optional) Restricts the display to tunnels destined to the specified IP address.
source-id	(Optional) Restricts the display to tunnels with a matching source IP address or tunnel number.
num	Tunnel number.
ipaddress	Source IP address.
ipaddress num	Source IP address and tunnel number.
role	(Optional) Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
all	Displays all tunnels.
head	Displays tunnels with their head at this router.
middle	Displays tunnels with a midpoint at this router.
tail	Displays tunnels with a tail at this router.
remote	Displays tunnels with their head at some other router; this is a combination of **middle** and **tail**.
up	(Optional) Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
down	(Optional) Displays tunnels that are down.
name *name*	(Optional) Displays tunnel with the specified string. The tunnel string is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel string is included in the signaling message so that it is available at all hops.
suboptimal constraints none	(Optional) Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the Interior Gateway Protocol's (IGP) shortest path.
suboptimal constraints current	(Optional) Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options. Selected tunnels would have a shorter path if they were reoptimized immediately.
suboptimal constraints max	(Optional) Displays information for the specified tunneling interface.

interface in *phys-intf*	(Optional) Displays information for the specified input interface.
interface out *phys-intf*	(Optional) Displays information for the specified output interface.
interface *phys-intf*	(Optional) Displays tunnels that use the specified interface as an input or output interface.
property backup	(Optional) Selects Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels being used to protect physical interfaces on this router. A tunnel configured to protect a link against failure is a backup tunnel and has the backup tunnel property.
property fast-reroute	(Optional) Selects Fast Reroute-protected MPLS TE tunnels originating, transmitting, or terminating on this router.
brief	(Optional) Specifies a format with one line per tunnel.
backup	(Optional) Displays information about the Fast Reroute protection provided by each tunnel selected by other options specified with this command. The information includes the physical interface protected by the tunnel, the number of TE label-switched packets (LSPs) (that is, tunnels) protected, and the bandwidth protected.
protection	(Optional) Displays information about the protection provided by each tunnel selected by other options specified with this command. The information includes whether protection is configured for the tunnel, the protection (if any) provided to the tunnel by this router, and the bandwidth protected.

Defaults

If you specify this command without any arguments or keywords, the command displays general information about each MPLS TE tunnel known to the router.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	Input and output interface information was added to the new **brief** form of the output. The **suboptimal** and **interface** keywords were added to the nonbrief format. The nonbrief, nonsummary formats contain the history of the LSP selection.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	The **property** and **protection** keywords were added. The command is supported on the Cisco 10000 series routers.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	The command displays output for a master tunnel.

Usage Guidelines

To select the tunnels for which information is displayed, use the **destination**, **source-id**, **role**, **up**, **down**, **name**, **suboptimal**, **interface,** and **property** keywords and options singly or combined.

To select the type of information displayed about the selected tunnels, use the **brief**, **backup**, or **protection** keyword.

Examples

The following is sample output from the **show mpls traffic-eng tunnels brief** command. It displays brief information about every MPLS TE tunnel known to the router.

```
Router# show mpls traffic-eng tunnels brief 500

Signalling Summary:
    LSP Tunnels Process:           running
    RSVP Process:                  running
    Forwarding:                    enabled
    Periodic reoptimization:       every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t1                        10.112.0.12      -         PO4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
Router_t3                        10.112.0.12      -         unknown   admin-down
Router_t1000                     10.110.0.10      -         unknown   up/down
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Table 20 describes the significant fields shown in the displays.

Table 20 show mpls traffic-eng tunnels Field Descriptions

Field	Description
LSP Tunnels Process	Status of the LSP tunnels process.
RSVP Process	Status of the Resource Reservation Protocol (RSVP) process.
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Schedule for periodic reoptimization (in seconds).
TUNNEL NAME	Name of the interface that is configured at the tunnel head.
DESTINATION	Identifier of the tailend router.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.
STATE/PROT	For tunnel heads, admin-down. up, or down. For nonheads, signaled.

The following is sample output from the **show mpls traffic-eng tunnels property backup brief** command. It displays brief information about all MPLS TE tunnels acting as Fast Reroute backup tunnels (**property backup**) for interfaces on the router.

```
Router# show mpls traffic-eng tunnels property backup brief

Signalling Summary:
    LSP Tunnels Process:            running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 2231 seconds
    Periodic FRR Promotion:         every 300 seconds, next in 131 seconds
    Periodic auto-bw collection:    disabled
TUNNEL NAME                      DESTINATION      UP IF     DOWN IF   STATE/PROT
Router_t2000                     10.110.0.10      -         PO4/0/1   up/up
Router_t2                        10.112.0.12      -         unknown   up/down
```

```
Router_t3                        10.112.0.12      -         unknown   admin-down
Displayed 3 (of 9) heads, 0 (of 1) midpoints, 0 (of 0) tails
```

The following is sample output from the **show mpls traffic-eng tunnels backup** command. This command selects every MPLS TE tunnel known to the router and displays information about the Fast Reroute protection each selected tunnels provides for interfaces on this router; the command does not generate output for tunnels that do not provide Fast Reroute protection of interfaces on this router.

```
Router# show mpls traffic-eng tunnels backup

Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 7.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

The following is sample output from the **show mpls traffic-eng tunnels property fast-reroute protection** command. This command selects every MPLS TE tunnel known to the router that was signaled as a Fast Reroute-protected LSP (**property fast-reroute**) and displays information about the protection this router provides each selected tunnel.

```
Router# show mpls traffic-eng tunnels property fast-reroute protection

Router_t1
  LSP Head, Tunnel1, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 25
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
      Backup Tu5711 to LSP nhop
        Tu5711: out i/f: PO1/1, label: implicit-null
      LSP signalling info:
        Original: out i/f: PO1/0, label: 12304, nhop: 10.1.1.7
        With FRR: out i/f: Tu5711, label: 12304
      LSP bw: 6000 kbps, Backup level: any unlimited, type: any pool
Router_t2
  LSP Head, Tunnel2, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 2
  Fast Reroute Protection: Requested
    Outbound: FRR Ready
      Backup Tu578 to LSP nhop
        Tu578: out i/f: PO1/0, label: 12306
      LSP signalling info:
        Original: out i/f: PO3/3, label: implicit-null, nhop: 10.3.3.8
        With FRR: out i/f: Tu578, label: implicit-null
      LSP bw: 100 kbps, Backup level: any unlimited, type: any pool
r9_t1
```

```
LSP Midpoint, signalled, connection up
Src 10.9.9.9, Dest 10.88.88.88, Instance 2347
Fast Reroute Protection: Requested
  Inbound:  FRR Inactive
    LSP signalling info:
      Original: in i/f: PO1/2, label: 12304, phop: 10.205.0.9
  Outbound: FRR Ready
    Backup Tu5711 to LSP nhop
      Tu5711: out i/f: PO1/1, label: implicit-null
    LSP signalling info:
      Original: out i/f: PO1/0, label: 12305, nhop: 10.1.1.7
      With FRR: out i/f: Tu5711, label: 12305
    LSP bw: 10 kbps, Backup level: any unlimited, type: any pool
```

Related Commands

Command	Description
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng tunnels (configuration)	Enables MPLS traffic engineering tunnel signaling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signaling on an interface.

show mpls traffic-eng tunnels summary

To display summary information about tunnels, use the **show mpls traffic-eng tunnels summary** command in user EXEC or privileged EXEC mode.

show mpls traffic-eng tunnels summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(10)ST	This command was integrated into Cisco IOS Release 12.0(10)ST.
12.0(22)S	The command output was updated to display periodic Fast Reroute information. The command is supported on the Cisco 10000 series ESRs.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show mpls traffic-eng tunnels summary** command**:**

```
Router# show mpls traffic-eng tunnels summary

Signalling Summary:
  LSP Tunnels Process:          running
  RSVP Process:                 running
  Forwarding:                   enabled
  Head: 4 interfaces, 3 active signalling attempts, 3 established
     5 activations, 2 deactivations
  Midpoints: 1, Tails: 0
  Periodic reoptimization:     every 3600 seconds, next in 2778 seconds
  Periodic fastreroute:        every 300 seconds, next in 168 seconds
  Periodic auto-bw collection: every 300 seconds, next in 78 seconds
```

Table 21 describes the significant fields shown in the display.

Table 21 show mpls traffic-eng tunnels summary Field Descriptions

Field	Description
LSP Tunnels Process	Multiprotocol Label Switching (MPLS) traffic engineering has or has not been enabled.
RSVP Process	Resource Reservation Protocol (RSVP) has or has not been enabled. (This feature is enabled as a consequence of MPLS traffic engineering being enabled.)

Table 21 show mpls traffic-eng tunnels summary Field Descriptions (continued)

Field	Description
Forwarding	Indicates whether appropriate forwarding is enabled. (Appropriate forwarding on a router is Cisco Express Forwarding switching.)
Head	Summary information about tunnel heads at this device.
Interfaces	Number of MPLS traffic engineering tunnel interfaces.
Active signalling attempts	LSPs currently successfully signaled or being signaled.
Established	LSPs currently signaled.
activations	Signaling attempts initiated.
deactivations	Signaling attempts terminated.
Periodic reoptimization	Frequency of periodic reoptimization and time (in seconds) until the next periodic reoptimization.
Periodic fastreroute	Frequency that scanning occurs to determine if link-state packets (LSPs) should be promoted to better backup tunnels, and time (in seconds) until the next scanning.
Periodic auto-bw collection	Frequency of automatic bandwidth collection and time left (in seconds) until the next collection.

Related Commands

Command	Description
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng tunnels (configuration)	Enables MPLS traffic engineering tunnel signaling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signaling on an interface.

tunnel mpls traffic-eng backup-bw

To specify what types of label-switched paths (LSPs) can use a backup tunnel, whether the backup tunnel should provide bandwidth protection, and if so, how much, use the **tunnel mpls traffic-eng backup-bw** command in interface configuration mode.

tunnel mpls traffic-eng backup-bw {*bandwidth* | [**sub-pool** {*bandwidth* | **Unlimited**}] [**global-pool** {*bandwidth* | **Unlimited**}]}

Syntax Description

global-pool	Only LSPs using bandwidth from the global pool can use the backup tunnel.
sub-pool	Only LSPs using bandwidth from the subpool can use the backup tunnel.
bandwidth	Amount of bandwidth this backup tunnel can protect. The router limits the LSPs that can use this backup tunnel so that the sum of the bandwidth of the LSPs does not exceed the specified amount of bandwidth. If there are multiple backup tunnels, the router will use the best-fit algorithm.
Unlimited	Backup tunnel does not provide bandwidth protection. Any number of LSPs can use the backup tunnel, regardless of their bandwidth.

Command Default

If neither **sub-pool** nor **global-pool** is entered, it is assumed that any LSP (those using bandwidth from the subpool or global pool) can use this backup tunnel.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If both **sub-pool** and **global-pool** are specified, **sub-pool** must be specified first on the command line. For example, **tunnel mpls traffic-eng backup-bw sub-pool 100 global-pool Unlimited** is legal, but it is not legal to specify **tunnel mpls traffic-eng backup-bw global-pool Unlimited sub-pool 100**.

To limit both subpool and global pool LSPs, enter **tunnel mpls traffic-eng backup-bw sub-pool** *bandwidth* **global-pool** *bandwidth*.

If subpool is **Unlimited**, global pool cannot also be **Unlimited**. Entering such a command (**tunnel mpls traffic-eng backup-bw sub-pool Unlimited global-pool Unlimited**) would be the same as entering nothing at all because it is the default behavior.

Examples

In the following example, backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. The backup tunnel does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
Router(config)# interface Tunnel1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited
Router(config-if)# end

Router(config)# interface Tunnel2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
Router(config-if)# end
```

Related Commands

Command	Description
mpls traffic-eng backup path	Assigns one or more backup tunnels to a protected interface.

tunnel mpls traffic-eng fast-reroute

To enable a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel to use an established backup tunnel in the event of a link or node failure, use the **tunnel mpls traffic-eng fast-reroute** command in interface configuration mode. To disable this capability, use the **no** form of this command.

tunnel mpls traffic-eng fast-reroute [**bw-protect**]

no tunnel mpls traffic-eng fast-reroute

Syntax Description

bw-protect	(Optional) Sets the “bandwidth protection desired” bit so that backup bandwidth protection is enabled.

Command Default

There is no backup bandwidth protection.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(08)ST	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18)SXD	This command was implemented on the Catalyst 6000 series with the SUP720 processor.
12.0(29)S	The **bw-protect** keyword was added.
12.2(28)SB	This command was implemented on the Cisco 10000(PRE-2) router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you specify the **bw-protect** keyword, all path messages for the tunnel’s label-switched path (LSP) are sent with the bandwidth protection bit set.

After you enter the command, with or without the **bw-protect** keyword, the requested action or change propagates quickly along all hops of the LSP. Midpoint routers that are point of local repairs (PLRs) for the LSP take the appropriate action based on whether the bit was just set or cleared. If the bit was just set or cleared, a new backup tunnel selection happens for the LSP because it now has a higher or lower priority in the backup tunnel selection process.

To unconfigure only backup bandwidth protection, enter the **tunnel mpls traffic-eng fast-reroute** command.

To disable an MPLS TE tunnel from using an established backup tunnel in the event of a link or node failure, enter the **no** form of the command.

Examples

In the following example, backup bandwidth protection is enabled:

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
```

Related Commands

Command	Description
mpls traffic-eng backup-path tunnel	Configures the interface to use a backup tunnel in the event of a detected failure on the interface.
mpls traffic-eng fast-reroute backup-prot-preemption	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted.
show tunnel mpls traffic-eng fast-reroute	Displays information about fast reroute for MPLS traffic engineering.

Feature Information for MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

Table 22 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/cfn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 22 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

Table 22 Feature Information for MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection

Feature Name	Releases	Feature Information
MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection	12.0(10)ST 12.0(16)ST 12.0(22)S 12.0(23)S 12.0(24)S 12.0(29)S 12.2(33)SRA	The MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection feature supports link protection (backup tunnels that bypass only a single link of the label-switched path (LSP), node protection (backup tunnels that bypass next-hop nodes along LSPs), and the following FRR features: backup tunnel support, backup bandwidth protection, and RSVP Hellos. In 12.0(10)ST, the Fast Reroute Link Protection feature was introduced. In 12.0(16)ST, Link Protection for Cisco series 7200 and 7500 platforms was added. In 12.0(22)S, Fast Reroute enhancements were added. In 12.0(23)S, the **show mpls traffic-eng fast-reroute database** command was revised. In 12.0(24)S, support for the Cisco 10720 Internet router and the Cisco 12000 series router engine 3 was added. In 12.0(29)S, backup bandwidth protection was added. In 12.2(33)SRA, the commands were integrated into this release.

Glossary

backup bandwidth—The usage of NHOP and NNHOP backup tunnels to provide bandwidth protection for rerouted LSPs.

backup tunnel—An MPLS TE tunnel used to protect other (primary) tunnels' traffic when a link or node failure occurs.

bandwidth—The available traffic capacity of a link.

Cisco Express Forwarding—A means for accelerating the forwarding of packets within a router, by storing route lookup.

enterprise network—A large and diverse network connecting most major points in a company or other organization.

Fast Reroute—Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the headend.

global pool—The total bandwidth allocated to an MPLS traffic engineering link or node.

headend—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

hop—Passage of a data packet between two network nodes (for example, between two routers).

instance—A Hello instance implements the RSVP Hello extensions for a given router interface address and remote IP address. Active Hello instances periodically send Hello Request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

interface—A network connection.

Intermediate System-to-Intermediate System—IS-IS. Link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

link—A point-to-point connection between adjacent nodes. There can be more than one link between adjacent nodes. A link is a network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

limited backup bandwidth—Backup tunnels that provide bandwidth protection.

load balancing—A configuration technique that shifts traffic to an alternative link if a certain threshold is exceeded on the primary link. Load balancing is similar to redundancy in that if an event causes traffic to shift directions, alternative equipment must be present in the configuration. In load balancing, the alternative equipment is not necessarily redundant equipment that operates only in the event of a failure.

LSP—label-switched path. A connection between two routers in which MPLS forwards the packets.

merge point—The backup tunnel's tail.

MPLS—Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

MPLS global label allocation—There is one label space for all interfaces in the router. For example, label 100 coming in one interface is treated the same as label 100 coming in a different interface.

NHOP—next hop. The next downstream node along an LSP's path.

NHOP backup tunnel—next-hop backup tunnel. Backup tunnel terminating at the LSP's next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link, and is used to protect primary LSPs that were using this link before the failure.

NNHOP—next-next hop. The node after the next downstream node along an LSP's path.

NNHOP backup tunnel—next-next-hop backup tunnel. Backup tunnel terminating at the LSP's next-next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link and/or node, and is used to protect primary LSPs that were using this link or node before the failure.

node—Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network. Nodes can be processors, controllers, or workstations.

OSPF—Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

primary LSP—The last LSP originally signaled over the protected interface before the failure. The primary LSP is the LSP before the failure.

primary tunnel—Tunnel whose LSP may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

promotion—Conditions, such as a new backup tunnel comes up, cause a reevaluation of a backup tunnel that was chosen for an LSP. If the reevaluation is successful, it is called a promotion.

protected interface—An interface that has one or more backup tunnels associated with it.

redundancy—The duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

RSVP—Resource Reservation Protocol. A protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

scalability—An indicator showing how quickly some measure of resource usage increases as a network gets larger.

SRLG—shared risk link group. Sets of links that are likely to go down together.

state—Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

sub-pool—The more restrictive bandwidth in an MPLS traffic engineering link or node. The subpool is a portion of the link or node's overall global pool bandwidth.

tailend—The router upon which an LSP is terminated. This is the last router in the LSP's path.

topology—The physical arrangement of network nodes and media within an enterprise networking structure.

tunnel—Secure communications path between two peers, such as two routers.

unlimited backup bandwidth—Backup tunnels that provide no bandwidth (best-effort) protection (that is, they provide best-effort protection).

Note

See *Internetworking Terms and Acronyms* for terms not included in this glossary.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.