

MPLS Traffic Engineering--Fast Reroute MIB

The MPLS Traffic Engineering--Fast Reroute MIB provides Simple Network Management Protocol (SNMP)-based network management of the Multiprotocol Label Switching (MPLS) Fast Reroute (FRR) feature in Cisco software.

The Fast Reroute MIB has the following features:

- Notifications can be created and queued.
- Command-line interface (CLI) commands enable notifications, and specify the IP address to where the notifications will be sent.
- The configuration of the notifications can be written into nonvolatile memory.

The MIB includes objects describing features within MPLS FRR, and it includes the following tables:

- cmplsFrrConstTable
- cmplsFrrLogTable
- cmplsFrrFacRouteDBTable

The MIB also includes scalar objects (that is, objects that are not in a table). For more information, see theMPLS Traffic Engineering--Fast Reroute MIB, on page 1 .

- Prerequisites for the MPLS Traffic Engineering--Fast Reroute MIB, on page 1
- Restrictions for the MPLS Traffic Engineering--Fast Reroute MIB, on page 2
- Information About the MPLS Traffic Engineering--Fast Reroute MIB, on page 2
- How to Configure the MPLS Traffic Engineering--Fast Reroute MIB, on page 8
- Configuration Examples for the MPLS Traffic Engineering--Fast Reroute MIB, on page 13
- Additional References, on page 14
- Feature Information for MPLS Traffic Engineering--Fast Reroute MIB, on page 15
- Glossary, on page 15

Prerequisites for the MPLS Traffic Engineering--Fast Reroute MIB

- The network must support the Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) protocol.

- The SNMP is installed and enabled on the label switch routers (LSRs).
- MPLS is enabled globally on each LSR.
- Cisco Express Forwarding is enabled on the LSRs.
- Traffic engineering (TE) tunnels are enabled.
- MPLS FRR is enabled on one of the TE tunnels.
- The Resource Reservation Protocol (RSVP) is enabled.

Restrictions for the MPLS Traffic Engineering--Fast Reroute MIB

- The implementation of the FRR MIB is limited to read-only (RO) permission for MIB objects.
- The following tables are not implemented:
  - mplsFrrOne2OnePlrTable
  - mplsFrrDetourTable.

Information About the MPLS Traffic Engineering--Fast Reroute MIB

Feature Design of the MPLS Traffic Engineering--Fast Reroute MIB

The FRR MIB enables standard, SNMP-based network management of FRR in Cisco software. This capability requires that SNMP agent code executes on a designated network management station (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MIB.

The FRR MIB is based on the Internet Engineering Task Force (IETF) draft MIB specification *draft-ietf-mpls-fastreroute-mib-02.txt* . The IETF draft MIB, which undergoes revisions periodically, is evolving toward becoming a standard. The Cisco implementation of the FRR MIB is expected to track the evolution of the IETF draft MIB, and may change accordingly.

Slight differences between the IETF draft MIB and the implementation of FRR within Cisco software require some minor translations between the FRR MIB objects and the internal data structures of Cisco software. These translations are accomplished by the SNMP agent, which runs in the background on the NMS workstation as a low priority process and provides a management interface to Cisco software.

You can use an SNMP agent to access FRR MIB objects using standard SNMP GET operations. All the objects in the FRR MIB follow the conventions defined in the IETF draft MIB.

Functional Structure of the MPLS Traffic Engineering--Fast Reroute MIB

The SNMP agent code supporting the FRR MIB follows the existing model for such code in Cisco software and is, in part, generated by the Cisco tool set, based on the MIB source code. The basis for the generated code is the Cisco version of the FRR MIB CISCO-ietf-frr-mib.

The SNMP agent code, which has a layered structure that is common to MIB support code in Cisco software, consists of the following layers:

- Platform-independent layer--This layer is generated primarily by the MIB development Cisco tool set and incorporates platform- and implementation-independent functions. These functions handle SNMP standard functionality in the context of the specific MIB. This layer handles indexes and range or enumeration value checks for GET, GET-NEXT, and SET SNMP operations. A function is generated for each SNMP table or group of objects. This layer calls into the next layer.
- Application interface layer--The Cisco tool set generates the function names and template code for MIB objects.
- Application-specific layer--This layer provides the mechanism for retrieving relevant data from the managed application layer. It includes an entry point function for each table. This function calls two other functions; one that searches the TE tunnel database that RSVP maintains for the relevant data according to the indexes, and another function that fills the data into the structure.
- Managed application layer--This layer includes all the structures and mechanisms, and is managed by the MIB.

System Flow of SNMP Protocol Requests and Response Messages

All SNMP protocol requests and response messages are ultimately handled by the SNMP master agent. When such a message is received on a router, the master agent parses the requests and identifies the MIB to which the request refers. The master agent then queries the subagent responsible for the MIB with a GET, GET-NEXT, or SET request. The FRR MIB subagent retrieves the appropriate data, and returns it to the master agent. The master agent is then responsible for returning an SNMP response to the NMS. All queries occur within the IP SNMP Cisco software process, which runs as a low priority task.

FRR MIB Scalar Objects

Scalar objects are objects that are not in tables. A scalar object has one instance (that is, one occurrence).

The table below describes the FRR MIB scalar objects.

Table 1: Scalar Objects

MIB Object	Function
cmplsFrrDetourIncoming	Number of detour link-state packets (LSPs) entering the device. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrDetourOutgoing	Number of detour LSPs leaving the device. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrDetourOriginating	Number of detour LSPs originating from the device. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).

MIB Object	Function
cmplsFrrSwitchover	Number of tunnels that are being backed up because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrNumOfConfIfs	Number of MPLS interfaces FRR configured for protection; 0 indicates that LSPs traversing any interface can be protected.
cmplsFrrActProtectedIfs	Number of interfaces FRR is protecting because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrConfProtectingTuns	Number of backup Fast Reroute-protected tunnels configured because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrActProtectedTuns	Number of tunnels protected by the Fast Reroute feature. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrActProtectedLSPs	Number of LSPs that FRR is protecting. If cmplsFrrConstProtectionMethod is set to facilityBackup(1), this object returns 0.
cmplsFrrConstProtectionMethod	This object always returns facilityBackup(1) because Cisco software supports only the facility backup protection method.
cmplsFrrNotifsEnabled	A value that indicates whether FRR notifications defined in this MIB are enabled or disabled. This object returns True(1) for enabled, or False(2) for disabled. The default is that notifications are disabled.
cmplsFrrLogTableMaxEntries	Maximum number of entries allowed in the FRR log table.
cmplsFrrLogTableCurrEntries	Current number of entries in the FRR log table. This object always returns 0.
cmplsFrrNotifMaxRate	Maximum interval rate between FRR MIB notifications. This object always returns 0.

FRR MIB Notification Generation Events

Notifications are issued after particular FRR events occur.

When you enable FRR MIB notification functionality by issuing the **snmp-server enable traps mpls fast-reroute** command, FRR events generate notification messages that are sent to a designated NMS in the network to signal the occurrence of specific events in Cisco software.

The FRR MIB objects involved in FRR status transitions and event notifications include cmplsFrrProtected. This message is sent to an NMS if there is a major TE tunnel change (that is, fast rerouting of TE tunnels).

FRR MIB Notification Specification

Notifications are issued after particular FRR events occur.

Each FRR notification has a generic type identifier and an enterprise-specific type identifier for identifying the notification type. The generic type for all FRR notifications is “enterprise Specific” because this is not one of the generic notification types defined for SNMP. The enterprise-specific type is 1 for cmplsFrrProtected.

Each notification contains the following objects from the FRR MIB so that the FRR tunnel can be easily identified:

- cmplsFrrConstNumProtectingTunOnIf
- cmplsFrrConstNumProtectedTunOnIf
- cmplsFrrConstBandwidth

Upon being invoked, the appropriate FRR interface indexes have already been retrieved by existing FRR code. The FRR interfaces are then used to fill in data for the three objects included in the notification.

FRR MIB Notification Monitoring

Notifications are issued after particular FRR events occur.

When FRR MIB notifications are enabled (see the **snmp-server enable traps** command), notification messages relating to specific FRR events within Cisco software are generated and sent to a specified NMS in the network. Any utility that supports SNMPv1 or SNPv2 notifications can receive notification messages.

To monitor FRR MIB notifications, log in to an NMS that supports a utility that displays SNMP notifications, and start the display utility.

MIB Tables in the MPLS Traffic Engineering--Fast Reroute MIB

The FRR MIB consists of the following tables:

The tables access various data structures to obtain information regarding detours, the FRR database, and logging.

cmplsFrrConstTable

cmplsFrrConstTable displays the configuration of an FRR-enabled tunnel and the characteristics of its accompanying backup tunnels. For each protected tunnel, there can be multiple backup tunnels.

The table is indexed by the following:

- cmplsFrrConstIfIndex
- cmplsFrrConstTunnelIndex
- cmplsFrrConstTunnelInstance

The table below describes the MIB objects for cmplsFrrConstTable.

Table 2: cmplsFrrConstTable Objects

MIB Object	Function
cmplsFrrConstIfIndex	Uniquely identifies an interface on which FRR is configured. If an index has a value of 0, the configuration applies to all interfaces on the device on which the FRR feature can operate.
cmplsFrrConstTunnelIndex	Tunnel for which FRR is requested.
cmplsFrrConstTunnelInstance	Tunnel for which FRR is requested. The value always is 0 because only tunnel heads are represented, and tunnel heads have an instance value of 0.

MIB Object	Function
cmplsFrrConstSetupPrio	Setup priority of the backup tunnel.
cmplsFrrConstHoldingPrio	Holding priority of the backup tunnel.
cmplsFrrConstInclAnyAffinity	Attribute bits that must be set for the tunnel to traverse a link.
cmplsFrrConstInclAllAffinity	Attribute bits that must not be set for the tunnel to traverse a link.
cmplsFrrConstExclAllAffinity	A link satisfies the exclude-all constraint only if the link contains none of the administrative groups specified in the constraint.
cmplsFrrConstHopLimit	The maximum number of hops that the backup tunnel can traverse.
cmplsFrrConstBandwidth	The bandwidth of the backup tunnels for this tunnel, in thousands of bits per second (kbps).
cmplsFrrConstRowStatus	Creates, modifies, and deletes a row in this table.

cmplsFrrLogTable

cmplsFrrLogTable is indexed by the object cmplsFrrLogIndex. The index corresponds to a log entry in the FRR feature's **show mpls traffic-eng fast-reroute log reroutes** command. That **show** command stores up to 32 entries at a time. If entries are added, the oldest entry is overwritten with new log information.

cmplsFrrLogTable can store up to 32 entries at a time, overwriting older entries as newer ones are added. The index cmplsFrrLogIndex is incremented to give each log table entry of the MIB a unique index value. Therefore, it is possible to have indexes greater than 32 even though only 32 entries are displaying.

The table below describes the MIB objects for cmplsFrrLogTable.

Table 3: cmplsFrrLogTable Objects

MIB Object	Function
cmplsFrrLogIndex	Number of the FRR event.
cmplsFrrLogEventTime	Number of milliseconds that elapsed from bootstrap time to the time that the event occurred.
cmplsFrrLogInterface	Identifies the interface that was affected by this FRR event. The value can be set to 0 if mplsFrrConstProtectionMethod is set to oneToOneBackup(0).
cmplsFrrLogEventType	The type of FRR event that occurred. The object returns Protected or Other.
cmplsFrrLogEventDuration	Duration of the event, in milliseconds.
cmplsFrrLogEventReasonString	Implementation-specific explanation of the event. The object returns interface down event or interface other event.

cmplsFrrFacRouteDBTable

The following indexes specify which interface and tunnel are being protected by the FRR feature:

- cmplsFrrFacRouteProtectedIfIndex

- cmplsFrrFacRouteProtectedTunIndex

The following indexes specify the backup tunnel that provides protection to the protected tunnel:

- cmplsFrrFacRouteProtectedIfIndex
- cmplsFrrFacRouteProtectingTunIndex
- cmplsFrrFacRouteProtectedTunIndex
- cmplsFrrFacRouteProtectedTunInstance
- cmplsFrrFacRouteProtectedTunIngressLSRId
- cmplsFrrFacRouteProtectedTunEgressLSRId

This version of the MIB will attempt to leverage the work already done for the MPLS TE MIB because it contains similar lookup functions for TE tunnels.

The table below describes the MIB objects for cmplsFrrFacRouteDBTable.

Table 4: cmplsFrrFacRouteDBTable Objects

MIB Object	Function
cmplsFrrFacRouteProtectedIfIndex	Interface configured for FRR protection.
cmplsFrrFacRouteProtectingTunIndex	The tunnel number of the protecting (backup) tunnel.
cmplsFrrFacRouteProtectedTunIndex	The mplsTunnelEntry primary index for the tunnel head interface designated to protect the interface specified in mplsFrrFacRouteIfProtIdx (and all the tunnels using this interface).
cmplsFrrFacRouteProtectedTunInstance	An mplsTunnelEntry that is being protected by FRR. An instance uniquely identifies a tunnel.
cmplsFrrFacRouteProtectedTunIngressLSRId	Inbound label for the backup LSR.
cmplsFrrFacRouteProtectedTunEgressLSRId	Outbound label for the backup LSR.
cmplsFrrFacRouteProtectedTunStatus	State of the protected tunnel. Valid values are: • active--Tunnel label has been placed in the Label Forwarding Information Base (LFIB) and is ready to be applied to incoming packets. • ready--Tunnel's label entry has been created, but is not in the LFIB. • partial--Tunnel's label entry has not been fully created.
cmplsFrrFacRouteProtectingTunResvBw	Amount of bandwidth, in megabytes per second, that is reserved by the backup tunnel.
cmplsFrrFacRouteProtectingTunProtectionType	Type of protection: 0 designates link protection; 1 designates node protection.

How to Configure the MPLS Traffic Engineering--Fast Reroute MIB

Enabling the SNMP Agent for FRR MIB Notifications

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro**] [*access-list-number*]
5. **snmp-server enable traps mpls fast-reroute protected**
6. **end**
7. **write memory**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** `Router# show running-config`	Displays the running configuration of the router to determine if an SNMP agent is already running on the device. If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify or change the information.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**snmp-server community** *string* [**view** *view-name*] [**ro**] [*access-list-number*] **Example:** `Router(config)# snmp-server community public ro`	Configures read-only (ro) SNMP community strings for the FRR MIB.

	Command or Action	Purpose
Step 5	**snmp-server enable traps mpls fast-reroute protected** **Example:** `Router(config)# snmp-server enable traps mpls fast-reroute protected`	Enables Fast Reroute traps.
Step 6	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.
Step 7	**write memory** **Example:** `Router# write memory`	Writes the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.

Enabling Cisco Express Forwarding

SUMMARY STEPS

1. **enable**
2. **configure teminal**
3. **ip cef distributed**
4. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure teminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef distributed** **Example:** `Router(config)# ip cef distributed`	Enables distributed Cisco Express Forwarding.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Enabling TE Tunnels

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **mpls traffic-eng tunnels**
5. **interface** *type slot/subslot/port*[**.***subinterface*]
6. **mpls traffic-eng tunnels**
7. **end**

DETAILED STEPS

Procedure

	Command or Action	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	**ip cef** **Example:** `Router(config)# ip cef`	Enables standard Cisco Express Forwarding operations.
Step 4	**mpls traffic-eng tunnels** **Example:** `Router(config)# mpls traffic-eng tunnels`	Enables the MPLS TE tunnel feature on a device.
Step 5	**interface** *type slot/subslot/port*[**.***subinterface*] **Example:**	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
	`Router(config)# interface POS1/0/0`	
Step 6	**mpls traffic-eng tunnels** **Example:** `Router(config-if)# mpls traffic-eng tunnels`	Enables the MPLS TE tunnel feature on an interface.
Step 7	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Enabling MPLS FRR on Each TE Tunnel

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/subslot/port*[**.***subinterface*]
4. **tunnel mode mpls traffic-eng**
5. **tunnel mpls traffic-eng fast-reroute**
6. **end**

DETAILED STEPS

Procedure

	Command or Action	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/subslot/port*[**.***subinterface*] **Example:** `Router(config)# interface POS1/0/0`	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**tunnel mode mpls traffic-eng** **Example:** `Router(config-if)# tunnel mode mpls traffic-eng`	Sets the mode of a tunnel to MPLS for traffic engineering.
Step 5	**tunnel mpls traffic-eng fast-reroute** **Example:** `Router(config-if)# tunnel mpls traffic-eng fast-reroute`	Enables Fast Reroute on the TE tunnel being protected.
Step 6	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Enabling a Backup Tunnel on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *typeslot/subslot/port*[**.***subinterface*]
4. **mpls traffic-eng backup-path tunnel** *interface*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	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** *typeslot/subslot/port*[**.***subinterface*] **Example:**	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
	`Router(config)# interface POS1/0/0`	
Step 4	**mpls traffic-eng backup-path tunnel** *interface* **Example:** `Router(config-if)# mpls traffic-eng backup-path tunnel1`	Enables a backup tunnel on a specified interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits to privileged EXEC mode.

Configuration Examples for the MPLS Traffic Engineering--Fast Reroute MIB

Example Enabling an SNMP Agent on a Host NMS

```
enable
 show running-config
 configure terminal
 snmp-server community public ro
 snmp-server enable traps mpls fast-reroute protected
 end
 write memory
```

Example Enabling Cisco Express Forwarding

```
enable
 configure terminal
 ip cef
 end
```

Example Enabling TE Tunnels

```
enable
 configure terminal
 ip cef
 mpls traffic-eng tunnels
 interface FastEthernet1/0/0
 mpls traffic-eng tunnels
 end
```

Example Enabling MPLS FRR on Each TE Tunnel

```
enable
 configure terminal
 interface POS1/0/0
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng fast-reroute
 end
```

Example Enabling a Backup Tunnel on an Interface

```
enable
 configure terminal
 interface POS1/0/0
 mpls traffic-eng backup-path tunnel1
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Description of commands associated with MPLS and MPLS applications	*Multiprotocol Label Switching Command Reference*
SNMP agent support for the MPLS Traffic Engineering MIB	MPLS Traffic Engineering MIB
Fast Reroute	MPLS Traffic Engineering: Fast Reroute Link and Node Protection

Standards

Standard	Title
MPLS-FRR-MIB	*draft-ietf-mpls-fastreroute-mib-02.txt*

MIBs

MIB	MIBs Link
MPLS Traffic Engineering (TE) MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for MPLS Traffic Engineering--Fast Reroute MIB

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

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

Table 5: Feature Information for MPLS Traffic Engineering--Fast Reroute MIB

Feature Name	Releases	Feature Information
MPLS Embedded Management--MPLS Fast Reroute MIB (IETF draft v01)	Cisco IOS XE Release 2.3	The Fast Reroute MIB provides SNMP-based network management of the Multiprotocol Label Switching (MPLS) Fast Reroute (FRR) feature.

Glossary

FEC—Forwarding Equivalence Class. A set of packets that can be handled equivalently for forwarding purposes and are thus suitable for binding to a single label. Examples include the set of packets destined for one address prefix and any flow.

flow—Generally, a set of packets traveling between a pair of hosts, or a pair of transport protocol ports on a pair of hosts. For example, packets with the same source address, source port, destination address, and destination port might be considered a flow.

A flow is also a stream of data traveling between two endpoints across a network (for example, from one LAN station to another). Multiple flows can be transmitted on a single circuit.

fragmentation—Process of breaking a packet into smaller units when transmitting over a network medium that cannot support the original size of the packet.

ICMP— Internet Control Message Protocol. A network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. It is documented in RFC 792.

LFIB—label forwarding information base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

localhost—A name that represents the host name of a device. The localhost uses the reserved loopback IP address 127.0.0.1.

LSP—label switched path. A connection between two devices that uses MPLS to carry the packets.

LSPV—Label Switched Path Verification. An LSP Ping subprocess that encodes and decodes MPLS echo requests and replies; interfaces with IP, MPLS, and AToM switching for sending and receiving MPLS echo requests and replies; and, at the MPLS echo request originator device, maintains a database of outstanding echo requests for which echo responses have not been received.

MPLS router alert label—An MPLS label of 1. An MPLS packet with a router alert label is redirected by the device to the Route Processor (PR) processing level for handling. This allows these packets to bypass any forwarding failures in hardware routing tables.

MRU—maximum receive unit. Maximum size, in bytes, of a labeled packet that can be forwarded through an LSP.

MTU—maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

punt—Redirect packets with a router alert from the line card or interface to Route Processor (RP) level processing for handling.

PW—pseudowire. A mechanism that carries the essential elements of an emulated circuit from one provider edge (PE) device to another PE device over a packet-switched network.

RP—Route Processor. Processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the device. It is sometimes called a supervisory processor.

RSVP—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. Is is also known as Resource Reservation Setup Protocol.

UDP—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.