7750 SR OS MPLS Guide

Software Version: 7750 SR OS 8.0 r4
July 2010
Document Part Number: 93-0075-07-02

Table of Contents

Label Distribution Protocol

List of Tables

List of Figures

MPLS and RSVP

Label Distribution Protocol

Preface

About This Guide

This guide describes the services and protocol support provided by the 7750 SR OS and presents examples to configure and implement MPLS, RSVP, and LDP protocols.

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This manual is intended for network administrators who are responsible for configuring the 7750 SR routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols and concepts described in this manual include the following:

- Multiprotocol Label Switching (MPLS)
- Resource Reservation Protocol (RSVP)
- Label Distribution Protocol (LDP)

List of Technical Publications

The 7750 SR documentation set is composed of the following books:

- 7750 SR OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.
- 7750 SR OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.
- 7750 SR OS Interface Configuration Guide

This guide describes card, Media Dependent Adapter (MDA), MCM (MDA Carrier Module), CMA (Compact Media Adapter), and port provisioning.

- 7750 SR OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering, and VRRP, and Cflowd and Cflowd.

- 7750 SR OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for RIP, OSPF, IS-IS, Multicast, BGP, Multicast, BGP, and route policies.

- 7750 SR OS MPLS Guide

  This guide describes how to configure Multiprotocol Label Switching (MPLS), Resource Reservation Protocol (RSVP), and Label Distribution Protocol (LDP).

- 7750 SR OS Services Guide

  This guide describes how to configure service parameters such as service distribution points (SDPs), customer information, and user services.

- 7750 SR OS OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.

- 7750 SR OS Triple Play Guide

  This guide describes Triple Play services and support provided by the 7750 SR7450 ESS7710 SR and presents examples to configure and implement various protocols and services.

- 7750 SR OS Quality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.

- OS Multi-Service ISA Guide

  This guide describes services provided by integrated service adapters such as Application Assurance, IPSec, ad insertion (ADI) and Network Address Translation (NAT).

Technical Support

If you purchased a service agreement for your 7750 SR-series router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center:

Web: http://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml

GETTING STARTED

In This Chapter

This chapter provides process flow information to configure MPLS, RSVP, and LDP protocols.

Alcatel-Lucent 7750 SR-Series Router Configuration Process

Table 1 lists the tasks necessary to configure MPLS applications functions.

This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration Process

Area	Task	Chapter
Protocol configuration	Configure MPLS protocols:	
	• MPLS	MPLS on page 19
	• RSVP	RSVP on page 42
	• LDP	Label Distribution Protocol on page 271
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 389

MPLS and RSVP

In This Chapter

This chapter provides information to configure MPLS and RSVP.

MPLS

Multiprotocol Label Switching (MPLS) is a label switching technology that provides the ability to set up connection-oriented paths over a connectionless IP network. MPLS facilitates network traffic flow and provides a mechanism to engineer network traffic patterns independently from routing tables. MPLS sets up a specific path for a sequence of packets. The packets are identified by a label inserted into each packet. MPLS is not enabled by default and must be explicitly enabled.

MPLS is independent of any routing protocol but is considered multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols.

MPLS Label Stack

MPLS requires a set of procedures to enhance network layer packets with label stacks which thereby turns them into labeled packets. Routers that support MPLS are known as Label Switching Routers (LSRs). In order to transmit a labeled packet on a particular data link, an LSR must support the encoding technique which, when given a label stack and a network layer packet, produces a labeled packet.

In MPLS, packets can carry not just one label, but a set of labels in a stack. An LSR can swap the label at the top of the stack, pop the stack, or swap the label and push one or more labels into the stack. The processing of a labeled packet is completely independent of the level of hierarchy. The processing is always based on the top label, without regard for the possibility that some number of other labels may have been above it in the past, or that some number of other labels may be below it at present.

As described in RFC 3032, *MPLS Label Stack Encoding*, the label stack is represented as a sequence of label stack entries. Each label stack entry is represented by 4 octets. Figure 1 displays the label placement in a packet.

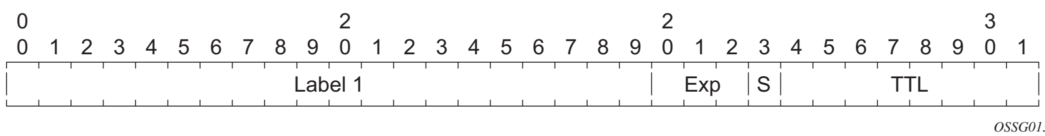

Figure 1: Label Placement

Table 2: Packet/Label Field Description

Field	Description
Label	This 20-bit field carries the actual value (unstructured) of the label.
Exp	This 3-bit field is reserved for experimental use. It is currently used for Class of Service (CoS).
S	This bit is set to 1 for the last entry (bottom) in the label stack, and 0 for all other label stack entries.
TTL	This 8-bit field is used to encode a TTL value.

A stack can carry several labels, organized in a last in/first out order. The top of the label stack appears first in the packet and the bottom of the stack appears last (Figure 2).

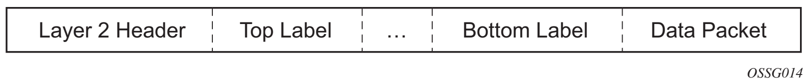

Figure 2: Label Packet Placement

The label value at the top of the stack is looked up when a labeled packet is received. A successful lookup reveals:

- The next hop where the packet is to be forwarded.
- The operation to be performed on the label stack before forwarding.

In addition, the lookup may reveal outgoing data link encapsulation and other information needed to properly forward the packet.

An empty label stack can be thought of as an unlabeled packet. An empty label stack has zero (0) depth. The label at the bottom of the stack is referred to as the Level 1 label. The label above it (if it exists) is the Level 2 label, and so on. The label at the top of the stack is referred to as the Level *m* label.

Labeled packet processing is independent of the level of hierarchy. Processing is always based on the top label in the stack which includes information about the operations to perform on the packet's label stack.

Label Values

Packets travelling along an LSP (see Label Switching Routers on page 23) are identified by its label, the 20-bit, unsigned integer. The range is 0 through 1,048,575. Label values 0-15 are reserved and are defined below as follows:

- A value of 0 represents the IPv4 Explicit NULL Label. This Label value is legal only at the bottom of the Label stack. It indicates that the Label stack must be popped, and the packet forwarding must be based on the IPv4 header.
- A value of 1 represents the router alert Label. This Label value is legal anywhere in the Label stack except at the bottom. When a received packet contains this Label value at the top of the Label stack, it is delivered to a local software module for processing. The actual packet forwarding is determined by the Label beneath it in the stack. However, if the packet is further forwarded, the router alert Label should be pushed back onto the Label stack before forwarding. The use of this Label is analogous to the use of the router alert option in IP packets. Since this Label cannot occur at the bottom of the stack, it is not associated with a particular network layer protocol.
- A value of 2 represents the IPv6 explicit NULL Label. This Label value is only legal at the bottom of the Label stack. It indicates that the Label stack must be popped, and the packet forwarding must be based on the IPv6 header.
- A value of 3 represents the Implicit NULL Label. This is a Label that a Label Switching Router (LSR) can assign and distribute, but which never actually appears in the encapsulation. When an LSR would otherwise replace the Label at the top of the stack with a new Label, but the new Label is Implicit NULL, the LSR pops the stack instead of doing the replacement. Although this value may never appear in the encapsulation, it needs to be specified in the Label Distribution Protocol (LDP), so a value is reserved.
- Values 4-15 are reserved for future use.

7750 SR OS uses labels for MPLS, RSVP-TE, and LDP, as well as packet-based services such as VLL and VPLS.

Label values 16 through 1,048,575 are defined as follows:

- Label values 16 through 31 are reserved for future use.
- Label values 32 through 1,023 are available for static assignment.
- Label values 1,024 through 2,047 are reserved for future use.
- Label values 2,048 through 18,431 are statically assigned for services.
- Label values 28,672 through 131,071 are dynamically assigned for both MPLS and services.
- Label values 131,072 through 1,048,575 are reserved for future use.

Label Switching Routers

LSRs perform the label switching function. LSRs perform different functions based on it's position in an LSP. Routers in an LSP do one of the following:

- The router at the beginning of an LSP is the ingress label edge router (ILER). The ingress router can encapsulate packets with an MPLS header and forward it to the next router along the path. An LSP can only have one ingress router.
- A Label Switching Router (LSR) can be any intermediate router in the LSP between the ingress and egress routers. An LSR swaps the incoming label with the outgoing MPLS label and forwards the MPLS packets it receives to the next router in the MPLS path (LSP). An LSP can have 0-253 transit routers.
- The router at the end of an LSP is the egress label edge router (ELER). The egress router strips the MPLS encapsulation which changes it from an MPLS packet to a data packet, and then forwards the packet to its final destination using information in the forwarding table. Each LSP can have only one egress router. The ingress and egress routers in an LSP cannot be the same router.

A router in your network can act as an ingress, egress, or transit router for one or more LSPs, depending on your network design.

An LSP is confined to one IGP area for LSPs using constrained-path. They cannot cross an autonomous system (AS) boundary.

Static LSPs can cross AS boundaries. The intermediate hops are manually configured so the LSP has no dependence on the IGP topology or a local forwarding table.

LSP Types

The following are LSP types:

- Static LSPs — A static LSP specifies a static path. All routers that the LSP traverses must be configured manually with labels. No signaling such as RSVP or LDP is required.
- Signaled LSP — LSPs are set up using a signaling protocol such as RSVP-TE or LDP. The signaling protocol allows labels to be assigned from an ingress router to the egress router. Signaling is triggered by the ingress routers. Configuration is required only on the ingress router and is not required on intermediate routers. Signaling also facilitates path selection.

  There are two signaled LSP types:

  → Explicit-path LSPs — MPLS uses RSVP-TE to set up explicit path LSPs. The hops within the LSP are configured manually. The intermediate hops must be configured as either strict or loose meaning that the LSP must take either a direct path from the previous hop router to this router (strict) or can traverse through other routers (loose). You can control how the path is set up. They are similar to static LSPs but require less configuration. See RSVP on page 42.

→ Constrained-path LSPs — The intermediate hops of the LSP are dynamically assigned. A constrained path LSP relies on the Constrained Shortest Path First (CSPF) routing algorithm to find a path which satisfies the constraints for the LSP. In turn, CSPF relies on the topology database provided by the extended IGP such as OSPF or IS-IS.

  Once the path is found by CSPF, RSVP uses the path to request the LSP set up. CSPF calculates the shortest path based on the constraints provided such as bandwidth, class of service, and specified hops.

If fast reroute is configured, the ingress router signals the routers downstream. Each downstream router sets up a detour for the LSP. If a downstream router does not support fast reroute, the request is ignored and the router continues to support the LSP. This can cause some of the detours to fail, but otherwise the LSP is not impacted.

No bandwidth is reserved for the rerouted path. If the user enters a value in the bandwidth parameter in the **config>router>mpls>lsp>fast-reroute** context, it will have no effect on the LSP backup LSP establishment.

Hop-limit parameters specifies the maximum number of hops that an LSP can traverse, including the ingress and egress routers. An LSP is not set up if the hop limit is exceeded. The hop count is set to 255 by default for the primary and secondary paths. It is set to 16 by default for a bypass or detour LSP path.

MPLS Facility Bypass Method of MPLS Fast Re-Route (FRR)

The MPLS facility bypass method of MPLS Fast Re-Route (FRR) functionality is extended to the ingress node.

The behavior of an LSP at an ingress LER with both fast reroute and a standby LSP path configured is as follows:

- When a down stream detour becomes active at a point of local repair (PLR):

  The ingress LER switches to the standby LSP path. If the primary LSP path is repaired subsequently at the PLR, the LSP will switch back to the primary path. If the standby goes down, the LSP is switched back to the primary, even though it is still on the detour at the PLR. If the primary goes down at the ingress while the LSP is on the standby, the detour at the ingress is cleaned up and for one-to-one detours a “path tear” is sent for the detour path. In other words, the detour at the ingress does not protect the standby. If and when the primary LSP is again successfully re-signaled, the ingress detour state machine will be restarted.
- When the primary fails at the ingress:

  The LSP switches to the detour path. If a standby is available then LSP would switch to standby on expiration of **hold-timer**. If **hold-timer** is disabled then switchover to standby would happen immediately. On successful global revert of primary path, the LSP would switch back to the primary path.
- Admin groups are not taken into account when creating detours for LSPs.

Manual Bypass LSP

In prior releases, the 7750 implemented dynamic bypass tunnels as per RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*. When an LSP is signaled and the local protection flag is set in the session_attribute object and/or the FRR object in the path message indicates that facility backup is desired, the PLR will establish a bypass tunnel to provide node and link protection. If a bypass LSP which merges in a downstream node with the protected LSP exist, and if this LSP satisfies the constraints in the FRR object, then this bypass tunnel is selected.

With the manual bypass feature, an LSP can be pre-configured from a PLR which will be used exclusively for bypass protection. When a path message for a new LSP requests bypass protection, the node will first check if a manual bypass tunnel satisfying the path constraints exists. If one is found, it will be selected. If no manual bypass tunnel is found, the 7750 will dynamically signal a bypass LSP in the default behavior. Users can disable the dynamic bypass creation on a per node basis using the CLI.

A maximum of 1000 associations of primary LSP paths can be made with a single manual bypass at the PLR node. If dynamic bypass creation is disabled on the node, it is recommended to configure additional manual bypass LSPs to handle the required number of associations.

Refer to Configuring Manual Bypass Tunnels on page 113 for configuration information.

PLR Bypass LSP Selection Rules

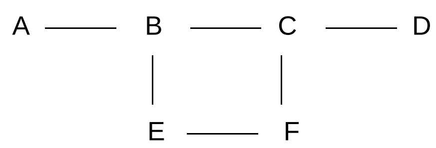

Figure 3: Bypass Tunnel Nodes

The PLR uses the following rules to select a bypass LSP among multiple manual and dynamic bypass LSP’s at the time of establishment of the primary LSP path or when searching for a bypass for a protected LSP which does not have an association with a bypass tunnel:

1. The MPLS/RSVP task in the PLR node checks if an existing manual bypass satisfies the constraints. If the path message for the primary LSP path indicated node protection desired, which is the default LSP FRR setting at the head end node, MPLS/RSVP task searches for a node-protect’ bypass LSP. If the path message for the primary LSP path indicated link protection desired, then it searches for a link-protect bypass LSP.
2. If multiple manual bypass LSPs satisfying the path constraints exist, it will prefer a manual-bypass terminating closer to the PLR over a manual bypass terminating further away. If multiple manual bypass LSPs satisfying the path constraints terminate on the same downstream node, it selects one with the lowest IGP path cost or if in a tie, picks the first one available.
3. If none satisfies the constraints and dynamic bypass tunnels have not been disabled on PLR node, then the MPLS/RSVP task in the PLR will check if any of the already established dynamic bypasses of the requested type satisfies the constraints.
4. If none do, then the MPLS/RSVP task will ask CSPF to check if a new dynamic bypass of the requested type, node-protect or link-protect, can be established.
5. If the path message for the primary LSP path indicated node protection desired, and no manual bypass was found after Step 1, and/or no dynamic bypass LSP was found after 3 attempts of performing Step 3, the MPLS/RSVP task will repeat Steps 1-3 looking for a suitable link-protect bypass LSP. If none are found, the primary LSP will have no protection and the PLR node must clear the “local protection available” flag in the IPv4

address sub-object of the RRO starting in the next Resv refresh message it sends upstream.

6. If the path message for the primary LSP path indicated link protection desired, and no manual bypass was found after step 1, and/or no dynamic bypass LSP was found after performing Step 3, the primary LSP will have no protection and the PLR node must clear the “local protection available” flag in the IPv4 address sub-object of the RRO starting in the next RESV refresh message it sends upstream. The PLR will not search for a node-protect’ bypass LSP in this case.
7. If the PLR node successfully makes an association, it must set the “local protection available” flag in the IPv4 address sub-object of the RRO starting in the next RESV refresh message it sends upstream.
8. For all primary LSP that requested FRR protection but are not currently associated with a bypass tunnel, the PLR node on reception of RESV refresh on the primary LSP path repeats Steps 1-7.

If the user disables dynamic-bypass tunnels on a node while dynamic bypass tunnels were activated and were passing traffic, traffic loss will occur on the protected LSP. Furthermore, if no manual bypass exist that satisfy the constraints of the protected LSP, the LSP will remain without protection.

If the user configures a bypass tunnel on node B and dynamic bypass tunnels have been disabled, LSPs which have been previously signaled and which were not associated with any manual bypass tunnel, for example, none existed, will be associated with the manual bypass tunnel if suitable. The node checks for the availability of a suitable bypass tunnel for each of the outstanding LSPs every time a RESV message is received for these LSPs.

If the user configures a bypass tunnel on node B and dynamic bypass tunnels have not been disabled, LSPs which have been previously signaled over dynamic bypass tunnels will not automatically be switched into the manual bypass tunnel even if the manual bypass is a more optimized path. The user will have to perform a make before break at the head end of these LSPs.

If the manual bypass goes into the down state in node B and dynamic bypass tunnels have been disabled, node B (PLR) will clear the “protection available” flag in the RRO IPv4 sub-object in the next RESV refresh message for each affected LSP. It will then try to associate each of these LSPs with one of the manual bypass tunnels that are still up. If it finds one, it will make the association and set again the “protection available” flag in the next RESV refresh message for each of these LSPs. If it could not find one, it will keep checking for one every time a RESV message is received for each of the remaining LSPs. When the manual bypass tunnel is back UP, the LSPs which did not find a match will be associated back to this tunnel and the protection available flag is set starting in the next RESV refresh message.

If the manual bypass goes into the down state in node B and dynamic bypass tunnels have not been disabled, node B will automatically signal a dynamic bypass to protect the LSPs if a suitable one does not exist. Similarly, if an LSP is signaled while the manual bypass is in the down state, the node will only signal a dynamic bypass tunnel if the user has not disabled dynamic tunnels.

When the manual bypass tunnel is back into the UP state, the node will not switch the protected LSPs from the dynamic bypass tunnel into the manual bypass tunnel.

FRR Node-Protection (Facility)

The MPLS Fast Re-Route (FRR) functionality enables PLRs to be aware of the missing node protection and lets them regularly probe for a node-bypass. The following describes an LSP scenario:

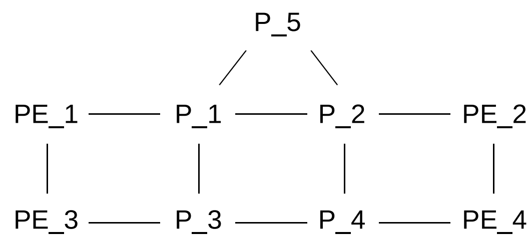

Figure 4: FRR Node-Protection Example

Where:

- LSP 1: between PE_1 to PE_2, with CSPF, FRR facility node-protect enabled.
- P_1 protects P_2 with bypass-nodes P_1 -P_3 - P_4 - PE_4 -PE_3.
- If P_4 fails, P_1 tries to establish the bypass-node three times.
- When the bypass-node creation fails, P_1 will protect link P_1-P_2.
- P_1 protects the link to P_2 through P_1 - P_5 - P_2.
- P_4 returns online.

Since LSP 1 had requested node protection, but due to lack of any available path, it could only obtain link protection. Therefore, every 60 seconds the PLR for LSP 1 will search for a new path that might be able to provide node protection. Once P_4 is back online and such a path is available, A new bypass tunnel will be signalled and LSP 1 will get associated with this new bypass tunnel.

Automatic Bandwidth Allocation for RSVP LSPs

Enabling and Disabling Auto-Bandwidth Allocation on an LSP

This section discusses an auto-bandwidth hierarchy configurable in the **config>router>mpls>lsp** context.

Adding auto-bandwidth at the lsp level starts the measurement of LSP bandwidth described in 5.1.2 Measurement of LSP Bandwidth on page 134 and allows auto-bandwidth adjustments to take place based on the triggers described in sections Periodic Automatic Bandwidth Adjustment on page 33 through 5.1.67.

When an LSP is first established, the bandwidth reserved along its primary path is controlled by the bandwidth parameter in the **config>router>mpls>lsp>primary** context, whether or not the LSP has auto-bandwidth enabled. When auto-bandwidth is enabled and a trigger occurs, the system will attempt to change the bandwidth of the LSP to some value between min-bandwidth and max-bandwidth, which are configurable values in the **lsp>auto-bandwidth** context. min-bandwidth is the minimum bandwidth that auto-bandwidth can signal for the LSP and max-bandwidth is the maximum bandwidth that can be signaled. It is expected that many customers will set min-bandwidth to the same value as the primary path bandwidth but the system will not enforce this restriction. More generally, the system will allow

- No **min-bandwidth** to be configured. In this case, the implicit minimum is 0 Mbps
- No **min-bandwidth** to be configured, as long as overflow-triggered auto-bandwidth (section 5.1.5) is not configured. In this case, the implicit maximum is infinite (effectively 100 Gbps).
- The configured primary path bandwidth to be outside the range of min-bandwidth to max-bandwidth.
- **auto-bandwidth** parameters can be changed at any time on an operational LSP; in most cases the changes have no immediate impact but subsequent sections will describe some exceptions

All of the auto-bandwidth adjustments discussed in this PRD must be performed using MBB procedures. As per existing MBB implementation, the bandwidth adjustment is performed on the active path at the time of re-signaling. Auto bandwidth on LSPs with secondary paths defined and therefore only primary path bandwidth is updated is not yet supported.

Auto bandwidth can be added to an operational LSP at any time (without the need to shutdown the LSP or path), but no bandwidth change occurs until a future trigger event. Auto bandwidth may also be removed from an operational LSP at any time and this causes an immediate MBB bandwidth change to be attempted using the configured primary path bandwidth.

Note that changing the configured bandwidth of an auto-bandwidth LSP has no immediate affect, it will only matters if the LSP/path goes down (due to failure or administrative action) and comes back up or if auto-bandwidth is removed from the LSP. The operator can force an auto-bandwidth LSP to be resized immediately to an arbitrary bandwidth using the appropriate tools commands.

Measurement of LSP Bandwidth

Automatic adjustment of RSVP LSP bandwidth based on measured traffic rate into the tunnel requires the LSP to be configured for egress statistics collection at the ingress LER. (Note that the system will not check if egress statistics has been enabled. If the user configures auto-bandwidth and does not enable egress-statistics then no auto-bandwidth measurements or adjustments will take place.) The following CLI shows an example:

```
config router mpls lsp name
      egress-statistics
      accounting-policy 99
      collect-stats
      no shutdown
     exit
```

All LSPs configured for accounting, including any configured for auto-bandwidth based on traffic measurements, must reference the same accounting policy, and this accounting policy must have the **auto-bandwidth** command to designate its purpose, as shown. An example configuration of such an accounting-policy is shown below: in the CLI example below.

```
config log
     accounting-policy 99
          auto-bandwidth
      collection-interval 5
          record combined-mpls-lsp-egress
     exit
exit
```

Note that the record **combined-mpls-lsp-egress** command in the accounting policy has the effect of recording both egress packet and byte counts and bandwidth measurements based on the byte counts if auto-bandwidth is enabled on the LSP.

When egress statistics are enabled the CPM collects stats from of all IOMs involved in forwarding traffic belonging to the LSP (whether the traffic is currently leaving the ingress LER via the primary LSP path, a secondary LSP path, an FRR detour path or an FRR bypass path). The egress statistics have counts for the number of packets and bytes forwarded per LSP on a per-forwarding class, per-priority (in-profile vs. out-of-profile) basis. When auto-bandwidth is configured for an LSP the ingress LER calculates a traffic rate for the LSP as follows:

Average data rate of LSP[x] during interval[i] = F(x, i)—F(x, i-1)/sample interval

F(x, i) — The total number of bytes belonging to LSP[x], regardless of forwarding-class or priority, at time[i]

sample interval = time[i] — time [i-1], time[i+1] — time[i], etc.

The sample interval is the product of sample-count and the collection-interval specified in the auto-bandwidth accounting policy. A default sample-count for all LSPs may be configured using the **config>router>mpls>auto-bandwidth-defaults** command but this value can be overridden on a per-LSP basis at the **config>router>mpls>lsp>auto-bandwidth** context. The default value of sample-count (the value that would result from the no auto-bandwidth-defaults command) is 1, which means the default sample interval is 300 seconds.

Over a longer period of time called the adjust interval the router keeps track of the maximum average data rate recorded during any constituent sample interval. The adjust interval is the product of adjust-count and the collection-interval specified in the auto-bandwidth accounting-policy. A default adjust-count for all LSPs may be configured using the **config>router>mpls>auto-bandwidth-defaults** command but this value can be overridden on a per-LSP basis at the **config>router>mpls>lsp>auto-bandwidth** context. The default value of adjust-count (the value that would result from the no auto-bandwidth-defaults command) is 288, which means the default adjust interval is 86400 seconds or 24 hours. The system enforces the restriction that adjust-count is equal to or greater than sample-count.

The collection-interval in the auto-bandwidth accounting policy can be changed at any time, without disabling any of the LSPs that rely on that policy for statistics collection. The change in duration of the sample interval will occur at the beginning of the next sample interval; at this instant the remaining time in the adjust interval will be (remaining adjust-count x new collection-interval). Information about the current adjust interval (such as the remaining adjust-count, the maximum average data rate) shall not be lost when the change takes effect.

The sample-count (at the **mpls>auto-bandwidth** level or the **lsp>auto-bandwidth** level) can be changed at any time. As with a collection-interval change this will have no effect until the beginning of the next sample interval. In this case the adjust-interval does not change and information about the current adjust interval (such as the remaining adjust-count, the maximum average data rate) must not be lost when the sample-count change takes effect.

The system allows adjust-count (at the **mpls>auto-bandwidth** level or the **lsp>auto-bandwidth** level) to be changed at any time as well but in this case the new value shall have no effect until the beginning of the next adjust interval.

Byte counts collected for LSP statistics include layer 2 encapsulation (Ethernet headers and trailers) and therefore average data rates measured by this feature include Layer 2 overhead as well.

Passive Monitoring of LSP Bandwidth

The system offers the option to measure the bandwidth of an RSVP LSP, per the description in the Measurement of LSP Bandwidth on page 31 section, without taking any action to adjust the bandwidth reservation, regardless of how different the measured bandwidth is from the current reservation. Passive monitoring is enabled using the **config>router>mpls>lsp>auto-bandwidth>monitor-bandwidth** command.

The **show>router>mpls>lsp detail** command can be used to view the maximum average data rate in the current adjust interval and the remaining time in the current adjust interval.

Periodic Automatic Bandwidth Adjustment

Automatic bandwidth allocation is supported on any RSVP LSP that has both CSPF and MBB enabled. CSPF is enabled using the config>router>mpls>lsp>cspf command and MBB is enabled using the **config>router>mpls>lsp>adaptive** command. For automatic adjustments of LSP bandwidth to occur the monitor-bandwidth command must not be present at **config>router>mpls>lsp>auto-bandwidth** context, otherwise only passive measurements will occur, .

If an eligible RSVP LSP is configured for auto-bandwidth, by entering auto-bandwidth at the config>router>mpls>lsp context, then the ingress LER decides every adjust interval whether to attempt auto-bandwidth adjustment. The following parameters are defined:

- current_bw — The currently reserved bandwidth of the LSP; this is the operational bandwidth that is already maintained in the MIB
- measured_bw — The maximum average data rate in the current adjust interval
- signaled_bw — The bandwidth that is provided to the CSPF algorithm and signaled in the SENDER_TSPEC and FLOWSPEC objects when an auto-bandwidth adjustment is attempted
- min — The configured min-bandwidth of the LSP
- max — The configured max-bandwidth of the LSP
- up% — Thee minimum difference between measured_bw and current_bw, expressed as a percentage of current_bw, for increasing the bandwidth of the LSP
- up — The minimum difference between measured_bw and current_bw, expressed as an absolute bandwidth relative to current_bw, for increasing the bandwidth of the LSP. This is an optional parameter; if not defined the value is 0.
- down% — Theminimum difference between current_bw and measured_bw, expressed as a percentage of current_bw, for decreasing the bandwidth of the LSP
- down — The minimum difference between current_bw and measured_bw, expressed as an absolute bandwidth relative to current_bw, for decreasing the bandwidth of the LSP. This is an optional parameter; if not defined the value is 0.

At the end of every adjust interval the system decides if an auto-bandwidth adjustment should be attempted. The heuristics are as follows:

if {(measured_bw/current_bw – 1)>= up%} && {(measured_bw - current_bw) >= up} then signaled_bw = max {(min (measured_bw, max)), min}

if {(1 – measured_bw/current_bw)>= down%} && {(current_bw - measured_bw) >= down} then signaled_bw = min {(max (measured_bw, min)), max}

if (current_bw > max) then signaled_bw = max

if (current_bw < min) then signaled_bw = min

Changes to min-bandwidth, max-bandwidth and any of the threshold values (up, up%, down, down%) are permitted at any time on an operational LSP but the changes have no effect until the next auto-bandwidth trigger (for example adjust interval expiry).

Note that min-bandwidth, max-bandwidth, up and down are all configured in units of Mbps, with a granularity of 1 Mbps. However in the threshold calculations outlined above measured_bw should be represented as precisely as possible (for example, 2.541 Mbps). If this results in signaled_bw, per the above algorithm, being a fractional quantity then the actual signaled bandwidth in the RSVP messages must be rounded up to the nearest integer multiple of 1 Mbps, in order to conform with existing implementation. This implies that current_bw will always be an exact multiple of 1 Mbps as well.

The adjust-timer and maximum average data rate are reset whether the adjustment succeeds or fails. If the bandwidth adjustment fails (e.g. CSPF cannot find a path) then the existing LSP is maintained with its existing bandwidth reservation. The system does not retry the bandwidth adjustment (i.e. per the configuration of the LSP retry-timer and retry-limit). If the re-signal timer expires after an auto-bandwidth adjustment failure the path reoptimization is based on the current operational bandwidth, not the last attempted bandwidth (that failed).

Overflow-Triggered Auto-Bandwidth Adjustment

For cases where the measured bandwidth of an LSP has increased significantly since the start of the current adjust interval it may be desirable for the system to pre-emptively adjust the bandwidth of the LSP and not wait until the end of the adjust interval.

The following parameters are defined:

- current_bw — The currently reserved bandwidth of the LSP
- sampled_bw — The average data rate of the sample interval that just ended
- measured_bw — The maximum average data rate in the current adjust interval (same meaning as in section 5.1.4)
- signaled_bw — The bandwidth that is provided to the CSPF algorithm and signaled in the SENDER_TSPEC and FLOWSPEC objects when an auto-bandwidth adjustment is attempted (same meaning as in section 5.1.4)
- max — The configured max-bandwidth of the LSP
- %_threshold — The minimum difference between sampled_bw and current_bw, expressed as a percentage of the current_bw, for counting an overflow event
- min_threshold — The minimum difference between sampled_bw and current_bw, expressed as an absolute bandwidth relative to current_bw, for counting an overflow event. This is an optional parameter; if not defined the value is 0.

When a sample interval ends it is counted as an overflow if:

{(sampled_bw/current_bw — 1) >= %_threshold} && {(sampled_bw— current_bw) >= min_threshold}

When the number of overflow samples reaches a configured limit auto-bandwidth adjustment is attempted immediately using MBB procedures, per the following rules.

if (measured_bw >= max) then signaled_bw = max;

if (measured_bw <= min) then signaled_bw = min;

else signaled_bw = measured_bw

If the bandwidth adjustment is successful then the adjust-count, maximum average data rate and overflow count are all reset. If the bandwidth adjustment fails then the overflow count is reset but the adjust-count and maximum average data rate continue with current values. It is possible that the overflow count will once again reach the configured limit before the adjust-count is reached and this will once again trigger an immediate auto-bandwidth adjustment attempt.

The overflow configuration command fails if the max-bandwidth of the LSP has not been defined or if it has been set to zeroinfinite (100 Gbps).

The threshold limit can be changed on an operational auto-bandwidth LSP at any time and the change should take effect at the end of the current sample interval (for example, if the user decreases the overflow limit to a value lower than the current overflow count then auto-bandwidth adjustment will take place as soon as the sample interval ends). The threshold values change be changed at any time (for example, %_threshold and min_threshold) but the new values will not take effect until the end of the current sample interval.

Manually-Triggered Auto-Bandwidth Adjustment

Manually-triggered auto-bandwidth adjustment featureis configured with the **tools>perform>router>mpls adjust-autobandwidth** [**lsp** *lsp-name* [**force** [**bandwidth** *mbps*]]] command to attempt immediate auto-bandwidth adjustment for either one specific LSP or all active LSPs. If the LSP is not specified then the system assumes the command applies to all LSPs. If an LSP name is provided then the command applies to that specific LSP only and the optional **force** parameter (with or without a bandwidth) can be used.

If **force** is not specified (or the command is not LSP-specific) then measured_bw is compared to current_bw and bandwidth adjustment may or may not occur

If **force** is specified and a bandwidth is not provided then the threshold checking is bypassed and the following logic is used:

if (measured_bw >= max) then signaled_bw = max;

if (measured_bw <= min) then signaled_bw = min;

else signaled_bw = measured_bw

If **force** is specified with a bandwidth (in Mbps) then signaled_bw is set to this bandwidth. There is no requirement that the bandwidth entered as part of the command fall within the range of min-bandwidth to max-bandwidth.

All manually-triggered auto-bandwidth adjustments must be performed using MBB procedures.

The adjust-count, maximum average data rate and overflow count are not reset by the manual auto-bandwidth command, whether or not the bandwidth adjustment succeeds or fails.

VLL CAC Triggered Auto-Bandwidth Adjustment

So far the scope of the auto-bandwidth feature has been restricted to measurement-based or manually-triggered adjustments of LSP bandwidth. However, there is another case where automatic bandwidth adjustments may be useful.

When a user binds a VLL service to an SDP they have the option (starting in 6.0) of also specifying a bandwidth for CAC purposes. Bandwidth reserved for a VLL service gets deducted from the maximum available bandwidth of the SDP, which is the sum of the LSP bandwidths comprising the SDP (the active paths) multiplied by a booking factor.

Currently, when the bandwidth of a VLL service exceeds the SDP available bandwidth the VLL service is not activated and a notification is issued. With auto-bandwidth adjustment, the system could have automatically increased the bandwidth of the SDP prior to this happening. The specifics are detailed below.

A new object, [no] auto-bandwidth, is introduced in the config>service>sdp context. When this parameter is present, the SDP supports auto-bandwidth adjustment, and VLL services bound to this SDP benefit from this capability. In order for auto-bandwidth to be enabled on an SDP:

- The SDP type must be MPLS.
- The SDP must comprise of only RSVP LSPs.
- All of the RSVP LSPs must have **auto-bandwidth** enabled.
- The **adjust-up**, **adjust-down** and **overflow-limit** commands must not be enabled in the **auto-bandwidth** configuration of any of the RSVP LSPs.

The **config>service>sdp>auto-bandwidth** context has 4 commands:

- min-bandwidth — The minimum bandwidth of the SDP (the system will never automatically set the SDP bandwidth below this value). This value must be greater than or equal to the sum of the min-bandwidth parameters of the LSPs in the SDP.
- max-bandwidth — The maximum bandwidth of the SDP (the system will never automatically set the SDP bandwidth above this value). This value must be less than or equal to the sum of the max-bandwidth parameters of the LSPs in the SDP.
- threshold-up — When sdp-available-bw, expressed as a percentage of max-sdp-available-bw, falls below this value (for exampl,e due to a VLL service addition or manual auto-bandwidth adjustment of an LSP in the SDP) the system attempts to increase the bandwidth of the SDP by a multiple of the bandwidth step (U) configured as part of this command. The multiple (N) is the minimum value of N such that SDP-Available-bw (after the service has been added) divided by (max-sdp-available-bw + NxU) is greater than threshold-up.
- threshold-down — When sdp-available-bw, expressed as a percentage of max-sdp-available-bw, exceeds this value (for example, due to a VLL service removal or manual

auto-bandwidth adjustment of an LSP in the SDP) the system attempts to decrease the bandwidth of the SDP by a multiple of the bandwidth step (D) configured as part of this command. The multiple (N) is the minimum value of N such that SDP-Available-bw (after the service has been removed) divided by (Max-SDP-available-bw ?NxD) is less than threshold-down.

The increase or decrease of SDP bandwidth is achieved by dividing the SDP bandwidth change by the number of LSPs in the SDP and adjusting the bandwidth of each LSP by that same amount. LSP bandwidth adjustments use MBB procedures and apply to the primary path of each LSP.

When VLL CAC adjusts the bandwidth of an LSP it does not reset of the adjust-timer or maximum average data rate of the LSP.

Displaying Auto-Bandwidth Information

This feature adds the following additional fields to the output of the show>router>mpls>lsp detail command in order to display information about the operation of auto-bandwidth allocation on the LSP:

- Whether auto-bandwidth is enabled or disabled on the LSP.
- The configured value of min-bandwidth.
- The configured value of max-bandwidth.
- The value of the adjust interval, calculated from adjust-count x collection-interval.
- The value of the sample interval, calculated from sample-count x collection-interval.
- The configured values of bandwidth increase thresholds (up and up%).
- The configured values of bandwidth decrease thresholds (down and down%).
- The system time when the current adjust interval will next expire.
- The maximum average data rate since the start of the current adjust interval.
- The average data rate from the last sample interval.
- The configured value of the overflow-limit.
- The current overflow count.
- The system time of the last auto-bandwidth adjustment, and the cause (manual, adjust-timer, overflow).
- The currently reserved bandwidth along the primary path (in addition to the current field that displays the configured bandwidth).

Clearing Auto-Bandwidth Counters

This feature resets all counters and timers associated with auto-bandwidth allocation on the referenced LSP. This is performed in the **clear>router>mpls> lsp-autobandwidth** *lsp-name* context, to . Specifically this means that:

- The sample-count is reset to its configured value, and the average data rate of the current sample interval is discarded.
- The adjust-count is reset to its configured value.
- The maximum average data rate is zeroed.
- The overflow count is zeroed.

Feature Interaction

This feature interworks with:

- Diff-Serv TE — The class-type of an LSP remains the same at each re-signaling of the LSP due to auto-bandwidth adjustment.
- VLL CAC — Any change to the active path bandwidth caused by auto-bandwidth adjustment updates the maximum SDP available bandwidth used by the VLL CAC algorithm.
- LSPs with auto-bandwidth adjustment support soft pre-emption. The setup and holding priorities of an LSP remain the same at each re-signaling of the LSP due to auto-bandwidth adjustment.
- LSPs with auto-bandwidth adjustment supports existing CSPF capabilities including admin-groups (include/exclude), use of TE-metric vs. IGP metric, ECMP least-fill loadbalancing and SRLGs.

RSVP

The Resource Reservation Protocol (RSVP) is a network control protocol used by a host to request specific qualities of service from the network for particular application data streams or flows. RSVP is also used by routers to deliver quality of service (QoS) requests to all nodes along the path(s) of the flows and to establish and maintain state to provide the requested service. RSVP requests generally result in resources reserved in each node along the data path. MPLS leverages this RSVP mechanism to set up traffic engineered LSPs. RSVP is not enabled by default and must be explicitly enabled.

RSVP requests resources for simplex flows. It requests resources only in one direction (unidirectional). Therefore, RSVP treats a sender as logically distinct from a receiver, although the same application process may act as both a sender and a receiver at the same time. Duplex flows require two LSPs, to carry traffic in each direction.

RSVP is not a routing protocol. RSVP operates with unicast and multicast routing protocols. Routing protocols determine where packets are forwarded. RSVP consults local routing tables to relay RSVP messages.

RSVP uses two message types to set up LSPs, PATH and RESV. Figure 5 depicts the process to establish an LSP.

- The sender (the ingress LER (ILER)), sends PATH messages toward the receiver, (the egress LER (ELER)) to indicate the FEC for which label bindings are desired. PATH messages are used to signal and request label bindings required to establish the LSP from ingress to egress. Each router along the path observes the traffic type.

  PATH messages facilitate the routers along the path to make the necessary bandwidth reservations and distribute the label binding to the router upstream.
- The ELER sends label binding information in the RESV messages in response to PATH messages received.
- The LSP is considered operational when the ILER receives the label binding information.

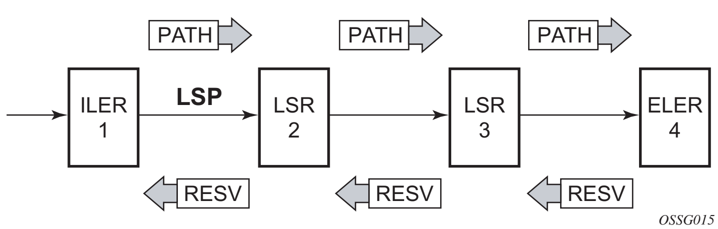

Figure 5: Establishing LSPs

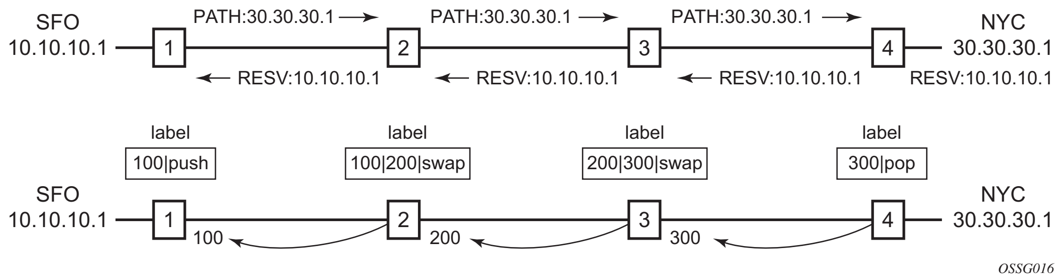

Figure 6: LSP Using RSVP Path Set Up

Figure 6 displays an example of an LSP path set up using RSVP. The ingress label edge router (ILER 1) transmits an RSVP path message (path: 30.30.30.1) downstream to the egress label edge router (ELER 4). The path message contains a label request object that requests intermediate LSRs and the ELER to provide a label binding for this path.

In addition to the label request object, an RSVP PATH message can also contain a number of optional objects:

- Explicit route object (ERO) — When the ERO is present, the RSVP path message is forced to follow the path specified by the ERO (independent of the IGP shortest path).
- Record route object (RRO) — Allows the ILER to receive a listing of the LSRs that the LSP tunnel actually traverses.
- A session attribute object controls the path set up priority, holding priority, and local-rerouting features.

Upon receiving a path message containing a label request object, the ELER transmits a RESV message that contains a label object. The label object contains the label binding that the downstream LSR communicates to its upstream neighbor. The RESV message is sent upstream towards the ILER, in a direction opposite to that followed by the path message. Each LSR that processes the RESV message carrying a label object uses the received label for outgoing traffic associated with the specific LSP. When the RESV message arrives at the ingress LSR, the LSP is established.

Using RSVP for MPLS

Hosts and routers that support both MPLS and RSVP can associate labels with RSVP flows. When MPLS and RSVP are combined, the definition of a flow can be made more flexible. Once an LSP is established, the traffic through the path is defined by the label applied at the ingress node of the LSP. The mapping of label to traffic can be accomplished using a variety of criteria. The set of packets that are assigned the same label value by a specific node are considered to belong to the same FEC which defines the RSVP flow.

For use with MPLS, RSVP already has the resource reservation component built-in which makes it ideal to reserve resources for LSPs.

RSVP Traffic Engineering Extensions for MPLS

RSVP has been extended for MPLS to support automatic signaling of LSPs. To enhance the scalability, latency, and reliability of RSVP signaling, several extensions have been defined. Refresh messages are still transmitted but the volume of traffic, the amount of CPU utilization, and response latency are reduced while reliability is supported. None of these extensions result in backward compatibility problems with traditional RSVP implementations.

- Hello Protocol on page 44
- MD5 Authentication of RSVP Interface on page 45
- RSVP Overhead Refresh Reduction on page 47

Hello Protocol

The Hello protocol detects the loss of a neighbor node or the reset of a neighbor’s RSVP state information. In standard RSVP, neighbor monitoring occurs as part of RSVP’s soft-state model. The reservation state is maintained as cached information that is first installed and then periodically refreshed by the ingress and egress LSRs. If the state is not refreshed within a specified time interval, the LSR discards the state because it assumes that either the neighbor node has been lost or its RSVP state information has been reset.

The Hello protocol extension is composed of a hello message, a hello request object and a hello ACK object. Hello processing between two neighbors supports independent selection of failure detection intervals. Each neighbor can automatically issue hello request objects. Each hello request object is answered by a hello ACK object.

MD5 Authentication of RSVP Interface

When enabled on an RSVP interface, authentication of RSVP messages operates in both directions of the interface.

A node maintains a security association with its neighbors for each authentication key. The following items are stored in the context of this security association:

- The HMAC-MD5 authentication algorithm.
- Key used with the authentication algorithm.
- Lifetime of the key. A key is user-generated key using a third party software/hardware and enters the value as static string into CLI configuration of the RSVP interface. The key will continue to be valid until it is removed from that RSVP interface.
- Source Address of the sending system.
- Latest sending sequence number used with this key identifier.

The RSVP sender transmits an authenticating digest of the RSVP message, computed using the shared authentication key and a keyed-hash algorithm. The message digest is included in an Integrity object which also contains a Flags field, a Key Identifier field, and a Sequence Number field. The RSVP sender complies to the procedures for RSVP message generation in RFC 2747, *RSVP Cryptographic Authentication*.

An RSVP receiver uses the key together with the authentication algorithm to process received RSVP messages.

When a PLR node switches the path of the LSP to a bypass LSP, it does not send the Integrity object in the RSVP messages over the bypass tunnel. If an integrity object is received from the MP node, then the message is discarded since there is no security association with the next-next-hop MP node.

The 7750 MD5 implementation does not support the authentication challenge procedures in RFC 2747.

Reservation Styles

LSPs can be signaled with explicit reservation styles. A reservation style is a set of control options that specify a number of supported parameters. The style information is part of the LSP configuration. SR OS supports two reservation styles:

- Fixed Filter (FF) — The Fixed Filter (FF) reservation style specifies an explicit list of senders and a distinct reservation for each of them. Each sender has a dedicated reservation that is not shared with other senders. Each sender is identified by an IP address and a local identification number, the LSP ID. Because each sender has its own reservation, a unique label and a separate LSP can be constructed for each sender-receiver pair. For traditional RSVP applications, the FF reservation style is ideal for a video distribution application in which each channel (or source) requires a separate pipe for each of the individual video streams.
- Shared Explicit (SE) — The Shared Explicit (SE) reservation style creates a single reservation over a link that is shared by an explicit list of senders. Because each sender is explicitly listed in the RESV message, different labels can be assigned to different sender-receiver pairs, thereby creating separate LSPs.

  Note that if FRR option is enabled for the LSP and selects the facility FRR method at the head-end node, only the SE reservation style is allowed. Furthermore, if a 7750PLR node receives a path message with fast-reroute requested with facility method and the FF reservation style, it will reject the reservation. The one-to-one detour method supports both FF and SE styles.

RSVP Message Pacing

When a flood of signaling messages arrive because of topology changes in the network, signaling messages can be dropped which results in longer set up times for LSPs. RSVP message pacing controls the transmission rate for RSVP messages, allowing the messages to be sent in timed intervals. Pacing reduces the number of dropped messages that can occur from bursts of signaling messages in large networks.

RSVP Overhead Refresh Reduction

The RSVP refresh reduction feature consists of the following capabilities implemented in accordance to RFC 2961, *RSVP Refresh Overhead Reduction Extensions*:

- RSVP message bundling — This capability is intended to reduce overall message handling load. The 7750 supports receipt and processing of bundled message only, but no transmission of bundled messages.
- Reliable message delivery: — This capability consists of sending a message-id and returning a message-ack for each RSVP message. It can be used to detect message loss and support reliable RSVP message delivery on a per hop basis. It also helps reduce the refresh rate since the delivery becomes more reliable.
- Summary refresh — This capability consists of refreshing multiples states with a single message-id list and sending negative ACKs (NACKs) for a message_id which could not be matched. The summary refresh capability reduce the amount of messaging exchanged and the corresponding message processing between peers. It does not however reduce the amount of soft state to be stored in the node.

These capabilities can be enabled on a per-RSVP-interface basis are referred to collectively as “refresh overhead reduction extensions”. When the refresh-reduction is enabled on a 7750 RSVP interface, the node indicates this to its peer by setting a refresh-reduction- capable bit in the flags field of the common RSVP header. If both peers of an RSVP interface set this bit, all the above three capabilities can be used. Furthermore, the node monitors the settings of this bit in received RSVP messages from the peer on the interface. As soon as this bit is cleared, the node stops sending summary refresh messages. If a peer did not set the “refresh-reduction-capable” bit, a 7750 node does not attempt to send summary refresh messages.

RSVP LSP Statistics

This feature provides the following counters:

- Per forwarding class forwarded in-profile packet count
- Per forwarding class forwarded in-profile byte count
- Per forwarding class forwarded out of profile packet count
- Per forwarding class forwarded out of profile byte count

The counters are available for an RSVP LSP at the egress datapath of an ingress LER and at the ingress datapath of an egress LER. No LSR statistics are provided.

This feature is supported on IOM-2 and IOM-3 and requires chassis mode C or higher.

Configuring Implicit Null

The implicit null label option allows a 7x50 egress LER to receive MPLS packets from the previous hop without the outer LSP label. The operation of the previous hop is referred to as penultimate hop popping (PHP).

This option is signaled by the egress LER to the previous hop during the LSP signaling with RSVP control protocol. In addition, the egress LER can be configured to receive MPLS packet with the implicit null label on a static LSP.

The user can configure your router to signal the implicit null label value over all RSVP interfaces and for all RSVP LSPs for which this node is the egress LER using the following command:

config>router>rsvp>implicit-null-label

The user must shutdown RSVP before being able to change the implicit null configuration option.

The user can also override the RSVP level configuration for a specific RSVP interface:

config>router>rsvp>interface>implicit-null-label {enable | disable}

All LSPs for which this node is the egress LER and for which the path message is received from the previous hop node over this RSVP interface will signal the implicit null label. This means that if the egress LER is also the merge-point (MP) node, then the incoming interface for the path refresh message over the bypass dictates if the packet will use the implicit null label or not. The same for a 1-to-1 detour LSP.

By default, an RSVP interface inherits the RSVP level configuration. The user must shutdown the RSVP interface before being able to change the implicit null configuration option. Note that the RSVP interface must be shutdown regardless if the new value for the interface is the same or different than the one it is currently using.

The egress LER does not signal the implicit null label value on P2MP RSVP LSPs. However, the PHP node can honor a Resv message with the label value set to the implicit null value when the egress LER is a third party implementation..

The implicit null label option is also supported on a static label LSP. The following commands can be used to cause the node to push or to swap to an implicit null label on the MPLS packet:

config>router>mpls>static-lsp>push implicit-null-label nexthop *ip-address*

config>router>mpls>interface>label-map>swap implicit-null-label nexthop *ip-address*

Traffic Engineering

Without traffic engineering, routers route traffic according to the SPF algorithm, disregarding congestion or packet types.

With traffic engineering, network traffic is routed efficiently to maximize throughput and minimize delay. Traffic engineering facilitates traffic flows to be mapped to the destination through a different (less congested) path other than the one selected by the SPF algorithm.

MPLS directs a flow of IP packets along a label switched path (LSP). LSPs are simplex, meaning that the traffic flows in one direction (unidirectional) from an ingress router to an egress router. Two LSPs are required for duplex traffic. Each LSP carries traffic in a specific direction, forwarding packets from one router to the next across the MPLS domain.

When an ingress router receives a packet, it adds an MPLS header to the packet and forwards it to the next hop in the LSP. The labeled packet is forwarded along the LSP path until it reaches the destination point. The MPLS header is removed and the packet is forwarded based on Layer 3 information such as the IP destination address. The physical path of the LSP is not constrained to the shortest path that the IGP would choose to reach the destination IP address.

TE Metric (IS-IS and OSPF)

When the use of the TE metric is selected for an LSP, the shortest path computation after the TE constraints are applied will select an LSP path based on the TE metric instead of the IGP metric. The user configures the TE metric under the MPLS interface. Both the TE and IGP metrics are advertised by OSPF and IS-IS for each link in the network. The TE metric is part of the traffic engineering extensions of both IGP protocols.

A typical application of the TE metric is to allow CSPF to represent a dual TE topology for the purpose of computing LSP paths.

An LSP dedicated for real-time and delay sensitive user and control traffic has its path computed by CSPF using the TE metric. The user configures the TE metric to represent the delay figure, or a combined delay/jitter figure, of the link. In this case, the shortest path satisfying the constraints of the LSP path will effectively represent the shortest delay path.

An LSP dedicated for non delay sensitive user and control traffic has its path computed by CSPF using the IGP metric. The IGP metric could represent the link bandwidth or some other figure as required.

When the use of the TE metric is enabled for an LSP, CSPF will first prune all links in the network topology that do not meet the constraints specified for the LSP path. These constraints include bandwidth, admin-groups, and hop limit. CSPF will then run an SPF on the remaining links. The shortest path among the all SPF paths will be selected based on the TE metric instead of the IGP metric which is used by default. Note that the TE metric is only used in CSPF computations for MPLS paths and not in the regular SPF computation for IP reachability.

Diff-Serv Traffic Engineering

Diff-Serv traffic engineering provides the ability to manage bandwidth on a per Traffic Engineering (TE) class basis as per RFC 4124. In the base traffic engineering, LER computes LSP paths based on available BW of links on the path. Diff-Serv TE adds ability to perform this on a per TE class basis.

A TE class is a combination of Class Type and LSP priority. A Class Type is mapped to one or more system Forwarding Classes using a configuration profile. The operator sets different limits for admission control of LSPs in each TE class over each TE link. Eight TE classes are supported. Admission control of LSP paths bandwidth reservation is performed using the Maximum Allocation Bandwidth Constraint Model as per RFC 4125.

Mapping of Traffic to a Diff-Serv LSP

An LER will allow the operator to map traffic to a Diff-Serv LSP through one of the following methods:

1. Explicit RSVP SDP configuration of a VLL, VPLS, or VPRN service.
2. Class-based forwarding in an RSVP SDP. The operator can enable the checking by RSVP that a Forwarding Class (FC) mapping to an LSP under the SDP configuration is compatible with the Diff-Serv Class Type (CT) configuration for this LSP.
3. Auto-bind RSVP-TE option in a VPRN service.
4. Static routes with indirect next-hop being an RSVP LSP name.

Admission Control of Classes

There are a couple of admission control decisions made when an LSP with a specified bandwidth is to be signaled. The first is in the head-end node. CSPF will only consider network links that have sufficient bandwidth. Link bandwidth information is provided by IGP TE advertisement by all nodes in that network.

Another decision made is local CAC and is performed when the RESV message for the LSP path is received in the reverse direction by a 7750 SR node in that path. The bandwidth value selected by the egress LER will be checked against link bandwidth, otherwise the reservation is rejected. If accepted, the new value for the remaining link bandwidth will be advertised by IGP at the next advertisement event.

Both of these admission decisions are enhanced to be performed at the TE class level when Diff-Serv TE is enabled. In other words, CSPF in the head-end node will need to check the LSP bandwidth against the ‘unreserved bandwidth’ advertised for all links in the path of the LSP for that TE class which consists of a combination of a CT and a priority. Same for the admission control at 7750 SR node receiving the Resv message.

Maximum Allocation Model

The admission control rules for this model are described in RFC 4125. Each CT shares a percentage of the Maximum Reservable Link Bandwidth through the user-configured BC for this CT. The Maximum Reservable Link Bandwidth is the link bandwidth multiplied by the RSVP interface subscription factor.

The sum of all BC values across all CTs will not exceed the Maximum Reservable Link Bandwidth. In other words, the following rule is enforced:

SUM (BCc) =< Max-Reservable-Bandwidth, 0 <= c <= 7

An LSP of class-type CTc, setup priority p, holding priority h (h=<p), and bandwidth B is admitted into a link if the following condition is satisfied:

B <= Unreserved Bandwidth for TE-Class[i]

where TE-Class [i] maps to < CTc, p > in the definition of the TE classes on the node. The bandwidth reservation is effected at the holding priority, i.e., in TE-class [j] = <CTc, h>. Thus, the reserved bandwidth for CTc and the unreserved bandwidth for the TE classes using CTc are updated as follows:

Reserved(CTc) = Reserved(CTc) + B

Unreserved TE-Class [j] = BCc - SUM (Reserved(CTc,q)) for 0<= q <= h

Unreserved TE-Class [i] = BCc - SUM (Reserved(CTc,q)) for 0<= q <= p

The same is done to update the unreserved bandwidth for any other TE class making use of the same CTc. These new values are advertised to the rest of the network at the next IGP-TE flooding.

When Diff-Serv is disabled on the node, this model degenerates into a single default CT internally with eight pre-emption priorities and a non-configurable BC equal to the Maximum Reservable Link Bandwidth. This would behave exactly like CT0 with eight pre-emption priorities and BC= Maximum Reservable Link Bandwidth if Diff-Serv was enabled.

Russing Doll Model

The RDM model is defined using the following equations:

SUM (Reserved (CTc)) <= BCb,

where the SUM is across all values of **c** in the range **b <= c <= (MaxCT - 1)**, and **BCb** is the bandwidth constraint of **CTb**.

BC0= Max-Reservable-Bandwidth, so that:

SUM (Reserved(CTc)) <= Max-Reservable-Bandwidth,

where the **SUM** is across all values of **c** in the range **0 <= c <= (MaxCT - 1)**

An LSP of class-type **CTc**, setup priority **p**, holding priority **h (h=<p)**, and bandwidth **B** is admitted into a link if the following condition is satisfied:

B <= Unreserved Bandwidth for TE-Class[i],

where **TE-Class [i]** maps to < **CTc , p** > in the definition of the TE classes on the node. The bandwidth reservation is effected at the holding priority, i.e., in **TE-class [j] = <CTc, h>**. Thus, the reserved bandwidth for CTc and the unreserved bandwidth for the TE classes using CTc are updated as follows:

Reserved(CTc) = Reserved(CTc) + B

Unreserved TE-Class [j] = Unreserved (CTc, h) = Min [

BCc - SUM (Reserved (CTb, q) for 0<=q <= h, c <= b <= 7,

BC(c-1) – SUM (Reserved (CTb, q) for 0<=q <= h, (c-1) <= b <= 7,

…….

BC0 - SUM (Reserved (CTb, q) for 0<=q <= h, 0 <= b <= 7]

Unreserved TE-Class [i] = Unreserved (CTc, p) = Min [

BCc - SUM (Reserved (CTb, q) for 0<=q <= p, c <= b <= 7,

BC(c-1) – SUM (Reserved (CTb, q) for 0<=q <= p, (c-1) <= b <= 7,

…….

BC0 - SUM (Reserved (CTb, q) for 0<=q <= p, 0 <= b <= 7]

The same is done to update the unreserved bandwidth for any other TE class making use of the same CTc. These new values are advertised to the rest of the network at the next IGP-TE flooding.

Example CT Bandwidth Sharing with RDM

Below is a simple example with two CT values (CT0, CT1) and one priority 0 as shown in Figure 7.

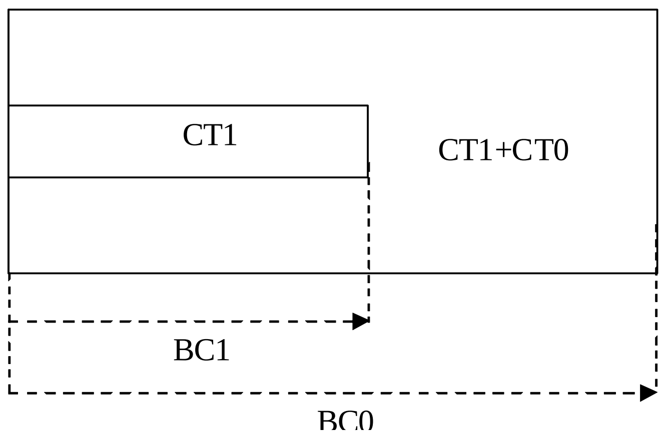

Figure 7: RDM with Two Class Types

Suppose CT1 bandwidth, or the CT1 percentage of Maximum Reservable Bandwidth to be more accurate is 100 Mbps and CT2 bandwidth is 100 Mbps and link bandwidth is 200 Mbps. BC constraints can be calculated as follows.

BC1 = CT1 Bandwidth = 100 Mbps.

BC0 = {CT1 Bandwidth} + {CT0 Bandwidth} = 200 Mbps.

Suppose an LSP comes with CT1, setup and holding priorities of 0 and a bandwidth of 50 Mbps.

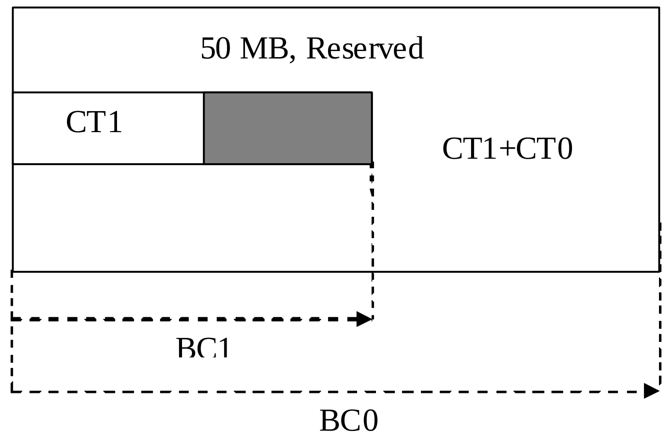

Figure 8: First LSP Reservation

According to the RDM admission control policy:

Reserved (CT1, 0) = 50 <= 100 Mbps

Reserved (CT0, 0) + Reserved (CT1, 0) = 50 <= 200 Mbps

This results in the following unreserved bandwidth calculation.

Unreserved (CT1, 0) = BC1 – Reserved (CT1, 0) = 100 – 50 = 50 Mbps

Unreserved (CT0, 0) = BC0 – Reserved (CT0, 0) – Reserved (CT1, 0) = 200 – 0 – 50= 150 Mbps.

Note that bandwidth reserved by a doll is not available to itself as well any of the outer dolls.

Suppose now another LSP comes with CT0, setup and holding priorities of 0 and a bandwidth 120 Mbps.

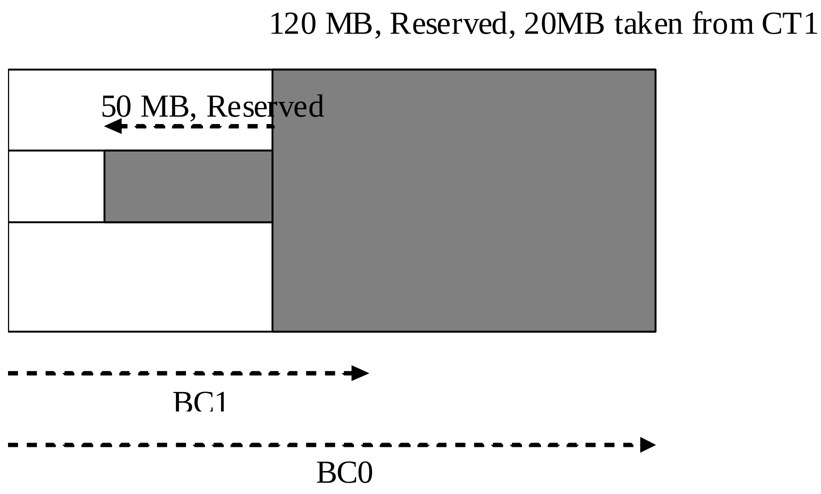

Figure 9: Second LSP Reservation

Reserved (CT0, 0) = 120 <= 150 Mbps

Reserved (CT0, 0) + Reserved (CT1, 0) = 120 + 50 = 170 <= 200 Mbps

Unreserved (CT0, 0) = 150 -120 = 30 Mbps

If we simply checked BC1, the formula would yield the wrong results:

Unreserved (CT1, 0) = BC1 – Reserved (CT1, 0) = 100 -50 = 50 Mbps

Because of the encroaching of CT0 into CT1, we would need to deduct the overlapping reservation. This would then yield:

Unreserved (CT1, 0) = BC0 – Reserved (CT0, 0) – Reserved (CT1, 0) = 200 – 120 - 50 = 30 Mbps,

which is the correct figure.

Extending the formula with both equations:

Unreserved (CT1, 0) = Min [BC1 – Reserved (CT1, 0), BC0 – Reserved (CT0, 0) – Reserved (CT1, 0)] = Min [100 – 50, 200 – 120 – 50] = 30 Mbps

Note that an outer doll can encroach into inner doll reducing the bandwidth available for inner dolls.

RSVP Control Plane Extensions

RSVP will use the Class Type object to carry LSP class-type information during path setup. Eight values will be supported for class-types 0 through 7 as per RFC 4124. Class type 0 is the default class which is supported today on the 7750 SR.

One or more 7750 SR forwarding classes will map to a Diff-Serv class type trough a system level configuration.

IGP Extensions

IGP extensions are defined in RFC 4124. Diff-Serv TE advertises link available bandwidth, referred to as unreserved bandwidth, by OSPF TE or IS-IS TE on a per TE class basis. A TE class is a combination of a class type and an LSP priority. In order to reduce the amount of per TE class flooding required in the network, the number of TE classes is set to eight. This means that eight class types can be supported with a single priority or four class types with two priorities, etc. In that case, the operator configures the desired class type on the LSP such that RSVP-TE can signal it in the class-type object in the path message.

IGP will continue to advertise the existing Maximum Reservable Link Bandwidth TE parameter to mean the maximum bandwidth that can be booked on a given interface by all classes. The value advertised is adjusted with the link subscription factor.

Diff-Serv TE Configuration and Operation

RSVP Protocol Level

The following are the configuration steps at the RSVP protocol level:

1. The operator enables Diff-Serv TE by executing the **diffserv-te** command in the **config>router>rsvp** context. When this command is enabled, IS-IS and OSPF will start advertising available bandwidth for each TE class configured under the **diffserv-te** node. The operator can disable Diff-Serv TE globally by using the no form of the command.

2. The enabling or disabling of Diff-Serv on the system requires that the RSVP and MPLS protocol be shutdown. The operator must execute the **no shutdown** command in each context once all parameters under both protocols are defined. When saved in the configuration file, the **no shutdown** command is automatically inserted under both protocols to make sure they come up after a node reboot.

3. IGP will advertise the available bandwidth in each TE class in the unreserved bandwidth TE parameter for that class for each RSVP interface in the system.

4. In addition, IGP will continue to advertise the existing Maximum Reservable Link Bandwidth TE parameter so the maximum bandwidth that can be booked on a given interface by all classes. The value advertised is adjusted with the link subscription factor configured in the **config>router>rsvp>interface>subscription** *percentage* context.

5. The operator can overbook (underbook) the maximum reservable bandwidth of a given CT by overbooking (underbooking) the interface maximum reservable bandwidth by configuring the appropriate value for the **subscription** *percentage* parameter.

6. The **diffserv-te** command will only have effect if the operator has already enabled traffic engineering at the IS-IS and/or OSPF routing protocol levels:
   config>router>isis>traffic-engineering
   and/or:
   config>router>ospf>traffic-engineering

7. The following Diff-Serv TE parameters are configured globally under the **diffserv-te** node. They apply to all RSVP interfaces on the system. Once configured, these parameters can only be changed after shutting down the MPLS and RSVP protocols:

   a. Definition of TE classes, TE Class = {Class Type (CT), LSP priority}. Eight TE classes can be supported. There is no default TE class once Diff-Serv is enabled. The operator must explicitly define each TE class. However, when Diff-Serv is disabled there will be an internal use of the default CT (CT0) and eight pre-emption priorities as shown in Table 3.

Table 3: Internal TE Class Definition when Diff-Serv TE is Disabled

Class Type (CT internal)	LSP Priority
0	7
0	6
0	5
0	4
0	3
0	2
0	1
0	0

b. A mapping of the system forwarding class to CT. The default settings are shown in Table 4.

Table 4: Default Mapping of Forwarding Class to TE Class

FC ID	FC Name	FC Designation	Class Type (CT)
7	Network Control	NC	7
6	High-1	H1	6
5	Expedited	EF	5
4	High-2	H2	4
3	Low-1	L1	3
2	Assured	AF	2
1	Low-2	L2	1
0	Best Effort	BE	0

c. Configuration of the percentage of RSVP interface bandwidth each CT shares, for example, the Bandwidth Constraint (BC), using the **class-type-bw** command. The absolute value of the CT share of the interface bandwidth is derived as the percentage of the bandwidth advertised by IGP in the maximum reservable link bandwidth TE parameter, for example, the link bandwidth multiplied by the RSVP interface **subscription** *percentage* parameter. Note that this configuration also exists at the RSVP interface level and the interface specific configured value overrides the global configured value. The BC value can be changed at any time. The operator can specify the BC for a CT which is not used in any of the TE class definition but that does not get used by any LSP originating or transiting this node.

d. Configuration of the Admission Control Policy to be used: only the Maximum Allocation Model (MAM) is supported. The MAM value represents the bandwidth constraint models for the admission control of an LSP reservation to a link.

RSVP Interface Level

The following are the configuration steps at the RSVP interface level:

1. The operator configures the percentage of RSVP interface bandwidth each CT shares, for example, the BC, using the **class-type-bw** command. The value entered at the interface level overrides the global value configured under the **diffserv-te** node.
2. The operator can overbook (underbook) the maximum reservable bandwidth of a given CT by overbooking (underbooking) the interface maximum reservable bandwidth via configuring the appropriate value for the **subscription** *percentage* parameter in the **config>router>rsvp>interface** context.
3. .Both the BC value and the subscription parameter can be changed at any time.

LSP and LSP Path Levels

The following are the configuration steps at the LSP and LSP path levels:

1. The operator configures the CT in which the LSP belongs by configuring the **class-type** *ct-number* command at the LSP level and/or the path level. The path level value overrides the LSP level value. By default, an LSP belongs to CT0.
2. Only one CT per LSP path is allowed per RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*. A multi-class LSP path is achieved through mapping multiple system Forwarding Classes to a CT.
3. The signaled CT of a dynamic bypass must always be CT0 regardless of the CT of the primary LSP path. The setup and hold priorities must be set to default values, for example, 7 and 0 respectively. This assumes that the operator configured a couple of TE classes, one which combines CT0 and a priority of 7 and the other which combines CTO and a priority of 0. If not, the bypass LSP will not be signaled and will go into the down state.
4. The operator cannot configure the CT, setup priority, and holding priority of a manual bypass. They are always signaled with CT0 and the default setup and holding priorities.
5. The signaled CT, setup priority and holding priority of a detour LSP matches those of the primary LSP path it is associated with.
6. The operator can also configure the setup and holding priorities for each LSP path.
7. An LSP which does not have the CT explicitly configured will behave like a CT0 LSP when Diff-Serv is enabled.

If the operator configured a combination of a CT and a setup priority and/or a combination of a CT and a holding priority for an LSP path that are not supported by the user-defined TE classes, the LSP path will be kept in a down state and error code will be shown within the show command output for the LSP path.

Diff-Serv TE LSP Class Type Change under Failure

An option to configure a main Class Type (CT) and a backup CT for the primary path of a Diff-Serv TE LSP is provided. The main CT is used under normal operating conditions, for example, when the LSP is established the first time and when it gets re-optimized due to timer based or manual re-signal. The backup CT is used when the LSP retries under failure.

The use of backup Class Type (CT) by an LSP is enabled by executing the **config>router>mpls>lsp>primary>backup-class-type** *ct-number* command at the LSP primary path level.

When this option is enabled, the LSP will use the CT configured using the following commands (whichever is inherited at the primary path level) as the main CT:

- **config>router>mpls>lsp>class-type** *ct-number*
- **config>router>mpls>lsp>primary>class-type** *ct-number*

The main CT is used at initial establishment and during a manual or a timer based re-signal Make-Before-Break (MBB) of the LSP primary path. The backup CT is used temporarily to signal the LSP primary path when it fails and goes into retry.

Note that any valid values may be entered for the backup CT and main CT, but they cannot be the same. No check is performed to make sure that the backup CT is a lower CT in Diff-Serv Russian-Doll Model (RDM) admission control context.

The secondary paths of the same LSP are always signaled using the main CT as in existing implementation.

LSP Primary Path Retry Procedures

This feature behaves according to the following procedures.

- When a LSP primary path retries due a failure, for example, it fails after being in the up state, or undergoes any type of MBB, MPLS will retry a new path for the LSP using the main CT. If the first attempt failed, the head-end node performs subsequent retries using the backup CT. This procedure must be followed regardless if the currently used CT by this path is the main or backup CT. This applies to both CSPF and non-CSPF LSPs.
- The triggers for using the backup CT after the first retry attempt are:
  - → A local interface failure or a control plane failure (hello timeout, etc.).
  - → Receipt of a PathErr message with a notification of a FRR protection becoming active downstream and/or receipt of a Resv message with a ‘Local-Protection-In-Use’ flag set. This invokes the FRR Global Revertive MBB.

→ Receipt of a PathErr message with error code=25 ("Notify") and sub-code=7 ("Local link maintenance required") or a sub-code=8 ("Local node maintenance required"). This invokes the TE Graceful Shutdown MBB. Note that in this case, only a single attempt is performed by MBB as in current implementation; only the main CT will be retried.

→ Receipt of a Resv refresh message with the ‘Preemption pending’ flag set or a PathErr message with error code=34 ("Reroute") and a value=1 ("Reroute request soft preemption"). This invokes the soft pre-emption MBB.

→ Receipt of a ResvTear message.

→ A configuration change MBB.

- When an unmapped LSP primary path goes into retry, it uses the main CT until the number of retries reaches the value of the new main-ct-retry-limit parameter. If the path did not come up, it must start using the backup CT at that point in time. By default, this parameter is set to infinite value. The new main-ct-retry-limit parameter has no effect on an LSP primary path, which retries due to a failure event. This parameter is configured using the following command: config>router>mpls>lsp>main-ct-retry-limit. If the user entered a value of the main-ct-retry-limit parameter that is greater than the LSP retry-limit, the number of retries will still stop when the LSP primary path reaches the value of the LSP retry-limit. In other words, the meaning of the LSP retry-limit parameter is not changed and always represents the upper bound on the number of retries. The unmapped LSP primary path behavior applies to both CSPF and non-CSPF LSPs.
- An unmapped LSP primary path is a path that never received a Resv in response to the first path message sent. This can occur when performing a “shut/no-shut” on the LSP or LSP primary path or when the node reboots. An unmapped LSP primary path goes into retry if the retry timer expired or the head-end node received a PathErr message before the retry timer expired.
- When the clear>router>mpls>lsp command is executed, the retry behavior for this LSP is the same as in the case of an unmapped LSP.
- If the value of the parameter main-ct-retry-limit is changed, the new value will only be used at the next time the LSP path is put into a “no-shut” state.
- The following is the behavior when the user changes the main or backup CT:

→ If the user changes the LSP level CT, all paths of the LSP are torn down and re-signaled in a break-before-make fashion. Specifically, the LSP primary path will be torn down and re-signaled even if it is currently using the backup CT.

→ If the user changes the main CT of the LSP primary path, the path will be torn down and re-signaled even if it is currently using the backup CT.

→ If the user changes the backup CT of an LSP primary path when the backup CT is in use, the path is torn down and is re-signaled.

  - → If the user changes the backup CT of an LSP primary path when the backup CT is not in use, no action is taken. If however, the path was in global Revertive, gshut, or soft pre-emption MBB, the MBB is restarted. This actually means the first attempt will be with the main CT and subsequent ones, if any, with the new value of the backup CT.
  - → Consider the following priority of the various MBB types form highest to lowest: Delayed Retry, Preemption, Global Revertive, Configuration Change, and TE Graceful Shutdown. If an MBB request occurs while a higher priority MBB is in progress, the latter MBB will be restarted. This actually means the first attempt will be with the main CT and subsequent ones, if any, with the new value of the backup CT.
- If the least-fill option is enabled at the LSP level, then CSPF must use least-fill equal cost path selection when the main or backup CT is used on the primary path.
- When the re-signal timer expires, CSPF will try to find a path with the main CT. The head-end node must re-signal the LSP even if the new path found by CSPF is identical to the existing one since the idea is to restore the main CT for the primary path. If a path with main CT is not found, the LSP remains on its current primary path using the backup CT. This means that the LSP primary path with the backup CT may no longer be the most optimal one. Furthermore, if the least-fill option was enabled at the LSP level, CSPF will not check if there is a more optimal path, with the backup CT, according to the least-fill criterion and will thus raise no trap to indicate the LSP path is eligible for least-fill re-optimization.
- When the user performs a manual re-signal of the primary path, CSPF will try to find a path with the main CT. The head-end node must re-signal the LSP as in current implementation.
- If a CPM switchover occurs while an the LSP primary path was in retry using the main or backup CT, for example, was still in operationally down state, the path retry will be restarted with the main CT until it comes up. This is because the LSP path retry count is not synchronized between the active and standby CPMs until the path becomes up.
- When the user configured secondary standby and non-standby paths on the same LSP, the switchover behavior between primary and secondary is the same as in existing implementation.

This feature is not supported on a P2MP LSP.

Bandwidth Sharing Across Class Types

In order to allow different levels of booking of network links under normal operating conditions and under failure conditions, it is necessary to allow sharing of bandwidth across class types.

This feature introduces the Russian-Doll Model (RDM) Diff-Serv TE admission control policy described in RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*. This mode is enabled using the following command: **config>router>rsvp>diffserv-te rdm**.

The Russian Doll Model (RDM) LSP admission control policy allows bandwidth sharing across Class Types (CTs). It provides a hierarchical model by which the reserved bandwidth of a CT is the sum of the reserved bandwidths of the numerically equal and higher CTs.

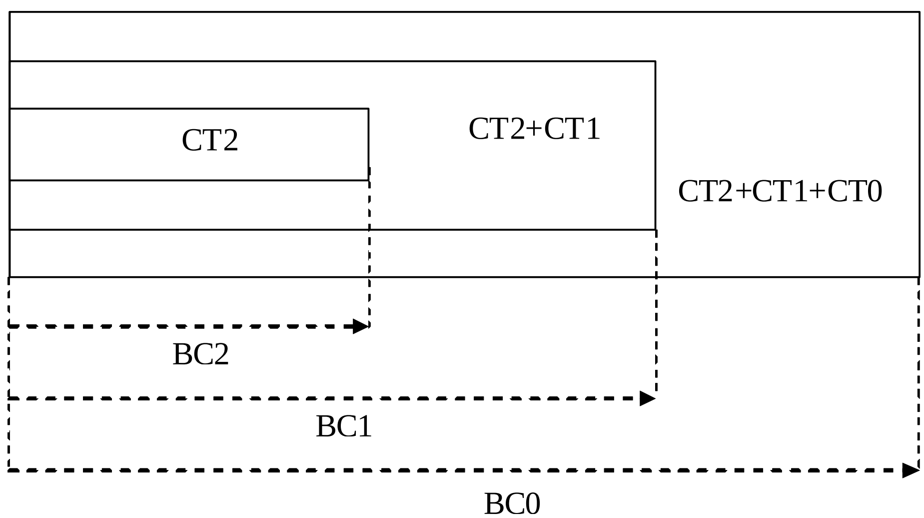

Figure 10: RDM Admission Control Policy Example

CT2 has a bandwidth constraint BC2 which represents a percentage of the maximum reservable link bandwidth. Both CT2 and CT1 can share BC1 which is the sum of the percentage of the maximum reservable bandwidth values configured for CT2 and CT1 respectively. Finally, CT2, CT1, and CT0 together can share BC0 which is the sum of the percentage of the maximum reservable bandwidth values configured for CT2, CT1, and CT0 respectively. The maximum value for BC0 is of course the maximum reservable link bandwidth.

What this means in practice is that CT0 LSPs can use up to BC0 in the absence of LSPs in CT1 and CT2. When this occurs and a CT2 LSP with a reservation less than or equal to BC2 requests admission, it is only admitted by pre-empting one or more CT0 LSPs of lower holding priority than this LSP setup priority. Otherwise, the reservation request for the CT2 LSP will be rejected.

It is required that multiple paths of the same LSP share common link bandwidth since they are signaled using the Shared Explicit (SE) style. Specifically, two instances of a primary path, one with the main CT and the other with the backup CT, must temporarily share bandwidth while MBB is in progress. Also, a primary path and one or many secondary paths of the same LSP must share bandwidth whether they are configured with the same or different CTs.

Downgrading the CT of Bandwidth Sharing LSP Paths

Consider a link configured with two class types CT0 and CT1 and making use of the RDM admission control model as shown in Figure 11.

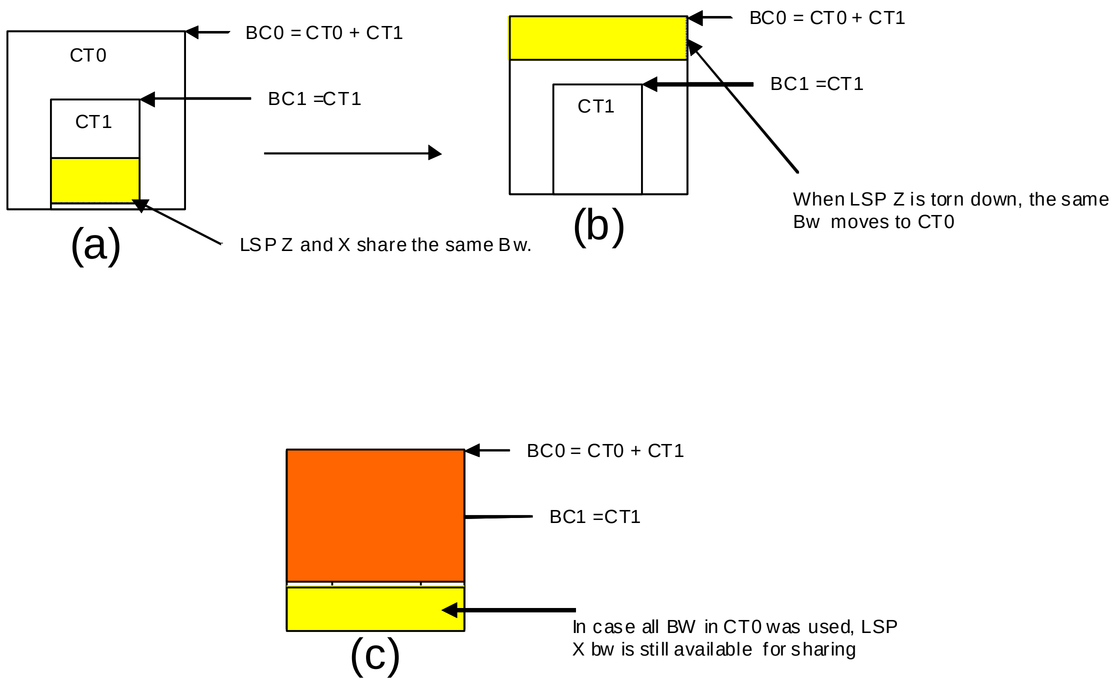

Figure 11: Sharing bandwidth when an LSP primary path is downgraded to backup CT

Consider an LSP path Z occupying bandwidth B at CT1. BC0 being the sum of all CTs below it, the bandwidth occupied in CT1 is guaranteed to be available in CT0. Thus when new path X of the same LSP for CT0 is setup, it will use the same bandwidth B as used by path Z as shown in Figure 11 (a). When path Z is torn down the same bandwidth now occupies CT0 as shown in Figure 11 (b). Even if there were no new BW available in CT0 as can be seen in Figure 11 (c), path X can always share the bandwidth with path Z.

CSPF at the head-end node and CAC at the transit LSR node will share bandwidth of an existing path when its CT is downgraded in the new path of the same LSP.

Upgrading the CT of Bandwidth Sharing LSP Paths

When upgrading the CT the following issue can be apparent. Assume an LSP path X exists with CT0. An attempt is made to upgrade this path to a new path Z with CT1 using an MBB.

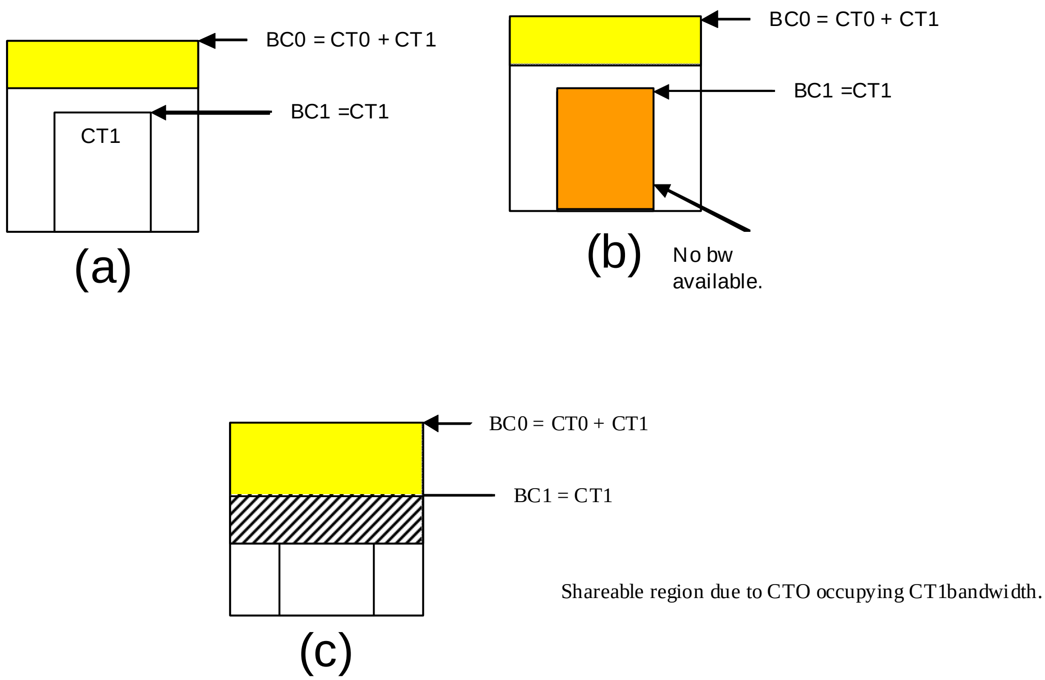

Figure 12: Sharing Bandwidth When an LSP Primary Path is Upgraded to Main CT

In Figure 12 (a), if the path X occupies the bandwidth as shown it can not share the bandwidth with the new path Z being setup. If a condition exists, as shown in Figure 12, (b) the path Z can never be setup on this particular link.

Consider Figure 12 (c). The CT0 has a region that overlaps with CT1 as CT0 has incursion into CT1. This overlap can be shared. However, in order to find whether such an incursion has occurred and how large the region is, it is required to know the reserved bandwidths in each class. Currently, IGP-TE advertises only the unreserved bandwidths. Hence, it is not possible to compute these overlap regions at the head end during CSPF. Moreover, the head end needs to then try and mimic each of the traversed links exactly which increases the complexity.

CSPF at the head-end node will only attempt to signal the LSP path with an upgraded CT if the advertised bandwidth for that CT can accommodate the bandwidth. In other words, it will assume that in the worst case this path will not share bandwidth with another path of the same LSP using a lower CT.

Advanced MPLS/RSVP Features

LSP Path Change

The **tools perform router mpls update-path** {**lsp** *lsp-name* **path** *current-path-name* **new-path** *new-path-name*} command instructs MPLS to replace the path of the primary or secondary LSP.

The primary or secondary LSP path is indirectly identified via the current-path-name value. In existing implementation, the same path name cannot be used more than once in a given LSP name.

This command is also supported on an SNMP interface.

This command applies to both CSPF LSP and to a non-CSPF LSP. However, it will only be honored when the specified current-path-name has the adaptive option enabled. The adaptive option can be enabled the LSP level or at the path level.

The new path must be first configured in CLI or provided via SNMP. The **configure router mpls path** *path-name* CLI command is used to enter the path.

The command fails if any of the following conditions are satisfied:

- The specified current-path-name of this LSP does not have the adaptive option enabled.
- The specified new-path-name value does not correspond to a previously defined path.
- The specified new-path-name value exists but is being used by any path of the same LSP, including this one.

When the command is executed, MPLS performs the following procedures:

- MPLS performs a single MBB attempt to move the LSP path to the new path.
- If the MBB is successful, MPLS updates the new path.
  - → MPLS writes the corresponding NHLFE in the data path if this path is the current backup path for the primary.

    → If the current path is the active LSP path, it will update the path, write the new NHLFE in the data path, which will cause traffic to switch to the new path.

- If the MBB is not successful, the path retains it current value.
- The update-path MBB has the same priority as the manual re-signal MBB.

RSVP-TE LSP Shortcut for IGP Resolution

RSVP-TE LSP shortcut for IGP route resolution allows forwarding of packets to IGP learned routes using an RSVP-TE LSP. This is also referred to as IGP shortcut. The use of RSVP-TE shortcut for resolving IGP routes is enabled by entering the following command at the IS-IS routing protocol level or at the OSPF routing protocol instance level:

- **config>router>isis>rsvp-shortcut**
- **config>router>ospf>rsvp-shortcut.**

These commands will instruct IS-IS and OSPF to include RSVP LSPs originating on this node and terminating on the router-id of a remote node as direct links with a metric equal to the operational metric provided by MPLS. By default, rsvp-shortcut is disabled in all IGP instances.

When rsvp-shortcut is enabled at the IGP instance level, all RSVP LSPs originating on this node are eligible by default as long as the destination address of the LSP as configured in config>router>mpls>lsp>to corresponds to a router-id of a remote node. RSVP LSPs with a destination address corresponding to an interface address of a remote node are automatically not considered by IS-IS or OSPF. It is possible to exclude a specific RSVP LSP from being used as a shortcut for resolving IGP routes by entering the **config>router>mpls>lsp>no igp-shortcut** command:

Also, the SPF in OSPF or IS-IS will only use RSVP LSPs as IGP shortcuts or as endpoints for LDP-over-RSVP. These applications of RSVP LSPs are mutually exclusive at the IGP instance level. If the user enabled both options at the IGP instance level, then the shortcut application takes precedence when the LSP level configuration has both options enabled.

The user can enable LDP-over-RSVP in IGP using the following commands:

- **config>router>isis>ldp-over-rsvp**
- **config>router>ospf>ldp-over-rsvp**

LDP-over-RSVP can be enabled/disabled at the RSVP LSP level using the following command:

- **config>router>mpls>lsp>**[**no**] **ldp-over-rsvp**

Table 5 provides the outcome of the configuration of the ldp-over-rsvp and rsvp-shortcut or igp-shortcut options at both the IGP instance level and at the LSP level. Whenever both options are enabled, the RSVP shortcut feature takes precedence and the RSVP LSP is used as a shortcut.

Table 5: Outcome of Configuration of LDP-over-LSP and RSVP-Shortcut or IGP-Shortcut

	IGP Instance resvp-shortcut enabled / ldp-over-rsp enabled	IGP Instance rsvp-shortcut enabled / ldp-over-rsvp disabled	IGP Instance rsvp-shortcut disabled / ldp-over-rsvp enabled	IGP Instance rsvp-shortcut disabled / ldp-over-rsvp disabled
LSP igp-shortcut enabled / ldp-over-rsvp enabled	Shortcut (Override case)	Shortcut (Override case)	LDP-over-RSVP	None
LSP igp-shortcut enabled / ldp-over-rsvp disabled	Shortcut	Shortcut	None	None
LSP igp-shortcut disabled / ldp-over-rsvp enabled	None	None	LDP-over-RSVP	None
LSP igp-shortcut disabled / ldp-over-rsvp disabled	None	None	None	None

RSVP-TE LSP Shortcut Forwarding Plane

When an IPv4 packet is received on an ingress network interface, a subscriber IES interface, or a regular IES interface, the lookup of the packet in RTM will result in the resolution of the packet to an RSVP LSP if all the following conditions are satisfied:

- RSVP shortcut is enabled on the IGP routing protocol which has a route for the packet’s destination address.
- SPF has pre-determined that the IGP path cost using the RSVP LSP shortcut is the best.

In this case, the packet is sent labeled with the label stack corresponding to the NHLFE of the RSVP LSP.

The failure of an RSVP LSP shortcut or of a local interface triggers a full SPF computation which may result in installing a new route over another RSVP LSP shortcut or a regular IP next-hop.

Note that if FRR is enabled on the RSVP LSP, the switchover of the shortcut packets from the failed primary path to the FRR bypass or detour backup path must be compatible with the ingress LER performance for service packets.

ECMP Considerations

When ECMP is enabled and multiple equal-cost paths exist for the IGP route, the ingress IOM will spray the packets for this route based on hashing routine currently supported for IPv4 packets. Spraying will be performed across a regular IP next-hop and across an RSVP shortcut next-hop as long as the IP path does not go over the tail-end of the RSVP LSP.

Handling of Control Packets

All control plane packets which require an RTM lookup and which destination is reachable over the RSVP shortcut will be forwarded over the shortcut. This is because RTM keeps a single route entry for each prefix except if there is ECMP over different outgoing interfaces.

Interface bound control packets are not impacted by the RSVP shortcut since RSVP LSPs with a destination address different than the router-id are not included by IGP in its SPF calculation.

Handling of Multicast Packets

Multicast packets cannot be forwarded or received from a P2P RSVP LSP. This is because there is no support for the configuration of such an LSP as a tunnel interfaces in PIM. Only an RSVP P2MP LSP is currently allowed. If a multicast packet is received over the physical interface and the RPF check indicates the source is reachable over an RSVP shortcut, the RPF check.

Thus, it is important to make sure that RSVP shortcuts are not enabled in the path to the multicast source.

Advertising LSP Tunnel Links in IGP

If configured, LSP shortcut must also be advertised into IGP similar to regular links such that other routers in the network can include it into their SPF computations. An LSP must exist in the reverse direction in order for the advertised link to pass the bi-directional link check and be usable by other routers in the network. However, this is not requierd for the node which originates the LSP. The LSP is advertised as an unnumbered point-to-point link and the link LSP/LSA has no Traffic Engineering opaque sub-TLVs as per RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*.

The advertisement of RSVP LSP shortcuts into IGP is configured using the following commands:

- **config>router>isis>advertise-tunnel-links**
- **config>router>ospf>advertise-tunnel-links**

By default, RSVP LSP shortcuts are not advertised into IGP.

LDP Forwarding over RSVP LSP Shortcut

The user can enable LDP FECs over RSVP-TE shortcuts by configuring T-LDP sessions to the destination of the RSVP LSP shortcuts. In this case, LDP FEC is tunneled over the RSVP LSP, effectivley implementing LDP-over-RSVP without having to enable the ldp-over-rsvp feature in OSPF or IS-IS. The ldp-over-rsvp and igp-shortcut options are mutually exclusive under OSFP or IS-IS.

Disabling TTL Propagation in an LSP Shortcut

This feature provides the option for disabling TTL propagation from a transit or a locally generated IP packet header into the LSP label stack when an RSVP LSP is used as a shortcut for BGP next-hop resolution, a static-route next-hop resolution, or for an IGP route resolution.

A transit packet is a packet received from an IP interface and forwarded over the LSP shortcut at ingress LER.

A locally-generated IP packet is any control plane packet generated from the CPM and forwarded over the LSP shortcut at ingress LER.

TTL handling can be configured for all RSVP LSP shortcuts originating on an ingress LER using the following global commands:

config>router>mpls>[no] shortcut-transit-ttl-propagate
config>router>mpls>[no] shortcut-local-ttl-propagate

These commands apply to all RSVP LSPs which are used to resolve static routes, BGP routes, and IGP routes.

When the **no** form of the above command is enabled for local packets, TTL propagation is disabled on all locally generated IP packets, including ICMP Ping, traceroute, and OAM packets that are destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack. This is referred to as pipe mode.

Similarly, when the **no** form is enabled for transit packets, TTL propagation is disabled on all IP packets received on any IES interface and destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack.

Dynamic RSVP LSP Signaling using Templates

This feature dynamically establishes LSP to far-end PE node that can be detected based on auto-discovery method, and enables the use of traffic engineering options available in RSVP-TE by using a template that is defined and bound to the client application.

VPN applications like VPRN and VPLS provide L3 and L2 connectivity across multiple sites. As new sites are setup, a configuration changes are required in the provider node to establish connectivity to equipments in the new site. If an LSP is not available to provide transport to the far-end PE node, or existing LSPs are not meeting SLA then a new LSP must be established from the ingress PE node to the far-end connected to the new site.

If an LSP is not available to provide transport to the far-end PE node (or existing LSPs are not meeting SLA assured) then a new LSP must be established from the ingress PE node to the far-end connected to customer site. Currently, an explicit static LSP must be configured to take advantage of traffic engineering tools available to signal RSVP-TE LSP. There is no provision to dynamically establish an LSP to a far-end that can be detected based on auto-discovery.

Multicast application in VPN also require support from the provider network to be able to connect to sites receiving multicast data streams. On learning a new multicast tree instance or based on data rate threshold, a P2MP LSP or an S2L is signaled and added to the tree dynamically. In a single MVPN instance, multiple P2MP LSPs may be required to connect a subset of receiver nodes based on C-group and data threshold rate defined for each.

Dynamic LSP Signaling using Templates

To allow signaling of LSP dynamically and also be able to use traffic engineering options available in RSVP-TE, a template is defined and bound to the client application. LSP template is based on type of LSP to be established. Client application binding to LSP template is based on type of LSP required. Binding a template defined for P2MP LSP is allowed only when multi-point LSP is required, and P2P LSP template when LSP is required between 2 PE nodes.

LSP template has options for all parameters available under an instance of static configuration of RSVP-TE LSP. An LSP established based on template must meet all constraints defined in template. If all constraints are not met then LSP retries after expiration of retry-time.

LSP Template

An LSP template is a construct defined as a guideline to create and signal multiple LSP instances. On request from client application, a new instance of LSP is created and signaled. LSP template has options for all parameters available under an instance of static configuration of RSVP-TE LSP.

No configuration changes must be allowed to LSP instance that is created based on the template.

LSP Template has 2 levels of definition:

1. LSP template global parameters - TE parameters applied to all LSP instances created based on template.

2. LSP template path bindings - a construct that has a prefix-range and TE parameters.
   - → TE parameter of a path binding is applied to an LSP signaled to a far-end if the far-end IP address is within the path prefix range.
   - → If multiple path prefix ranges are matched then the path with most specific IP match is be used.
   - → If the prefix-range does not match any path then the default-path TE parameters is applied.
   - → A default-path is defined for a template to be available to setup LSP.
   - → LSP template name “lsp-template-name” is used as a key to create a template container. “lsp-template-name” and “lsp-name” cannot be the same.
   - → Global LSP template parameters that is applied to all LSP instances are: adaptive, bandwidth, cspf, fast-reroute, hop-limit, record-label and retry-timer.
   - → Path specific TE parameters include: hop-list, exclude, and include of admin-groups.

LSP and LSP PATH Instance Based on Template

An LSP instance is defined upon a request from client application, and MIB object is populated for each LSP created based on the template. The CLI configuration is not allowed on dynamic LSP instance. “config router mpls lsp” for dynamic LSP is blocked and an error is logged on the console for the user.

The MIB object is read only and SNMP rejects SET call to modify the MIB object created for LSP instance.For each LSP instance, a LSP PATH is defined and MIB object is populated. The MIB object is read only and SNMP rejects SET call to modify the MIB object created for LSP PATH instance.

Lastly, Persistence index for statically configured LSP is strictly followed, and dynamic template based LSP is signaled after a configuration script for LSP has finished loading.

Shared Risk Link Groups

Shared Risk Link Groups (SRLGs) is a feature that allows the user to establish a backup secondary LSP path or a FRR LSP path which is disjoint from the path of the primary LSP. Links that are members of the same SRLG represent resources sharing the same risk, for example, fiber links sharing the same conduit or multiple wavelengths sharing the same fiber.

When the SRLG option is enabled on a secondary path, CSPF includes the SRLG constraint in the computation of the secondary LSP path. This requires that the primary LSP already be established and up since the head-end LER needs the most current ERO computed by CSPF for the primary path. CSPF would return the list of SRLG groups along with the ERO during primary path CSPF computation. At a subsequent establishment of a secondary path with the SRLG constraint, the MPLS/RSVP task will query again CSPF providing the list of SLRG group numbers to be avoided. CSPF prunes all links with interfaces which belong to the same SRLGs as the interfaces included in the ERO of the primary path. If CSPF finds a path, the secondary is setup. If not, MPLS/RSVP will keep retrying the requests to CSPF.

When the SRLG option is enabled on FRR, CSPF includes the SRLG constraint in the computation of a FRR detour or bypass for protecting the primary LSP path. CSPF prunes all links with interfaces which belong to the same SRLG as the interface which is being protected, for example, the outgoing interface at the PLR the primary path is using. If one or more paths are found, the MPLS/RSVP task will select one based on best cost and will signal the bypass/detour. If not and the user included the strict option, the bypass/detour is not setup and the MPLS/RSVP task will keep retrying the request to CSPF. Otherwise, if a path exists which meets the other TE constraints, other than the SRLG one, the bypass/detour is setup.

A bypass or a detour LSP path is not guaranteed to be SRLG disjoint from the primary path. This is because only the SRLG constraint of the outgoing interface at the PLR that the primary path is using is avoided.

Enabling Disjoint Backup Paths

A typical application of the SRLG feature is to provide for an automatic placement of secondary backup LSPs or FRR bypass/detour LSPs that minimizes the probability of fate sharing with the path of the primary LSP (Figure 13).

The following details the steps necessary to create shared risk link groups:

- For primary/standby SRLG disjoint configuration:
  - → Create an SRLG-group, similar to admin groups.
  - → Link the SRLG-group to MPLS interfaces.

→ Configure primary and secondary LSP paths and enable SRLG on the secondary LSP path. Note that the SRLG secondary LSP path(s) will *always* perform a strict CSPF query. The **srlg-frr** command is irrelevant in this case (see srlg-frr on page 144).

- For FRR detours/bypass SRLG disjoint configuration:

→ Create an SRLG group, similar to admin groups.

→ Link the SRLG group to MPLS interfaces.

→ Enable the **srlg-frr** (strict/non-strict) option, which is a system-wide parameter, and it force every LSP path CSPF calculation, to take the configured SRLG membership(s) (and propagated through the IGP opaque-te-database) into account.

→ Configure primary FRR (one-to-one/facility) LSP path(s). Consider that each PLR will create a detour/bypass that will only avoid the SRLG membership(s) configured on the primary LSP path egress interface. In a one-to-one case, detour-detour merging is out of the control of the PLR, thus the latter will not ensure that its detour will be prohibited to merge with a colliding one. For facility bypass, with the presence of several bypass type to bind to, the following priority rules will be followed:

1. Manual bypass disjoint
2. Manual bypass non-disjoint (eligible only if srlg-frr is non-strict)
3. Dynamic disjoint
4. Dynamic non-disjoint (eligible only if srlg-frr is non-strict)

Non-CSPF manual bypass is not considered.

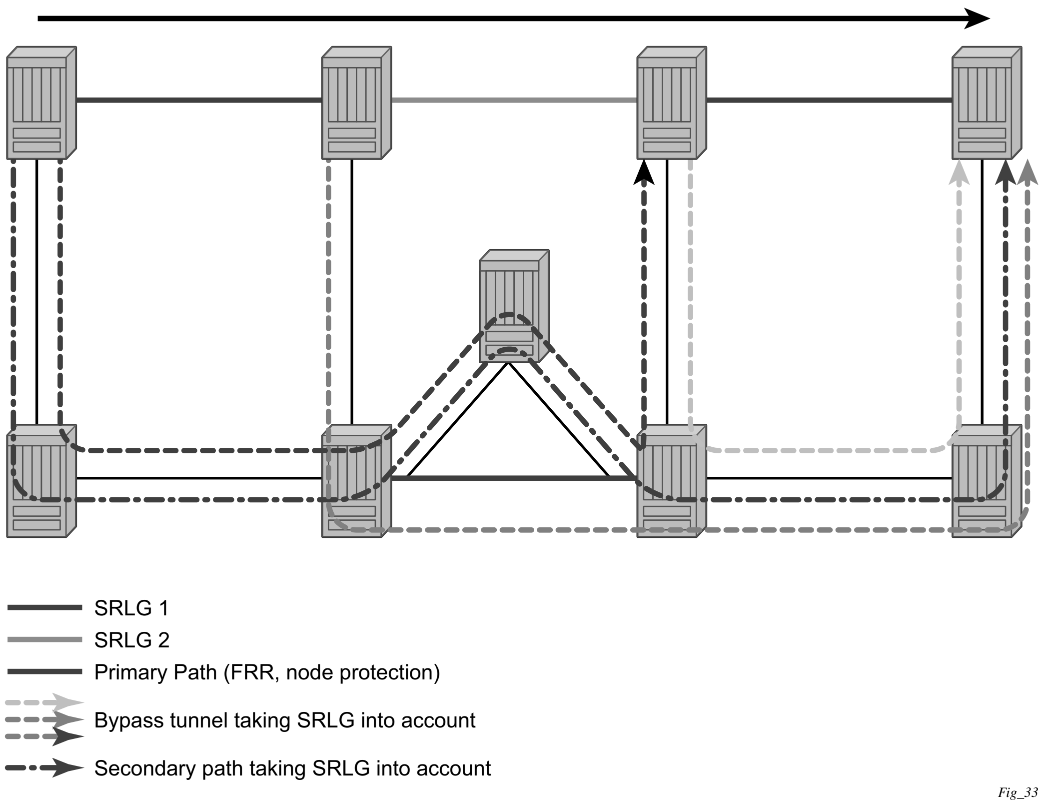

Figure 13: Shared Risk Link Groups

This feature is supported on OSPF and IS-IS interfaces on which RSVP is enabled.

Static Configurations of SRLG Memberships

This feature provides operations with the ability to enter manually the link members of SRLG groups for the entire network at any 7750 SR node which will need to signal LSP paths (for example, a head-end node).

The operator may explicitly enables the use by CSPF of the SRLG database. In that case, CSPF will not query the TE database for IGP advertised interface SRLG information.

Note, however, that the SRLG secondary path computation and FRR bypass/detour path computation remains unchanged.

There are deployments where the 7750 SR will interoperate with routers that do not implement the SRLG membership advertisement via IGP SRLG TLV or sub-TLV.

In these situations, the user is provided with the ability to enter manually the link members of SRLG groups for the entire network at any 7750 SR node which will need to signal LSP paths, for example, a head-end node.

The user enters the SRLG membership information for any link in the network by using the **interface** *ip-int-name* **srlg-group** *group-name* command in the **config>router>mpls> srlg-database>router-id** context. An interface can be associated with up to 5 SRLG groups for each execution of this command. The user can associate an interface with up to 64 SRLG groups by executing the command multiple times. The user must also use this command to enter the local interface SRLG membership into the user SRLG database. The user deletes a specific interface entry in this database by executing the **no** form of this command.

The *group-name* must have been previously defined in the SRLG **srlg-group** *group-name* **value** *group-value* command in the **config>router>mpls**. The maximum number of distinct SRLG groups the user can configure on the system is 1024.

The parameter value for *router-id* must correspond to the router ID configured under the base router instance, the base OSPF instance or the base IS-IS instance of a given node. Note however that a single user SLRG database is maintained per node regardless if the listed interfaces participate in static routing, OSPF, IS-IS, or both routing protocols. The user can temporarily disable the use by CSPF of all interface membership information of a specific router ID by executing the **shutdown** command in the **config>router>mpls> srlg-database> router-id** context. In this case, CSPF will assume these interfaces have no SRLG membership association. The operator can delete all interface entries of a specific router ID entry in this database by executing the **no router-id** *router-address* command in the **config>router>mpls> srlg-database** context.

CSPF will not use entered SRLG membership if an interface is not listed as part of a router ID in the TE database. If an interface was not entered into the user SRLG database, it will be assumed that it does not have any SRLG membership. CSPF will not query the TE database for IGP advertised interface SRLG information.

The operator enables the use by CSPF of the user SRLG database by entering the user-srlg-db enable command in the **config>router>mpls** context. When the MPLS module makes a request to CSPF for the computation of an SRLG secondary path, CSPF will query the local SRLG and computes a path after pruning links which are members of the SRLG IDs of the associated primary path. Similarly, when MPLS makes a request to CSPF for a FRR bypass or detour path to associate with the primary path, CSPF queries the user SRLG database and computes a path after pruning links which are members of the SRLG IDs of the PLR outgoing interface.

The operator can disable the use of the user SRLG database by entering the user-srlg-db disable in command in the **config>router>mpls** context. CSPF will then resumes queries into the TE database for SRLG membership information. However, the user SRLG database is maintained

The operator can delete the entire SRLG database by entering the **no srlg-database** command in the **config>router>mpls** context. In this case, CSPF will assume all interfaces have no SRLG membership association if the user has not disabled the use of this database.

TE Graceful Shutdown

Graceful shutdown provides a method to bulk re-route transit LSPs away from the node during software upgrade of a node. A solution is described in draft-ietf-ccamp-mpls-graceful-shutdown-x.txt, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*. This is achieved in this draft by using a PathErr message with a specific error code Local Maintenance on TE link required flag. When a LER gets this message, it performs a make-before-break on the LSP path to move the LSP away from the links/nodes which IP addresses were indicated in the PathErr message.

Graceful shutdown can flag the affected link/node resources in the TE database so other routers will signal LSPs using the affected resources only as a last resort. This is achieved by flooding an IGP TE LSA/LSP containing link TLV for the links under graceful shutdown with the traffic engineering metric set to 0xffffffff and 0 as unreserved bandwidth.

Soft Pre-emption of Diff-Serv RSVP LSP

A Diff-Serv LSP can pre-empt another LSP of the same or of a different CT if its setup priority is strictly higher (numerically lower) than the holding priority of that other LSP.

Least-Fill Bandwidth Rule in CSPF ECMP Selection

When multiples equal-cost paths satisfy the constraints of a given RSVP LSP path, CSPF in the router head-end node will select a path so that LSP bandwidth is balanced across the network links. In releases prior to R7.0, CSPF used a random number generator to select the path and returned it to MPLS. In the course of time, this method actually balances the number of LSP paths over the links in the network; it does not necessarily balance the bandwidth across those links.

The least-fill path selection algorithm identifies the single link in each of the equal cost paths which has the least available bandwidth in proportion to its maximum reserved bandwidth. It then selects the path which has the largest value of this figure. The net affect of this algorithm is that LSP paths will be spread over the network links over time such that percentage link utilization is balanced. When the least-fill option is enabled on an LSP, during a manual reset CSPF will apply this method to all path calculations of the LSP, also at the time of the initial configuration.

Point-to-Multipoint (P2MP) RSVP LSP

Point-to-multipoint (P2MP) RSVP LSP allows the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network core routers. A P2MP LSP tree is established in the control plane which path consists of a head-end node, one or many branch nodes, and the leaf nodes. Packets injected by the head-end node are replicated in the data plane at the branching nodes before they are delivered to the leaf nodes.

Application in Video Broadcast

Figure 14 illustrates the use of the SR product family in triple play application (TPSDA). The Broadband Service Router (BSR) is a 7750 SR and the Broadband Service Aggregator (BSA) is the 7450 ESS.

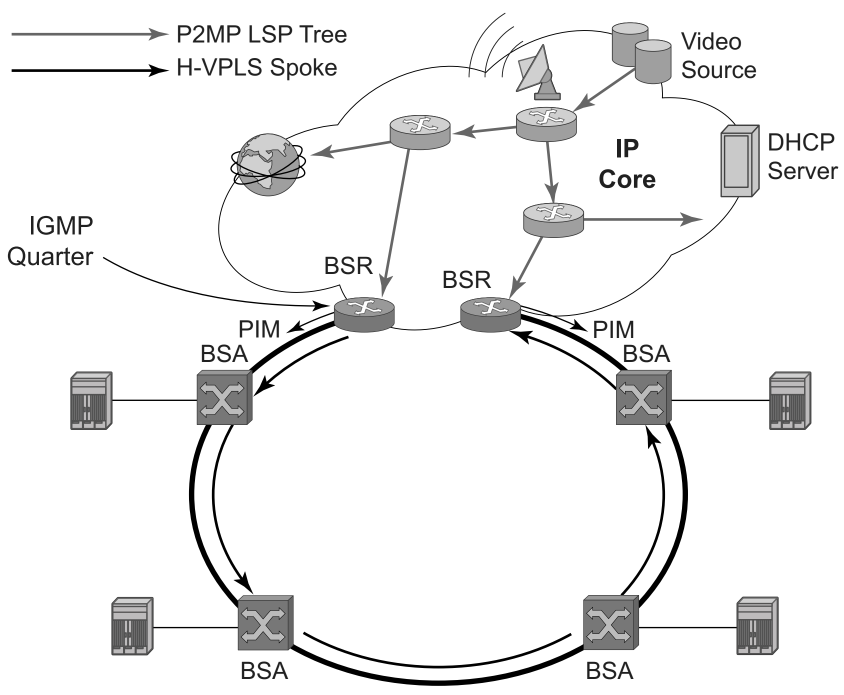

Figure 14: Application of P2MP LSP in Video Broadcast

A PIM-free core network can be achieved by deploying P2MP LSPs using other core routers. The 7750 SR can act as the ingress LER receiving the multicast packets from the multicast source and forwarding them over the P2MP LSP.

A 7750 BSR can act as a leaf for the P2MP LSP tree initiated from the head-end router co-located with the video source. The 7750 can also act as a branch node serving other leaf nodes and supports the replication of multicast packets over P2MP LSPs.

P2MP LSP Data Plane

A P2MP LSP is a unidirectional label switched path (LSP) which inserts packets at the root (ingress LER) and forwards the exact same replication of the packet to one or more leaf nodes (egress LER). The packet can be replicated at the root of P2MP LSP tree and/or at a transit LSR which acts as a branch node for the P2MP LSP tree.

Note that the data link layer code-point, for example Ethertype when Ethernet is the network port, continues to use the unicast codepoint defined in RFC 3032, *MPLS Label Stack Encoding*, and which is used on P2P LSP. This change is specified in draft-ietf-mpls-multicast-encaps, *MPLS Multicast Encapsulations*.

When a router sends a packet over a P2MP LSP which egresses on an Ethernet-based network interface, the Ethernet frame uses a MAC unicast destination address when sending the packet over the primary P2MP LSP instance or over a P2P bypass LSP). Note that a MAC multicast destination address is also allowed in the draft-ietf-mpls-multicast-encaps. Thus, at the ingress network interface on an Ethernet port, the router can accept both types of Ethernet destination addresses.

Procedures at Ingress LER Node

The following procedures occur at the root of the P2MP LSP (head-end or ingress LER node):

1. First, the P2MP LSP state is established via the control plane. Each leaf of the P2MP LSP will have a next-hop label forwarding entry (NHLFE) configured in the forwarding plane for each outgoing interface.

1. The user maps a specific multicast destination group address to the P2MP LSP in the base router instance by configuring a static multicast group under a tunnel interface representing the P2MP LSP.
2. An FTN entry is programmed at the ingress of the head-end node that maps the FEC of a received user IP multicast packet to a list of outgoing interfaces (OIF) and corresponding NHLFEs.
3. The head-end node replicates the received IP multicast packet to each NHLFE. Replication is performed at ingress toward the fabric and/or at egress IOM depending on the location of the OIF.
4. At ingress, the head-end node performs a PUSH operation on each of the replicated packets.

Procedures at LSR Node

The following procedures occur at an LSR node that is not a branch node:

- The LSR performs a label swapping operation on a leaf of the P2MP LSP. This is a conventional operation of an LSR in a P2P LSP. An ILM entry is programmed at the ingress of the LSR to map an incoming label to a NHLFE.

The following is an exception handling procedure for control packets received on an ILM in an LSR.

- Packets that arrive with the TTL in the outer label expiring are sent to the CPM for further processing and are not forwarded to the egress NHLFE.

Procedures at Branch LSR Node

The following procedures occur at an LSR node that is a branch node:

- The LSR performs a replication and a label swapping for each leaf of the P2MP LSP. An ILM entry is programmed at the ingress of the LSR to map an incoming label to a list of OIF and corresponding NHLFEs.
- There is a limit of 127 OIF/NHLFEs per ILM entry.

The following is an exception handling procedure for control packets received on an ILM in a branch LSR:

- Packets that arrive with the TTL in the outer label expiring are sent to the CPM for further processing and not copied to the LSP branches.

Procedures at Egress LER Node

The following procedures occur at the leaf node of the P2MP LSP (egress LER):

- The egress LER performs a pop operation. An ILM entry is programmed at the ingress of the egress LER to map an incoming label to a list of next-hop/OIF.

The following is an exception handling procedure for control packets received on an ILM in an egress LER.

- The packet is sent to the CPM for further processing if there is any of the IP header exception handling conditions set after the label is popped: 127/8 destination address, router alert option set, or any other options set.

Procedures at BUD LSR Node

The following are procedures at an LSR node which is both a branch node and an egress leaf node (bud node):

- The bud LSR performs a pop operation on one or many replications of the received packet and a swap operation of the remaining replications. An ILM entry is programmed at ingress of the LSR to map the incoming label to list of NHLFE/OIF and next-hop/OIF.

  Note however, the exact same packets are replicated to an LSP leaf and to a local interface.

The following are the exception handling procedures for control packets received on an ILM in a bud LSR:

- Packets which arrive with the TTL in the outer label expiring are sent to the CPM and are not copied to the LSP branches.
- Packets whose TTL does not expire are copied to all branches of the LSP. The local copy of the packet is sent to the CPM for further processing if there is any of the IP header exception handling conditions set after the label is popped: 127/8 destination address, router alert option set, or any other options set.

Ingress Path Management for P2MP LSP Packets

The 7750 SR provides the ingress multicast path management (IMPM) capability that allows users to manage the way IP multicast streams are forwarded over the router's fabric and to maximize the use of the fabric multicast path capacity.

IMPM consists of two components, a bandwidth policy and a multicast information policy. The bandwidth policy configures the parameters of the multicast paths to the fabric. This includes the rate limit and the multicast queue parameters of each path. The multicast information policy configures the bandwidth and preference parameters of individual multicast flows corresponding to a channel, for example, a <*,G> or a <S,G>, or a bundle of channels.

By default, both the IOM-2 and IOM-3 ingress data path provide two multicast paths through the fabric referred to as high-priority path and low-priority path respectively. When a multicast packet is received on an ingress network or access interface or on a VPLS SAP, the packet's classification will determine its forwarding class and priority or profile as per the ingress QoS policy. This then determines which of the SAP or interface multicast queues it must be stored in. By default SAP and interface expedited forwarding class queues forward over the high-priority multicast path and the non expedited forwarding class queues forward over the low-priority multicast path.

When IMPM on the ingress MDA is enabled, one or more multicast paths are enabled depending on the IOM type. In addition, multicast flows managed by IMPM will be stored in a separate shared multicast queue for each multicast path. These queues are configured in the bandwidth policy.

IMPM maps a packet to one of the paths dynamically based on monitoring the bandwidth usage of each packet flow matching a <*,G> or <S,G> record. The multicast bandwidth manager assigns multicast flows to a primary path, and ancillary path for IOM-2, based on the flow preference until the rate limits of each path is reached. At that point in time, a multicast flow is mapped to the secondary flow. If a path congests, the bandwidth manager will remove and black-hole lower preference flows to guarantee bandwidth to higher preference flows. The preference of a multicast flow is configured in the multicast info policy.

A packet received on a P2MP LSP ILM is managed by IMPM when IMPM is enabled on the ingress MDA and the packet matches a specific multicast record. When IMPM is enabled but the packet does not match a multicast record, or when IMPM is disabled, a packet received on a P2MP LSP ILM is mapped to a multicast path differently depending if the ingress IOM is an IOM-2 or IOM-3.

Ingress P2MP Path Management on IOM-3

On an ingress IOM-3, there are 16 multicast paths available to forward multicast packets. Each path has a set of multicast queues and associated with it. Paths 0 and 15 are enabled by default and represent the high-priority and low-priority paths respectively. Each VPLS SAP, access interface, and network interface will have a set of per forwarding class multicast and/or broadcast queues which are defined in the ingress QoS policy associated with them. The expedited queues will be attached to Path 0 while the non-expedited queues will be attached to Path 15.

When IMPM is enabled and/or when a P2MP LSP ILM exists on the ingress IOM-3, the remaining 14 multicast paths are also enabled for a total of 16 paths. The first 15 paths are renamed as primary paths while the 16th path is renamed as a secondary path.

A separate pair of shared multicast queues is created on each of the 15 primary paths, one for IMPM managed packets and one for P2MP LPS packets not managed by IMPM. The secondary path does not forward IMPM managed packets or P2MP LSP packets. These queues have default rate (PIR=CIR) and CBS/MBS/Hi-Priority-Only thresholds but can be changed away from default under the bandwidth policy.

A VPLS snooped packet, a PIM routed packet, or a P2MP LSP packet is managed by IMPM if it matches a <*,G> or a <S,G> multicast record in the ingress IOM-3 forwarding table and IMPM is enabled on the ingress MDA where the packet is received. The user enables IMPM on the ingress MDA data path using the **config>card>mda>ingress>mcast-path-management** command.

A packet received on an IP interface and to be forwarded to a P2MP LSP NHLFE or a packet received on a P2MP LSP ILM is not managed by IMPM when IMPM is disabled on the ingress MDA where the packet is received or when IMPM is enabled but the packet does not match any multicast record. A P2MP LSP packet duplicated at a branch LSR node is an example of a packet not managed by IMPM even when IMPM is enabled on the ingress MDA where the P2MP LSP ILM exists. A packet forwarded over a P2MP LSP at an ingress LER and which matches a <*,G> or a <S<G> is an example of a packet which is not managed by IMPM if IMPM is disabled on the ingress MDA where the packet is received.

When a P2MP LSP packet is not managed by IMPM, it is stored in the unmanaged P2MP shared queue of one of the 15 primary multicast paths.

The above ingress data path procedures apply to packets of a P2MP LSP at ingress LER, LSR, branch LSR, bud LSR, and egress LER. Note that in the presence of both IMPM managed traffic and unmanaged P2MP LSP traffic on the same ingress IOM-3, the user must account for the presence of the unmanaged traffic on the same path when setting the rate limit for an IMPM path in the bandwidth policy.

Ingress P2MP Path Management on IOM-2

The following procedures apply at the ingress data path for packets received from or to be forwarded to a P2MP LSP at ingress LER, LSR, branch LSR, bud LSR, and egress LER.

On ingress IOM-2, there are 3 multicast paths which are available for forwarding multicast packets. Each path has a set of multicast queues and a multicast VoQ associated with it. Paths 0 and 2 are enabled by default and represent the high-priority and low-priority paths respectively. Each VPLS SAP, access interface, and network interface will have a set of per forwarding class multicast and/or broadcast queues which are defined in the ingress QoS policy associated with them. The expedited queues will be attached to Path 0 while the non-expedited queues will be attached to Path 2.

When IMPM is disabled, packets of P2MP LSP arriving on a network interface will be queued in that interface queue corresponding to the forwarding class of the packet.

When the user enables IMPM on the ingress MDA, a third multicast path, referred to as ancillary path, is added on the ingress IOM-2. This path reuses unused capacity from the unicast paths. The high-priority and low-priority paths are renamed as primary and secondary paths respectively.

A VPLS snooped packet or a PIM routed packet is managed by IMPM if it matches a <*,G> or a <S,G> multicast record in the ingress IOM-2 forwarding table and IMPM is enabled on the ingress MDA where the packet is received. The user enables IMPM on the ingress MDA data path using the **config>card>mda>ingress>mcast-path-management** command.

A P2MP LSP packet which matches a multicast record is also managed by IMPM on ingress IOM-2 and is thus distributed to one of the primary, ancillary, or secondary path according to the congestion level of the paths and the preference of the packet's multicast flow as configured in the multicast info policy 2.

RSVP Control Plane in a P2MP LSP

P2MP RSVP LSP is specified in RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)* .

A P2MP LSP is modeled as a set of root-to-leaf (S2L) sub-LSPs. The root, for example the head-end node, triggers signaling using one or multiple path messages. A path message can contain the signaling information for one or more S2L sub-LSPs. The leaf sub-LSP paths are merged at branching points.

A P2MP LSP is identified by the combination of <P2MP ID, tunnel ID, extended tunnel ID> part of the P2MP session object, and <tunnel sender address, LSP ID> fields in the P2MP sender_template object.

A specific sub-LSP is identified by the <S2L sub-LSP destination address> part of the S2L_SUB_LSP object and an ERO and secondary ERO (SERO) objects.

The following are characteristics of this feature:

1. Supports the de-aggregated method for signaling the P2MP RSVP LSP. Each root to leaf is modeled as a P2P LSP in the RSVP control plane. Only data plane merges the paths of the packets.

5. Each S2L sub-LSP is signaled in a separate path message. Each leaf node responds with its own resv message. A branch LSR node will forward the path message of each S2L sub-LSP to the downstream LSR without replicating it. It will also forward the resv message of each S2L sub-LSP to the upstream LSR without merging it with the resv messages of other S2L sub-LSPs of the same P2MP LSP. The same is done for subsequent refreshes of the path and resv states.
6. The node will drop aggregated RSVP messages on the receive side if originated by another vendor’s implementation.
7. The user configures a P2MP LSP by specifying the optional create-time parameter **p2mp-lsp** following the LSP name. Next, the user creates a primary P2MP instance using the keyword **primary-p2mp-instance**. Then a path name of each S2L sub-LSP must added to the P2MP instance using the keyword **s2l-path**. The paths can be empty paths or can specify a list of explicit hops. The path name must exist and must have been defined in the **config>router>mpls>path** context.
8. The same path name can be re-used by more than one S2L of the primary P2MP instance. However the to keyword must have a unique argument per S2L as it corresponds to the address of the egress LER node.
9. The user can configure a secondary instance of the P2MP LSP to backup the primary one. In this case, the user enters the name of the secondary P2MP LSP instance under the same LSP name. One or more secondary instances can be created. The trigger for the head-end node to switch the path of the LSP from the primary P2MP instance to the secondary P2MP instance

is to be determined. This could be based on the number of leaf LSPs which went down at any given time.

10. The following parameters can be used with a P2MP LSP: adaptive, cspf, exclude, fast-reroute, from, hop-limit, include, metric, retry-limit, retry-timer, resignal-timer.
11. The following parameters cannot be used with a P2MP LSP: adspec, primary, secondary, to.
12. The node ingress LER will not inset an adspec object in the path message of an S2L sub-LSP. If received in the resv message, it will be dropped. The operational MTU of an S2L path is derived from the MTU of the outgoing interface of that S2L path.
13. The **to** parameter is not available at the LSP level but at the path level of each S2L sub-LSP of the primary or secondary instance of this P2MP LSP.
14. The hold-timer configured in the **config>router>mpls>hold-timer** context applies when signaling or re-signaling an individual S2L sub-LSP path. It does not apply when the entire tree is signaled or re-signaled.
15. The head-end node can add and/or remove a S2L sub-LSP of a specific leaf node without impacting forwarding over the already established S2L sub-LSPs of this P2MP LSP and without re-signaling them.
16. The head-end node performs a make-before break (MBB) on an individual S2L path of a primary P2MP instance whenever it applies the FRR global revertive procedures to this path. If CSPF finds a new path, RSVP signals this S2L path with the same LSP-ID as the existing path.
17. All other configuration changes, such as adaptive/no-adaptive, use-te-metric, no-frr, cspf/no-cspf, result in the tear-down and re-try of all affected S2L paths as is the case for P2P LSP paths.
18. MPLS requests CSPF to re-compute the whole set of S2L paths of a given active P2MP instance each time the P2MP re-signal timer expires. The P2MP re-signal timer is configured separately from the P2P LSP. MPLS performs a global MBB and moves each S2L sub-LSP in the instance into its new path using a new P2MP LSP ID if the global MBB is successful. This is regardless of the cost of the new S2L path.
19. MPLS will request CSPF to re-compute the whole set of S2L paths of a given active P2MP instance each time the user performs a manual re-signal of the P2MP instance. MPLS then always performs a global MBB and moves each S2L sub-LSP in the instance into its new path using a new P2MP LSP ID if the global MBB is successful. This is regardless of the cost of the new S2L path. The user executes a manual re-signal of the P2MP LSP instance using the command: **tools>perform>router>mpls>resignal p2mp-lsp** *lsp-name* **p2mp-instance** *instance-name*.
20. When performing global MBB, MPLS runs a separate MBB on each S2L in the P2MP LSP instance. If an S2L MBB does not succeed the first time, MPLS will re-try the S2L using the re-try timer and re-try count values inherited from P2MP LSP configuration. However, there will be a global MBB timer set to 600 seconds and which is not configurable. If the global MBB succeeds, for example, all S2L MBBs have succeeded, before the global timer expires, MPLS moves the all S2L sub-LSPs into their new path. Otherwise when this timer expires,

MPLS checks if all S2L paths have at least tried once. If so, it then aborts the global MBB. If not, it will continue until all S2Ls have re-tried once and then aborts the global MBB. Once global MBB is aborted, MPLS will move all S2L sub-LSPs into the new paths only if the set of S2Ls with a new path found is a superset of the S2Ls which have a current path which is up.

21. While make-before break is being performed on individual S2L sub-LSP paths, the P2MP LSP will continue forwarding packets on S2L sub-LSP paths which are not being re-optimized and on the older S2L sub-LSP paths for which make-before-break operation was not successful. MBB will thus result in duplication of packets until the old path is torn down.
22. The MPLS data path of an LSR node, branch LSR node, and bud LSR node will be able to re-merge S2L sub-LSP paths of the same P2MP LSP in case their ILM is on different incoming interfaces and their NHLFE is on the same or different outgoing interfaces. This could occur anytime there are equal cost paths through this node for the S2L sub-LSPs of this P2MP LSP.
23. Link-protect FRR bypass using P2P LSPs is supported. In link protect, the PLR protecting an interface to a branch LSR will only make use of a single P2P bypass LSP to protect all S2L sub-LSPs traversing the protected interface.
24. A manual bypass LSP cannot be used for protecting S2L paths of a P2MP LSP.
25. The following MPLS features do operate with P2MP LSP:
    - BFD on RSVP interface.
    - MD5 on RSVP interface.
    - IGP metric and TE metric for computing the path of the P2MP LSP with CSPF.
    - SRLG constraint for computing the path of the P2MP LSP with CSPF. SRLG is supported on FRR backup path only.
    - TE graceful shutdown.
    - Admin group constraint.

The following MPLS features are not operable with P2MP LSP:

- Class based forwarding over P2MP RSVP LSP.
- LDP-over-RSVP where the RSVP LSP is a P2MP LSP.
- Diff-Serv TE.
- Soft pre-emption of RSVP P2MP LSP.
- Refresh reduction on RSVP interface and on P2P bypass LSP protecting one or more S2L sub-LSPs.

Forwarding Multicast Packets over RSVP P2MP LSP in the Base Router

Multicast packets are forwarded over the P2MP LSP at the ingress LER based on a static join configuration of the multicast group against the tunnel interface associated with the originating P2MP LSP. At the egress LER, packets of a multicast group are received from the P2MP LSP via a static assignment of the specific <S,G> to the tunnel interface associated with a terminating LSP.

Procedures at Ingress LER Node

The forwarding of multicast packets over a P2MP LSP follows the following procedures:

1. The user creates a tunnel interface associated with the P2MP LSP: **configure>router>tunnel-interface rsvp-p2mp** *lsp-name*. The configure>router>pim>tunnel-interface command has been discontinued.

2. The user adds static multicast group joins to the PIM interface, either as a specific <S,G> or as a <*,G>: **configure>router>igmp>tunnel-interface>static>group>source** *ip-address* and **configure>router>igmp>tunnel-interface>static>group>starg**.

The tunnel interface identifier consists of a string of characters representing the LSP name for the RSVP P2MP LSP. Note that MPLS will actually pass to PIM a more structured tunnel interface identifier. The structure will follow the one BGP uses to distribute the PMSI tunnel information in BGP multicast VPN as specified in draft-ietf-l3vpn-2547bis-mcast-bgp, *Multicast in MPLS/BGP IP VPNs* .The format is: <extended tunnel ID, reserved, tunnel ID, P2MP ID> as encoded in the RSVP-TE P2MP LSP session_attribute object in RFC 4875.

The user can create one or more tunnel interfaces in PIM and associate each to a different RSVP P2MP LSP. The user can then assign static multicast group joins to each tunnel interface. Note however that a given <*,G> or <S,G> can only be associated with a single tunnel interface.

A multicast packet which is received on an interface and which succeeds the RPF check for the source address will be replicated and forwarded to all OIFs which correspond to the branches of the P2MP LSP. The packet is sent on each OIF with the label stack indicated in the NHLFE of this OIF. The packets will also be replicated and forwarded natively on all OIFs which have received IGMP or PIM joins for this <S,G>.

The multicast packet can be received over a PIM or IGMP interface which can be an IES interface, a spoke SDP-terminated IES interface, or a network interface.

In order to duplicate a packet for a multicast group over the OIF of both P2MP LSP branches and the regular PIM or IGMP interfaces, the tap mask for the P2MP LSP and that of the PIM based interfaces will need to be combined into a superset MCID.

Procedures at Egress LER Node

Procedures with a Primary Tunnel Interface

The user configures a tunnel interface and associates it with a terminating P2MP LSP leaf using the command: **config>router>tunnel-interface rsvp-p2mp lsp-name sender** *sender-address*. The **configure>router>pim>tunnel-interface** command has been discontinued.

The tunnel interface identifier consists of a couple of string of characters representing the LSP name for the RSVP P2MP LSP followed by the system address of the ingress LER. The LSP name must correspond to a P2MP LSP name configured by the user at the ingress LER and must not contain the special character ":" Note that MPLS will actually pass to PIM a more structured tunnel interface identifier. The structure will follow the one BGP uses to distribute the PMSI tunnel information in BGP multicast VPN as specified in draft-ietf-l3vpn-2547bis-mcast-bgp.The format is: <extended tunnel ID, reserved, tunnel ID, P2MP ID> as encoded in the RSVP-TE P2MP LSP session_attribute object in RFC 4875.

The egress LER accepts multicast packets the following methods:

1. The regular RPF check on unlabeled IP multicast packets, which is based on routing table lookup.

2. The static assignment which specifies the receiving of a multicast group <*,G> or a specific <S,G> from a primary tunnel-interface associated with an RSVP P2MP LSP.

One or more primary tunnel interfaces in the base router instance can be configured. In other words, the user will be able to receive different multicast groups, <*,G> or specific <S,G>, from different P2MP LSPs. This assumes that the user configured static joins for the same multicast groups at the ingress LER to forward over a tunnel interface associated with the same P2MP LSP.

A multicast info policy CLI option allows the user to define a bundle and specify channels in the bundle that must be received from the primary tunnel interface. The user can apply the defined multicast info policy to the base router instance.

At any given time, packets of the same multicast group can be accepted from either the primary tunnel interface associated with a P2MP LSP or from a PIM interface. These are mutually exclusive options. As soon as a multicast group is configured against a primary tunnel interface in the multicast info policy, it is blocked from other PIM interfaces.

However, if the user configured a multicast group to be received from a given primary tunnel interface, there is nothing preventing packets of the same multicast group from being received and accepted from another primary tunnel interface. However, an ingress LER will not allow the same multicast group to be forwarded over two different P2MP LSPs. The only possible case is that of two ingress LERs forwarding the same multicast group over two P2MP LSPs towards the same egress LER.

A multicast packet received on a tunnel interface associated with a P2MP LSP can be forwarded over a PIM or IGMP interface which can be an IES interface, a spoke SDP terminated IES interface, or a network interface.

Note that packets received from a primary tunnel-interface associated with a terminating P2MP LSP cannot be forwarded over a tunnel interface associated with an originating P2MP LSP.

MPLS Service Usage

Alcatel-Lucent routers routers enable service providers to deliver virtual private networks (VPNs) and Internet access using Generic Routing Encapsulation (GRE) and/or MPLS tunnels, with Ethernet and/or SONET/SDH interfaces.

Service Distribution Paths

A service distribution path (SDP) acts as a logical way of directing traffic from one 7750 SR router to another through a uni-directional (one-way) service tunnel. The SDP terminates at the far-end 7750 SR router which directs packets to the correct service egress service access point (SAP) on that device. All services mapped to an SDP use the same transport encapsulation type defined for the SDP (either GRE or MPLS).

For information about service transport tunnels, refer to the *Service Distribution Paths (SDPs)* section in the 7750 SR OS Services Guide. They can support up to eight forwarding classes and can be used by multiple services. Multiple LSPs with the same destination can be used to load-balance traffic.

MPLS/RSVP Configuration Process Overview

Figure 15 displays the process to configure MPLS and RSVP parameters.

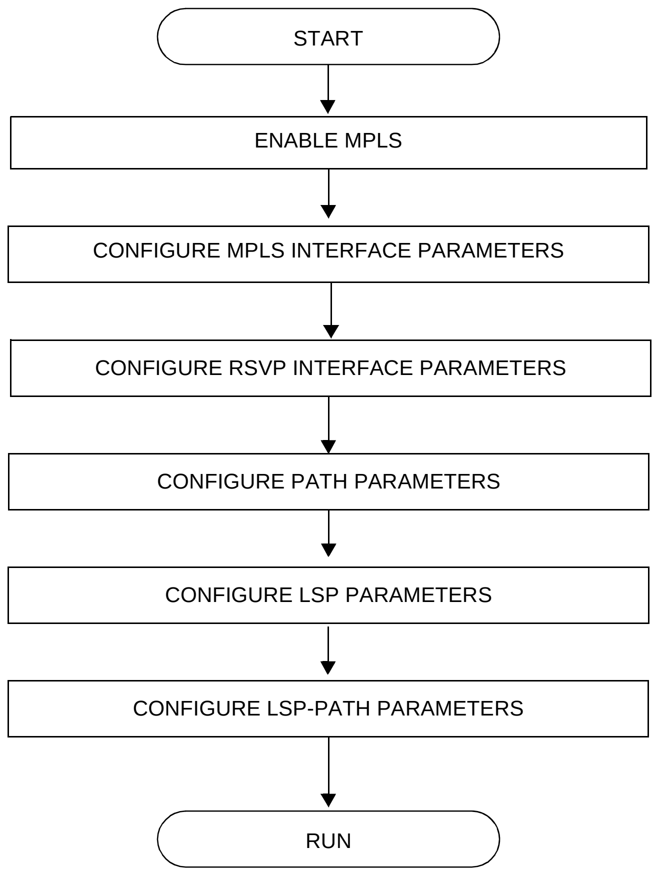

Figure 15: MPLS and RSVP Configuration and Implementation Flow

Configuration Notes

This section describes MPLS and RSVP caveats.

- Interfaces must already be configured in the `config>router>interface` context before they can be specified in MPLS and RSVP.
- A router interface must be specified in the `config>router>mpls` context in order to apply it or modify parameters in the `config>router>rsvp` context.
- A system interface must be configured and specified in the `config>router>mpls` context.
- Paths must be created before they can be applied to an LSP.

Configuring MPLS and RSVP with CLI

This section provides information to configure MPLS and RSVP using the command line interface.

Topics in this section include:

MPLS Configuration Overview

Multiprotocol Label Switching (MPLS) enables routers to forward traffic based on a simple label embedded into the packet header. A router examines the label to determine the next hop for the packet, saving time for router address lookups to the next node when forwarding packets. MPLS is not enabled by default and must be explicitly enabled.

In order to implement MPLS, the following entities must be configured:

- LSPs on page 104
- Paths on page 104
- Router Interface on page 105

LSPs

To configure MPLS-signaled label-switched paths (LSPs), an LSP must run from an ingress router to an egress router. Configure only the ingress router and configure LSPs to allow the software to make the forwarding decisions or statically configure some or all routers in the path. The LSP is set up by Resource Reservation Protocol (RSVP), through RSVP signaling messages. The 7750 SR OS automatically manages label values. Labels that are automatically assigned have values ranging from 1,024 through 1,048,575 (see Label Values on page 22).

A static LSP is a manually set up LSP where the nexthop IP address and the outgoing label are explicitly specified.

Paths

To configure signaled LSPs, you must first create one or more named paths on the ingress router. For each path, the transit routers (hops) in the path are specified.

Router Interface

At least one router interface and one system interface must be defined in the **config>router>interface** context in order to configure MPLS on an interface.

Choosing the Signaling Protocol

If only static label switched paths are used in your configurations, then you must manually define the paths through the MPLS network. Label mappings and actions configured at each hop must be specified. You do not need to enable RSVP or LDP if you are configuring static LSPs.

If dynamic LSP signaling is implemented in your network, then one of the two supported signaling protocols, RSVP or LDP, must be specified. Enable signaling protocols only on the links where the functionality is required.

In order to implement MPLS, the following entities must be enabled:

- MPLS must be enabled on all routers that are part of an LSP.
- RSVP or LDP must be enabled on the same routers.

When MPLS is enabled and either RSVP or LDP is also enabled, MPLS uses RSVP or LDP to set up the configured LSPs. For example, when you configure an LSP with both MPLS and RSVP running, RSVP initiates a session for the LSP. RSVP uses the local router as the RSVP session sender and the LSP destination as the RSVP session receiver. When the RSVP session is created, the LSP is set up on the path created by the session. If the session is not successfully created, RSVP notifies MPLS; MPLS can then either initiate backup paths or retry the initial path.

Basic MPLS Configuration

This section provides information to configure MPLS and configuration examples of common configuration tasks. To enable MPLS on 7750 SR-Series routers, you must configure at least one MPLS interface. The other MPLS configuration parameters are optional. This follow displays an example of an MPLS configuration.

```
A:ALA-1>config>router>mpls# info
------------------------------------------
     admin-group "green" 15
            admin-group "yellow" 20
            admin-group "red" 25
            interface "system"
            exit
            interface "StaticLabelPop"
                admin-group "green"
                label-map 50
                    pop
                    no shutdown
                exit
            exit
            interface "StaticLabelPop"
                label-map 35
                    swap 36 nexthop 10.10.10.91
                    no shutdown
                exit
            exit
            path "secondary-path"
                no shutdown
            exit
            path "to-NYC"
                hop 1 10.10.10.104  strict
                no shutdown
            exit
            lsp "lsp-to-eastcoast"
                to 10.10.10.104
                from 10.10.10.103
                fast-reroute one-to-one
                exit
                primary "to-NYC"
                exit
                secondary "secondary-path"
                exit
                no shutdown
            exit
            static-lsp "StaticLabelPush"
                to 10.10.11.105
                push 60 nexthop 10.10.11.105
                no shutdown
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>mpls#
```

Common Configuration Tasks

This section provides a brief overview of the tasks to configure MPLS and provides the CLI commands.

The following protocols must be enabled on each participating router.

- MPLS
- RSVP (for RSVP-signaled MPLS only)
- LDP

In order for MPLS to run, you must configure at least one MPLS interface in the **config>router>mpls** context.

- An interface must be created in the **config>router>interface** context before it can be applied to MPLS.
- In the **config>router>mpls** context, configure path parameters for configuring LSP parameters. A path specifies some or all hops from ingress to egress. A path can be used by multiple LSPs.
- When an LSP is created, the egress router must be specified in the `to` command and at least one primary or secondary path must be specified. All other statements under the LSP hierarchy are optional.

Configuring MPLS Components

Use the MPLS and RSVP CLI syntax displayed below for:

- Configuring Global MPLS Parameters on page 108
- Configuring an MPLS Interface on page 109
- Configuring MPLS Paths on page 110
- Configuring an MPLS LSP on page 111
- Configuring a Static LSP on page 111
- Configuring Manual Bypass Tunnels on page 113
- Configuring RSVP Parameters on page 115
- Configuring RSVP Message Pacing Parameters on page 116
- Configuring Graceful Shutdown on page 117

Configuring Global MPLS Parameters

Admin groups can signify link colors, such as red, yellow, or green. MPLS interfaces advertise the link colors it supports. CSPF uses the information when paths are computed for constrained-based LSPs. CSPF must be enabled in order for admin groups to be relevant.

To configure MPLS admin-group parameters, enter the following commands:

CLI Syntax:
```
mpls
  admin-group group-name group-value
  frr-object
  resignal-timer minutes
```

The following displays an admin group configuration example:

```
A:ALA-1>config>router>mpls# info
----------------------------------------------
            resignal-timer 500
            admin-group "green" 15
            admin-group "yellow" 20
            admin-group "red" 25
...
----------------------------------------------
A:ALA-1>config>router>mpls#
```

Configuring an MPLS Interface

Configure the `label-map` parameters if the interface is used in a static LSP.
To configure an MPLS interface on a router, enter the following commands:

CLI Syntax:
```
config>router>mpls
 interface
    no shutdown
    admin-group group-name [group-name...(up to 32 max)]
    label-map
       pop
       swap
       no shutdown
    srlg-group group-name [group-name...(up to 5 max)]
    te-metric value
```

The following displays an interface configuration example:

```
A:ALA-1>config>router>mpls# info
----------------------------------------------
...
            interface "to-104"
                admin-group "green"
                admin-group "red"
                admin-group "yellow"
                label-map 35
                    swap 36 nexthop 10.10.10.91
                    no shutdown
                exit
            exit
            no shutdown
...
----------------------------------------------
A:ALA-1>config>router>mpls#
```

Configuring MPLS Paths

Configure an LSP path to use in MPLS. When configuring an LSP, the IP address of the hops that the LSP should traverse on its way to the egress router must be specified. The intermediate hops must be configured as either `strict` or `loose` meaning that the LSP must take either a direct path from the previous hop router to this router (`strict`) or can traverse through other routers (`loose`).

Use the following CLI syntax to configure a path:

CLI Syntax:
```
config>router> mpls
  path path-name
     hop hop-index ip-address {strict|loose}
     no shutdown
```

The following displays a path configuration example:

```
A:ALA-1>config>router>mpls# info
------------------------------------------
            interface "system"
            exit
            path "secondary-path"
                hop 1 10.10.0.121  strict
                hop 2 10.10.0.145 strict
                hop 3 10.10.0.1 strict
                no shutdown
            exit
            path "to-NYC"
                hop 1 10.10.10.103 strict
                hop 2 10.10.0.210  strict
                hop 3 10.10.0.215  loose
            exit
------------------------------------------
A:ALA-1>config>router>mpls#
```

Configuring an MPLS LSP

Configure an LSP path for MPLS. When configuring an LSP, you must specify the IP address of the egress router in the `to` statement. Specify the primary path to be used. Secondary paths can be explicitly configured or signaled upon the failure of the primary path. All other statements are optional.

The following displays an MPLS LSP configuration:

```
A:ALA-1>config>router>mplp# info
----------------------------------------------
...
            lsp "lsp-to-eastcoast"
                to 192.168.200.41
                rsvp-resv-style ff
                cspf
                include "red"
                exclude "green"
                adspec
                fast-reroute one-to-one
                exit
                primary "to-NYC"
                    hop-limit 10
                exit
                secondary "secondary-path"
                    bandwidth 50000
                exit
                no shutdown
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>mpls#
```

Configuring a Static LSP

An LSP can be explicitly (statically) configured. Static LSPs are configured on every node along the path. The label’s forwarding information includes the address of the next hop router.

Use the following CLI syntax to configure a static LSP:

CLI Syntax:
```
config>router>mpls
 static-lsp lsp-name
    to ip-address
    push out-label nexthop ip-addr
    no shutdown
```

The following displays a static LSP configuration example:

```
A:ALA-1>config>router>mpls# info
----------------------------------------------
...
            static-lsp "static-LSP"
                to 10.10.10.124
                push 60 nexthop 10.10.42.3
                no shutdown
            exit
...
----------------------------------------------
A:ALA-1>config>router>mpls#
```

Configuring Manual Bypass Tunnels

Consider the following network setup.

```
A----B----C----D
     |    |
     E----F
```

The user first configures the option to disable the dynamic bypass tunnels on the 7750 node B if required. The CLI for this configuration is:

config>router>mpls>dynamic-bypass [disable | enable]

By default, dynamic bypass tunnels are enabled.

Next, the user configures an LSP on node B, such as B-E-F-C to be used only as bypass. The user specifies each hop in the path, for example, the bypass LSP has a strict path.

Note that including the bypass-only keyword disables the following options under the LSP configuration:

- bandwidth
- fast-reroute
- secondary

The following LSP configuration options are allowed:

- adaptive
- adspec
- cspf
- exclude
- hop-limit
- include
- metric

The following example displays a bypass tunnel configuration:

```
A:ALA-48>config>router>mpls>path# info
-------------------------------------------
...
            path "BEFC"
                hop 10 10.10.10.11  strict
                hop 20 10.10.10.12  strict
                hop 30 10.10.10.13  strict
                no shutdown
            exit


            lsp "bypass-BC"
                to 10.10.10.15
                primary "BEFC"
                exit
                no shutdown
...
-------------------------------------------
A:ALA-48>config>router>mpls>path#
```

Next, the configures an LSP from A to D and indicates fast-reroute bypass protection by selecting facility as the FRR method (config>router>mpls>lsp>fast-reroute facility). If the LSP goes through B, and bypass is requested, and the next hop is C, and there is a manually configured bypass-only tunnel from B to C, excluding link BC, then node B uses that.

Configuring RSVP Parameters

RSVP is used to set up LSPs. RSVP must be enabled on the router interfaces that are participating in signaled LSPs. The `keep-multiplier` and `refresh-time` default values can be modified in the RSVP context.

Initially, interfaces are configured in the `config>router>mpls>interface` context. Only these existing (MPLS) interfaces are available to modify in the `config>router> rsvp` context. Interfaces cannot be directly added in the RSVP context.

The following example displays an RSVP configuration example:

```
A:ALA-1>config>router>rsvp# info
----------------------------------------------
     interface "system"
             no shutdown
          exit
          interface to-104
             hello-interval 4000
             no shutdown
          exit
          no shutdown
----------------------------------------------
A:ALA-1>config>router>rsvp#
```

Configuring RSVP Message Pacing Parameters

RSVP message pacing maintains a count of the messages that were dropped because the output queue for the egress interface was full.

Use the following CLI syntax to configure RSVP parameters:

CLI Syntax:
```
config>router>rsvp
  no shutdown
  msg-pacing
     period milli-seconds
     max-burst number
```

The following example displays a RSVP message pacing configuration example:

```
A:ALA-1>config>router>rsvp# info
----------------------------------------------
            keep-multiplier 5
            refresh-time 60
            msg-pacing
                period 400
                max-burst 400
            exit
            interface "system"
                no shutdown
            exit
            interface to-104
                hello-interval 4000
                no shutdown
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>rsvp#
```

Configuring Graceful Shutdown

TE graceful shutdown can be enabled on a specific interface using the **config>router>rsvp>interface>graceful-shutdown** command. This interface is referred to as the maintenance interface.

Graceful shutdown can be disabled by executing the **no** form of the command at the RSVP interface level or at the RSVP level. In this case, the user configured TE parameters of the maintenance links are restored and the maintenance node floods them.

MPLS Configuration Management Tasks

This section discusses the following MPLS configuration management tasks:

- Modifying MPLS Parameters on page 118
- Modifying MPLS Path Parameters on page 120
- Modifying MPLS Static LSP Parameters on page 121
- Deleting an MPLS Interface on page 122

Deleting MPLS

NOTE: In order to remove the MPLS instance, MPLS must be disabled (shutdown) and all SDP bindings to LSPs removed. If MPLS is not shutdown first, when the `no mpls` command is executed, a warning message on the console displays indicating that MPLS is still administratively up.

When MPLS is shut down, the `no mpls` command deletes the protocol instance and removes all configuration parameters for the MPLS instance.
To disable MPLS, use the `shutdown` command.

To remove MPLS on a router, enter the following command:

CLI Syntax: `config>router# no mpls`

Modifying MPLS Parameters

NOTE: You must shut down MPLS entities in order to modify parameters. Re-enable (`no shutdown`) the entity for the change to take effect.

Modifying an MPLS LSP

Some MPLS LSP parameters such as primary and secondary, must be shut down before they can be edited or deleted from the configuration.

The following displays a MPLS LSP configuration example. Refer to the LSP configuration on page 111.

```
A:ALA-1>>config>router>mpls>lsp# info
----------------------------------------------
                shutdown
                to 10.10.10.104
                from 10.10.10.103
                rsvp-resv-style ff
                include "red"
                exclude "green"
                fast-reroute one-to-one
                exit
                primary "to-NYC"
                    hop-limit 50
                exit
                secondary "secondary-path"
                exit
----------------------------------------------
A:ALA-1>config>router>mpls#
```

Modifying MPLS Path Parameters

In order to modify path parameters, the `config>router>mpls>path` context must be shut down first.

The following displays a path configuration example. Refer to the LSP configuration on page 110.

```
A:ALA-1>config>router>mpls# info
#------------------------------------------
echo "MPLS"
#------------------------------------------
...
            path "secondary-path"
                hop 1 10.10.0.111  strict
                hop 2 10.10.0.222  strict
                hop 3 10.10.0.123  strict
                no shutdown
            exit
            path "to-NYC"
                hop 1 10.10.10.104  strict
                hop 2 10.10.0.210  strict
                no shutdown
            exit
...
---------------------------------------------
A:ALA-1>config>router>mpls#
```

Modifying MPLS Static LSP Parameters

In order to modify static LSP parameters, the `config>router>mpls>path` context must be shut down first.

The following displays a static LSP configuration example. Refer to the static LSP configuration on page 111.

```
A:ALA-1>config>router>mpls# info
----------------------------------------------
...
            static-lsp "static-LSP"
                to 10.10.10.234
                push 102704 nexthop 10.10.8.114
                no shutdown
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>mpls#
```

Deleting an MPLS Interface

In order to delete an interface from the MPLS configuration, the `interface` must be shut down first.

Use the following CLI syntax to delete an interface from the MPLS configuration:

CLI Syntax: mpls
  [no] interface *ip-int-name*
    shutdown

```
A:ALA-1>config>router>mpls# info
----------------------------------------------
...
     admin-group "green" 15
            admin-group "red" 25
            admin-group "yellow" 20
            interface "system"
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>mpls#
```

RSVP Configuration Management Tasks

This section discusses the following RSVP configuration management tasks:

- Modifying RSVP Parameters on page 123
- Modifying RSVP Message Pacing Parameters on page 124
- Deleting an Interface from RSVP on page 124

Modifying RSVP Parameters

Only interfaces configured in the MPLS context can be modified in the RSVP context.

The `no rsvp` command deletes this RSVP protocol instance and removes all configuration parameters for this RSVP instance.
The `shutdown` command suspends the execution and maintains the existing configuration.

The following example displays a modified RSVP configuration example:

```
A:ALA-1>config>router>rsvp# info
----------------------------------------------
            keep-multiplier 5
            refresh-time 60
            msg-pacing
                period 400
                max-burst 400
            exit
            interface "system"
            exit
            interface "test1"
                hello-interval 5000
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>rsvp#
```

Modifying RSVP Message Pacing Parameters

RSVP message pacing maintains a count of the messages that were dropped because the output queue for the egress interface was full.

The following example displays command usage to modify RSVP parameters:

The following example displays a modified RSVP message pacing configuration example. Refer to the RSVP message pacing configuration on page 115.

```
A:ALA-1>config>router>rsvp# info
----------------------------------------------
            keep-multiplier 5
            refresh-time 60
            msg-pacing
                period 200
                max-burst 200
            exit
            interface "system"
            exit
            interface "to-104"
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>rsvp#
```

Deleting an Interface from RSVP

Interfaces cannot be deleted directly from the RSVP configuration. An interface must have been configured in the MPLS context and then the RSVP context. The interface must first be deleted from the MPLS context. This removes the association from RSVP.

See Deleting an MPLS Interface on page 122 for information on deleting an MPLS interface.

MPLS/RSVP Command Reference

Command Hierarchies

MPLS Commands

config
— **router**
　— [**no**] **mpls**
　　— **admin-group** *group-name group-value*
　　— **no admin-group** *group-name*
　　— **auto-bandwidth-multipliers** **sample-multiplier** *number1* **adjust-multiplier** *number2*
　　— **no auto-bandwidth-multipliers**
　　— **dynamic-bypass** [**enable** | **disable**]
　　— [**no**] **frr-object**
　　— **hold-timer** *seconds*
　　— **no hold-timer**
　　— **ingress-statistics**
　　　— [**no**] **lsp** *lsp-name* **sender** *ip-address*
　　　　— **accounting-policy** *policy-id*
　　　　— **no accounting-policy**
　　　　— [**no**] **collect-stats**
　　　　— [**no**] **shutdown**
　　— [**no**] **interface** *ip-int-name*
　　　— [**no**] **admin-group** *group-name* [*group-name*...(up to 5 max)]
　　　— [**no**] **label-map** *in-label*
　　　　— [**no**] **pop**
　　　　— [**no**] **shutdown**
　　　　— **swap** {*out-label* | **implicit-null-label**} **nexthop** *ip-addr*
　　　　— **no swap** {*out-label* | **implicit-null-label**}
　　　— [**no**] **shutdown**
　　　— [**no**] **srlg-group** *group-name* [*group-name*...(up to 5 max)]
　　　— **te-metric** *metric*
　　　— **no te-metric**

— **ldp-over-rsvp** [**include** | **exclude**]
— **least-fill-min-thd** *percent*
— **no least-fill-min-thd**
— **least-fill-reoptim-thd** *percent*
— **no least-fill-reoptim-thd**
— **preemption-timer** *seconds*
— **no preemption-timer**
— **p2mp-resignal-timer** *minutes*
— **no p2mp-resignal-timer**
— **resignal-timer** *minutes*
— **no resignal-timer**
— **secondary-fast-retry-timer** *seconds*
— **no secondary-fast-retry-timer**
— [**no**] **shutdown**
— [**no**] **srlg-database**
    — [**no**] **router-id** *router-addr*
        — [**no**] **interface** *ip-addr* **srlg-group** *group-name* [*group-name..(up to 5 max)*]
    — [**no**] **shutdown**
— [**no**] **srlg-frr** [**strict**]
— **srlg-group** *group-name* {**value** *group-value*}
— **no srlg-group** *group-name*
— [**no**] **static-lsp** *lsp-name*
    — **push** {*label* | **implicit-null-label**} **nexthop** *ip-address*
    — **push** {*out-label* | **implicit-null-label**}
    — **[no] shutdown**
    — **to***ip-address*
— **user-srlg-db** [**enable | disable**]

LSP Commands

config
— **router**
— [**no**] **mpls**
— [**no**] **lsp** *lsp-name* [**bypass-only** | **p2mp-lsp**]
— [**no**] **adaptive**
— [**no**] **adspec**
— [**no**] **auto-bandwidth**
— **adjust-down** **percent** [**bw** *mbps*]
— **no adjust-down**
— **adjust-up** **percent** [**bw** *mbps*]
— **no adjust-up**
— **max-bandwidth** *mbps*
— **no max-bandwidth**
— **min-bandwidth** *mbps*
— **no min-bandwidth**
— [**no**] **monitor-bandwidth**
— **multipliers** **sample-multiplier** *num1* **adjust-multiplier** *num2*
— **no multipliers**
— **overflow-limit** *number* **threshold** percent [**bw** *mbps*]
— **no overflow-limit**
— **class-type** *ct-number*
— **no class-type**
— [**no**] **cspf** [*use-te-metric*]
— [**no**] **egress-statistics**
— **accounting-policy** *policy-id*
— **no accounting-policy**
— [**no**] **collect-stats**
— [**no**] **shutdown**
— [**no**] **exclude** *group-name* [*group-name*...(up to 5 max)]
— **fast-reroute** *frr-method*
— **no fast-reroute**
— **bandwidth** *rate-in-mbps*
— **no bandwidth**
— **hop-limit** *number*
— **no hop-limit**
— [**no**] **node-protect**
— **from** *ip-address*
— **hop-limit** *number*
— **no hop-limit**
— [**no**] **igp-shortcut**
— [**no**] **include** *group-name* [*group-name*...(up to 5 max)]
— **ldp-over-rsvp** [**include** | **exclude**]
— [**no**] **least-fill**
— [**no**] **ldp-over-rsvp** [**include** | **exclude**]
— **main-ct-retry-limit** *number*
— **no main-ct-retry-limit**
— **metric** *metric*
— **p2mp-id** *id*
— [**no**] **primary** *path-name*
— [**no**] **adaptive**
— **backup-class-type** *ct-number*

— **no backup-class-type**
— **bandwidth** *rate-in-mpbs*
— **no bandwidth**
— **class-type** *ct-number*
— **no class-type**
— [**no**] **exclude** *group-name* [*group-name*...(up to 5 max)]
— **hop-limit** *number*
— **no hop-limit**
— [**no**] **include** *group-name* [*group-name*...(up to 5 max)]
— **priority** *setup-priority hold-priority*
— **no priority**
— [**no**] **record**
— [**no**] **record-label**
— [**no**] **shutdown**
— [**no**] **primary-p2mp-instance** *instance-name*
— [**no**] **adaptive**
— **bandwidth** *rate-in-mbps*
— **no bandwidth**
— [**no**] **exclude** *group-name* [*group-name*...(up to 5 max)]
— [**no**] **hop-limit**
— **hop-limit** *number*
— **no hop-limit**
— [**no**] **include** *group-name* [*group-name*...(up to 5 max)]
— [**no**] **record**
— [**no**] **record-label**
— [**no**] **s2l-path** *path-name* **to** *ip-address*
— [**no**] **shutdown**
— [**no**] **shutdown**
— **retry-limit** *number*
— **no retry-limit**
— **retry-timer** *seconds*
— **no retry-timer**
— **rsvp-resv-style** [**se** | **ff**]
— [**no**] **secondary** *path-name*
— [**no**] **adaptive**
— **bandwidth** *rate-in-mbps*
— **no bandwidth**
— **class-type** *ct-number*
— **no class-type**
— [**no**] **exclude** *group-name* [*group-name*...(up to 5 max)]
— **hop-limit** *number*
— **no hop-limit**
— [**no**] **include** *group-name* [*group-name*...(up to 5 max)]
— **priority** *setup-priority hold-priority*
— **no priority**
— [**no**] **record**
— [**no**] **record-label**
— [**no**] **shutdown**
— [**no**] **srlg**
— [**no**] **standby**
— **[no] path-preference** *preference-number*
— [**no**] **shutdown**
— **to** *ip-address*
— **vprn-auto-bind** [**include** | **exclude**]
— **[no] lsp-template** *lsp-template-name* **p2mp-lsp**

— **[no] adaptive**
— **[no] bandwidth** *rate-in-mbps*
— **[no] cspf [use-te-metric]**
— **[no] default-path** *path-name*
— **[no] exclude** *group-name [group-name..(up to 5 max)]*
— **[no] fast-reroute**
    — **[no] bandwidth** *rate-in-mbps*
    — **[no] hop-limit** *limit*
— **[no] fast-reroute** *frr-method*
— **[no] hop-limit** *number*
— **[no] include** *group-name [group-name…(up to 5 max)]*
— **[no] lsp-name-rule {suffix-client-id | suffix-mpls-id}**
— **[no] record-label**
— **[no] retry-limit** *number*
— **[no] retry-timer** *seconds*
— **[no] shutdown**

MPLS Path Commands

config
— **router**
— [**no**] **mpls**
— [**no**] **path** *path-name*
— **hop** *hop-index ip-address* {**strict** | **loose**}
— **no hop** *hop-index*
— [**no**] **shutdown**
— [**no**] **static-lsp** *lsp-name*
— **push** *label* **nexthop** *ip-address*
— **no push** *out-label*
— **to** *ip-addr*
— [**no**] **shutdown**

RSVP Commands

config
— **router**
— [**no**] **rsvp**
— **diffserv-te** [**mam** | **rdm**]
— **no diffserv-te**
— **class-type-bw ct0** *%-link-bandwidth* **ct1** *%-link-bandwidth* **ct2** *%-link-bandwidth* **ct3** *%-link-bandwidth* ct4 *%-link-bandwidth* **ct5** *%-link-bandwidth* **ct6** *%-link-bandwidth* **ct7** *%-link-bandwidth*
— **no class-type-bw**
— **fc** *fc-name* **class-type** *ct-number*
— **no fc** *fc-name*
— **te-class** *te-class-number* **class-type** *ct-number* **priority** *priority*
— **no te-class** *te-class-number*
— [**no**] **graceful-shutdown**
— [**no**] **implicit-null-label**
— [**no**] **interface** *ip-int-name*
— **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
— **no authentication-key**
— [**no**] **bfd-enable**
— [**no**] **graceful-shutdown**
— **class-type-bw ct0** *%-link-bandwidth* **ct1** *%-link-bandwidth* **ct2** *%-link-bandwidth* **ct3** *%-link-bandwidth* ct4 *%-link-bandwidth* **ct5** *%-link-bandwidth* **ct6** *%-link-bandwidth* **ct7** *%-link-bandwidth*
— **no class-type-bw**
— [**no**] **graceful-shutdown**
— **hello-interval** *milli-seconds*
— **no hello-interval**
— **implicit-null-label** [**enable** | **disable**]
— **no implicit-null-label**
— [**no**] **refresh-reduction**
— [**no**] **reliable-delivery**
— [**no**] **shutdown**
— **subscription** *percentage*
— **no subscription**
— **te-up-threshold** *threshold-level* [*threshold-level,...*(up to 16 max)]
— **no te-up-threshold**
— **te-down-threshold** *threshold-level* [*threshold-level,...*(up to 16 max)]
— **no te-down-threshold**
— **keep-multiplier** *number*
— **no keep-multiplier**
— [**no**] **msg-pacing**
— **max-burst** *number*
— **no max-burst**
— **period** *milli-seconds*
— **no period**
— **preemption-timer** *seconds*
— **no preemption-timer**
— **rapid-retransmit-time** *hundred-milliseconds*
— **no rapid-retransmit-time**
— **rapid-retry-limit** *number*
— **no rapid-retry-limit**
— **refresh-reduction-over-bypass** [**enable** | **disable**]

— **refresh-time** *seconds*
— **no refresh-time**
— [**no**] **graceful-shutdown**
— [**no**] **shutdown**
— **te-threshold-update**
— **no te-threshold-update**
  — **on-cac-failure**
  — **update-timer** *seconds*
— **te-up-threshold** *threshold-level* [*threshold-level*...(up to 16 max)]
— **te-down-threshold** *threshold-level* [*threshold-level*...(up to 16 max)]

Show Commands

show
- — **router**
  - — **mpls**
    - — **admin-group** *group-name*
    - — **bypass-tunnel** [**to** *ip-address*] [**protected-lsp** *name*] [**dynamic** | **manual**| **p2mp**] [**detail**]
    - — **interface** [*ip-int-name*|*ip-address*] [**label-map** *label*]
    - — **interface** [*ip-int-name*|*ip-address*] **statistics**
    - — **label** *start-label* [*end-label* | *in-use* | **owner**]
    - — **label-range**
    - — **lsp** [*lsp-name*] [**status** {**up**|**down**}] [**from** *ip-address*| **to** *ip-address*] [**detail**]
    - — **lsp** {**transit** | **terminate**} [**status** {**up**|**down**}] [**from** *ip-address* | **to** *ip-address* | *lsp-name* **name**] [**detail**]
    - — **lsp** *count*
    - — **lsp** *lsp-name* **activepath**
    - — **lsp** [*lsp-name*] **path** [*path-name*] [**status** {**up** | **down**}] [**detail**]
    - — **lsp** [*lsp-name*] **path** [*path-name*] **mbb**
    - — **lsp-egress-stats**
    - — **lsp-egress-stats** *lsp-name*
    - — **lsp-ingress-stats** *ip-address* **lsp** *lsp-name*
    - — **p2mp-info** [**type** {**originate**|**transit**|**terminate**}] [**s2l-endpoint** *ip-address*]
    - — **p2mp-lsp** [*lsp-name*] [**detail**]
    - — **p2mp-lsp** [*lsp-name*] **p2mp-instance** [*p2mp-instance-name*] [**mbb**]
    - — **p2mp-lsp** [*lsp-name*] **p2mp-instance** [*p2mp-instance-name*] **s2l** [*s2l-name* [**to** *s2l-to-address*]][**status** {**up** | **down**}] [**detail**]
    - — **p2mp-lsp** [*lsp-name*] **p2mp-instance** [*p2mp-instance-name*] **s2l** [*s2l-name* [**to** *s2l-to-address*]] **mbb**
    - — **srlg-database** [**router-id** *ip-address*] [**interface** *ip-address*]
    - — **srlg-group** **[*group-name*]**
    - — **static-lsp** [*lsp-name*]
    - — **static-lsp** {**transit** | **terminate**}
    - — **static-lsp** **count**
    - — **statistics-summary**
    - — **status**

show
- — **router**
  - — **rsvp**
    - — **interface** [**interface** [*ip-int-name*]] **statistics** [**detail**]
    - — **neighbor** [*ip-address*] [**detail**]
    - — **session** [**session-type**] [**from** *ip-address*| **to** *ip-address*| **lsp-name** *name*] [**status** {**up**|**down**}][**detail**]
    - — **statistics**
    - — **status**

Tools Commands

tools
— **perform**
— **router**
— **mpls**
— **cspf to** *ip-addr* [**from** *ip-addr*] [**bandwidth** *bandwidth*] [**include-bitmap** *bitmap*] [**exclude-bitmap** *bitmap*] [**hop-limit** *limit*] [**exclude-address** *excl-addr* [*excl-addr*...(up to 8 max)]] [**use-te-metric**] [**strict-srlg**] [**srlg-group** *grp-id*...(up to 8 max)] [**exclude-node** *excl-node-id* [*excl-node-id*..(up to 8 max)]] [**skip-interface** *interface-name*] [**ds-class-type** *class-type*] [**cspf-reqtype** *req-type*] [**least-fill-min-thd** *thd*] [**setup-priority** *val*] [**hold-priority** *val*]
— **resignal** {**lsp** *lsp-name* **path** *path-name* | **delay** *minutes*}
— **resignal** {**p2mp-lsp** *p2mp-lsp-name* **p2mp-instance** *p2mp-instance-name* | **p2mp-delay** *p2mp-minutes*}
— **te-lspinfo** [**endpoint** *ip-address*] [**sender** *ip-address*] [**lspid** *lsp-id*] [**detail**] [**p2p** | *p2p-tid tunnel-id*]
— **te-lspinfo** [**endpoint** *ip-address*] [**sender** *ip-address*] [**lspid** *lsp-id*] [**detail**] [**p2p** | *p2p-tid tunnel-id*]{ [**phops**] [**nhops**] [**s2l** *ip-address*] } }
— **trap-suppress** *number-of-traps time-interval*
— **update-path** {**lsp** *lsp-name* **path** *current-path-name* **new-path** *new-path-name*}

Router Commands

config
— **router**
— [**no**] **igmp**
— [**no**] **tunnel-interface rsvp-p2mp** *lsp-name* [**sender** *ip-address*]
— [**no**] **tunnel-interface rsvp-p2mp** *lsp-name* [**sender** *ip-address*]

Clear Commands

clear
— **router**
— **mpls**
— **interface** [*ip-int-name*] [**statistics**]
— **lsp** *lsp-name*
— **lsp-egress-stats**
— **lsp-egress-stats** *lsp-name*
— **lsp-ingress-stats**
— **lsp-ingress-stats** *ip-address* **lsp** *lsp-name*
— **rsvp**
— **interface**
— **statistics**

Debug Commands

debug
— **router**
— **mpls** [**lsp** ***lsp-name***] [**sender** ***source-address***] [**endpoint** ***endpoint-address***] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**interface** *ip-int-name*]
— **no mpls**
— [**no**] **event**
— **all** [**detail**]
— **no all**
— **frr** [**detail**]
— **no frr**
— **iom** [**detail**]
— **no iom**
— **lsp-setup** [**detail**]
— **no lsp-setup**
— **mbb** [**detail**]
— **no mbb**
— **misc** [**detail**]
— **no misc**
— **xc** [**detail**]
— **no xc**
— **rsvp** [**lsp** ***lsp-name***] [**sender** ***source-address***] [**endpoint** ***endpoint-address***] [**tunnel-id tunnel-id**] [**lsp-id lsp-id**] [**interface ip-int-name**]
— **no rsvp**
— [**no**] **event**
— **all** [**detail**]
— **no all**
— **misc** [**detail**]
— **no misc**
— **nbr** [**detail**]
— **no nbr**
— **path** [**detail**]
— **no path**
— **resv** [**detail**]
— **no resv**
— **te-threshold-update**
— **no te-threshold-update**
— [**no**] **packet**
— **all** [**detail**]
— **no all**
— **hello** [**detail**]
— **no hello**
— **path** [**detail**]
— **no path**
— **patherr** [**detail**]
— **no patherr**
— **pathtear** [**detail**]
— **no pathtear**
— **resv** [**detail**]
— **no resv**
— **resverr** [**detail**]
— **no resverr**
— **resvtear** [**detail**]
— **no resvtear**

MPLS Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context config>router>mpls
config>router>mpls>interface
config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

MPLS is not enabled by default and must be explicitely enabled (**no shutdown**).

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command places the entity into an administratively enabled state.

Default **no shutdown**

MPLS Commands

mpls

Syntax [**no**] **mpls**

Context config>router

Description This command enables the context to configure MPLS parameters. MPLS is not enabled by default and must be explicitely enabled (**no shutdown**). The **shutdown** command administratively disables MPLS.

The **no** form of this command deletes this MPLS protocol instance; this will remove all configuration parameters for this MPLS instance.

MPLS must be **shutdown** and all SDP bindings to LSPs removed before the MPLS instance can be deleted. If MPLS is not shutdown, when the **no mpls** command is executed, a warning message on the console displays indicating that MPLS is still administratively up.

admin-group

Syntax **admin-group** *group-name group-value*
no admin-group *group-name*

Context config>router>mpls

Description This command is used to define administrative groups or link coloring for an interface. The admin group names can signify link colors, such as red, yellow, or green. MPLS interfaces advertise the link colors the support. CSPF uses the information when paths are computed for constraint-based LSPs. CSPF must be enabled in order for admin groups to be relevant.

Network resources (links) based on zones, geographic location, link location, etc., can be classified using admin groups. MPLS interfaces must be explicitly assigned to an admin group.

Admin groups must be defined in the **config>router>mpls** context before they can be assigned to an MPLS interface. The IGP communicates the information throughout the area.

Up to 32 group names can be defined in the **config>router>mpls** context. The **admin-group** names must be identical across all routers in a single domain.

The **no** form of this command deletes the administrative group. All configuration information associated with this LSP is lost.

Default none

Parameters *group-name* — Specify the name of the administrative group within a virtual router instance.

group-value — Specify the group value associated with this administrative group. This value is unique within a virtual router instance.

Values 0 — 31

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context config>router>mpls>ingr-stats
config>router>mpls>lsp>egr-stats

Description This command associates an accounting policy to the MPLS instance.

An accounting policy must be defined before it can be associated else an error message is generated.

The **no** form of this command removes the accounting policy association.

Default none

Parameters *acct-policy-id* — Enter the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 — 99

collect-stats

Syntax [**no**] **collect-stats**

Context config>router>mpls>ingr-stats
config>router>mpls>lsp>egr-stats

Description This command enables accounting and statistical data collection. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default collect-stats

dynamic-bypass

Syntax **dynamic-bypass** [**enable** | **disable**]
no dynamic-bypass

Context config>router>mpls

Description This command disables the creation of dynamic bypass LSPs in FRR. One or more manual bypass LSPs must be configured to protect the primary LSP path at the PLR nodes.

Default enable

egress-statistics

Syntax [**no**] **egress-statistics**

Context config>router>mpls>lsp

Description This command configures statistics in the egress data path of an originating LSP at a head-end node. The user must execute the no shutdown for this command to effectively enable statistics.

The same set of counters is updated for packets forwarded over any path of the LSP and over the lifetime of the LSP. In steady state, the counters are updated for packets forwarded over the active path of the LSP. The active path can be the primary path, one of the secondary paths, the FRR detour path, or the FRR bypass path when the head-end node is also the PLR.

LSP statistics are not collected on a dynamic or a static bypass tunnel itself.

When a hierarchy of LSPs is in use, statistics collection on the outermost label corresponding to the tunneling LSP and on the inner labels, corresponding to the tunneled LSPs, are mutually exclusive. A consequence of this is that when the user enables statistics collection on an RSVP LSP which is also used for tunneling LDP FECs with the LDP over RSVP feature, then statistics will be collected on the RSVP LSP only. There will be no statistics collected from an LDP FEC tunneled over this RSVP LSP regardless if the user enabled statistics collection on this FEC. When, the user disables statistics collection on the RSVP LSP, then statistics collection, if enabled, will be performed on a tunneled LDP FEC.

The **no** form of this command disables the statistics in the egress data path and removes the accounting policy association from the RSVP LSP.

Default no egress-statistics

frr-object

Syntax [**no**] **frr-object**

Context config>router>mpls

Description This command specifies whether fast reroute for LSPs using the **facility** bypass method is signalled with or without the fast reroute object using the **one-to-one** keyword. The value is ignored if fast reroute is disabled for the LSP or if the LSP is using one-to-one Backup.

Default frr-object — The value is by default inherited by all LSPs.

hold-timer

Syntax **hold-timer** *seconds*
no hold-timer

Context config>router>mpls

Description This command specifies the amount of time that the ingress node holds before programming its data plane and declaring the LSP up to the service module.

The **no** form of the command disables the hold-timer.

Parameters *seconds* — Specifies the time, in seconds, for which the ingress node holds before programming its data plane and declaring the LSP up to the service module.

Values 0 — 10

ingress-statistics

Syntax **ingress-statistics**

Context config>router>mpls

Description This command provides the context for the user to enter the LSP names for the purpose of enabling ingress data path statistics at the terminating node of the LSP, for example, egress LER.

Default none

least-fill-min-thd

Syntax **least-fill-min-thd** *percent*
no least-fill-min-thd

Context config>router>mpls

Description This parameter is used in the least-fill path selection process. When comparing the percentage of least available link bandwidth across the sorted paths, whenever two percentages differ by less than the value configured as the least-fill-min-thresh, CSPF will consider them equal and will apply a random number generator to select the path among these paths

The **no** form of the command resets this parameter to its default value.

Default 5

Parameters *percentage* — Specifies the least fill minimum threshold value as a percentage.

Values 1 — 100%

least-fill-reoptim-thd

Syntax **least-fill-reoptim-thd** *percent*
no least-fill-reoptim-thd

Context config>router>mpls

Description This parameter is used in the least-fill path selection method. During a timer-based re-signaling of an LSP path which has the least-fill option enabled, CSPF will first update the least-available bandwidth figure for the current path of this LSP. It then applies the least-fill path selection method to select a new path for this LSP. If the new computed path has the same cost as the current path, it will compare the least-available bandwidth figures of the two paths and if the difference exceeds the user configured optimization threshold, MPLS will generate a trap to indicate that a better least-fill path is available for this LSP. This trap can be used by an external SNMP based device to trigger a manual re-signaling of the LSP path since the timer-based re-signaling will not re-signal the path in this case. MPLS will generate a path update trap at the first MBB event which results in the re-signaling of the LSP path. This should clear the eligibility status of the path at the SNMP device.

The **no** form of this command resets this parameter to its default value.

Default 10

Parameters *percentage* — Specifies the least fill reoptimization threshold value as a percentage.

Values 1 — 100%

lsp

Syntax [**no**] **lsp** *lsp-name* **sender** *sender-address*

Context config>router>mpls>ingress-statistics

Description This command configures statistics in the ingress data path of a terminating RSVP LSP at an egress LER. The LSP name must correspond to the name configured by the operator at the ingress LER. It must not contain the special character “:” which is used as a field separator by the ingress LER for encoding the LSP and path names into the RSVP session name field in the session_attribute object. The operator must execute the **no shutdown** for this command to effectively enable statistics.

The same set of counters is updated for packets received over any path of this LSP and over the lifetime of the LSP. In steady-state, the counters are updated for packets received over the active path of the LSP. The active path can be the primary path, one of the secondary paths, the FRR detour path, or the FRR bypass path when the tail-end node is also the MP.

When a hierarchy of LSPs is in use, statistics collection on the outermost label corresponding to the tunneling LSP and on the inner labels, corresponding to the tunneled LSPs are mutually exclusive. A consequence of this is that when the operator enables statistics collection on an RSVP LSP which is also used for tunneling LDP FECs with the LDP over RSVP feature, then statistics will be collected on the RSVP LSP only. There will be no statistics collected for an LDP FEC tunneled over this RSVP LSP and also egressing on the same node regardless if the operator enabled statistics collection on this FEC. When, the operator disables statistics collection on the RSVP LSP, then statistics collection, if enabled, will be performed on a tunneled LDP FEC.

The operator can enable statistics collection on a manual bypass terminating on the egress LER. However all LSPs which primary path is protected by the manual bypass will not collect statistics when they activate forwarding over the manual bypass. When, the operator disables statistics collection on the manual bypass LSP, then statistics collection on the protected LSP, if enabled, will continue when the bypass LSP is activated.

The **no** form of this command disables statistics for this RSVP LSP in the ingress data path and removes the accounting policy association from the LSP.

Default none

Parameters **sender-address** *ip-address* **—** A string of 15 characters representing the IP address of the ingress LER for the LSP.

lsp-name — A string of up to 32 characters identifying the LSP name as configured at the ingress LER.

resignal-timer

Syntax **resignal-timer** *minutes*
no resignal-timer

Context config>router>mpls

Description This command specifies the value for the LSP resignal timer. The resignal timer is the time, in minutes, the software waits before attempting to resignal the LSPs.

When the resignal timer expires, if the new computed path for an LSP has a better metric than the current recorded hop list, an attempt is made to resignal that LSP using the make-before-break mechanism. If the attempt to resignal an LSP fails, the LSP will continue to use the existing path and a resignal will be attempted the next time the timer expires.

The **no** form of the command disables timer-based LSP resignalling.

Default no resignal-timer

Parameters *minutes* — The time the software waits before attempting to resignal the LSPs.

Values 30 — 10080

secondary-fast-retry-timer

Syntax **secondary-fast-retry-timer** *seconds*
no secondary-fast-retry-timer

Context config>router>mpls

Description This command specifies the value used as the fast retry timer for a secondary path. If the first attempt to set up a secondary path fails due to a path error, the fast retry timer will be started for the secondary path so that the path can be retried sooner. If the next attempt also fails, further retries for the path will use the configured value for LSP retry timer.

If retry-timer for the LSP is configured to be less than the MPLS secondary-fast-retry-timer, all retries for the secondary path will use the LSP retry-timer.

The **no** form of the command reverts to the default.

Default no secondary-fast-retry-timer

Parameters *seconds* — specifies the value, in seconds, used as the fast retry timer for a secondary path

Values 1 — 10

srlg-frr

Syntax **srlg-frr** [**strict**]
no srlg-frr

Context config>router>mpls

Description This command enables the use of the Shared Risk Loss Group (SRLG) constraint in the computation of FRR bypass or detour to be associated with any primary LSP path on this system.

When this option is enabled, CSPF includes the SRLG constraint in the computation of a FRR detour or bypass for protecting the primary LSP path.

CSPF prunes all links with interfaces which belong to the same SRLG as the interface which is being protected, i.e., the outgoing interface at the PLR the primary path is using. If one or more paths are found, the MPLS/RSVP task will select one based on best cost and will signal the bypass/detour. If not and the user included the strict option, the bypass/detour is not setup and the MPLS/RSVP task will keep retrying the request to CSPF. Otherwise, if a path exists which meets the other TE constraints, other than the SRLG one, the bypass/detour is setup.

A bypass or a detour LSP path is not guaranteed to be SRLG disjoint from the primary path. This is because only the SRLG constraint of the outgoing interface at the PLR the primary path is using is checked.

When the MPLS/RSVP task is searching for a SRLG bypass tunnel to associate with the primary path of the protected LSP, it will first check if any configured manual bypass LSP with CSPF enabled satisfies the SLRG constraints. The MPLS/RSVP skips any non-CSPF bypass LSP in the search as there is no ERO returned to check the SLRG constraint. If no path is found, it will check if an existing dynamic bypass LSP satisfies the SLRG and other primary path constraints. If not, then it will make a request to CSPF.

Once the primary path of the LSP is set up and is operationally up, any subsequent changes to the SRLG group membership of an interface the primary path is using would not be considered by the MPLS/RSVP task at the PLR for bypass/detour association until the next opportunity the primary path is re-signaled. The path may be re-signaled due to a failure or to a make-before break operation. Make-before break occurs as a result of a global revertive operation, a timer based or manual re-optimization of the LSP path, or a user change to any of the path constraints.

Once the bypass or detour path is setup and is operationally UP, any subsequent changes to the SRLG group membership of an interface the bypass/detour path is using would not be considered by the MPLS/RSVP task at the PLR until the next opportunity the association with the primary LSP path is re-checked. The association is re-checked if the bypass path is re-optimized. Detour paths are not re-optimized and are re-signaled if the primary path is down.

The user must first shutdown mpls before enabling or disabling the srlg-frr option in CLI.

An RSVP interface can belong to a maximum of 64 SRLG groups. The user configures the SRLG groups using the command **config>router>mpls>srlg-group**. The user configures the SRLG groups an RSVP interface belongs to using the **srlg-group** command in the **config>router>mpls>interface** context.

The **no** form of the command reverts to the default value.

Default no srlg-frr

Parameters **strict** **—** Specifies the name of the SRLG group within a virtual router instance.

Values
no slr-frr (default)
srlg-frr (non-strict)
srlg-frr **strict** (strict)

srlg-group

Syntax **srlg-group** *group-name* {**value** *group-value*}
no srlg-group *group-name*

Context config>router>mpls

Description This command is used to define shared risk loss groups (SRLGs). An SRLG group represents a set of interfaces which could be subject to the same failures or defects and thus share the same risk of failing.

RSVP interfaces must be explicitly assigned to an SRLG group. SRLG groups must be defined in the **config>router>mpls** context before they can be assigned to an RSVP interface. Two different SRLG group names cannot share the same value. Once an SRLG group has been bound to an MPLS interface, its value cannot be changed until the binding is removed.

The IGP communicates the information throughout the area using the TE link state advertisement. CSPF uses the information when paths are computed for constraint-based LSPs. CSPF must be enabled in order for SRLG groups to be relevant.

Up to 1024 group names can be defined in the **config>router>mpls** context. The SRLG group names must be identical across all routers in a single domain.

The **no** form of this command deletes the SRLG group.

Default none

Parameters *group-name* — Specifies the name of up to 32 characters of the SRLG group within a virtual router instance.

value *group-value* **—** Specifies the group value associated with this SRLG group. This value is unique within a virtual router instance.

Values 0 — 4294967295

user-srlg-db

Syntax **user-srlg-db** [**enable | disable**]

Context config>router>mpls

Description This command enables the use of CSPF by the user SRLG database. When the MPLS module makes a request to CSPF for the computation of an SRLG secondary path, CSPF will query the local SRLG and compute a path after pruning links that are members of the SRLG IDs of the associated primary path. When MPLS makes a request to CSPF for an FRR bypass or detour path to associate with the primary path, CSPF queries the user SRLG database and computes a path after pruning links that are members of the SRLG IDs of the PLR outgoing interface.

If an interface was not entered into the user SRLG database, it is assumed that it does not have any SRLG membership. CSPF will not query the TE database for IGP advertised interface SRLG information.

The disable keyword disables the use of the user SRLG database. CSPF will then resume queries into the TE database for SRLG membership information. The user SRLG database is maintained.

Default user-srlg-db disable

srlg-database

Syntax [**no**] **srlg-database**

Context config>router>mpls

Description This command provides the context for the user to enter manually the link members of SRLG groups for the entire network at any node that needs to signal LSP paths (for example, a head-end node).

The **no** form of the command deletes the entire SRLG database. CSPF will assume all interfaces have no SRLG membership association if the database was not disabled with the command **config>router>mpls>user-srlg-db disable**.

router-id

Syntax [**no**] **router-id** *ip*

Context config>router>mpls>srlg-database

Description This command provides the context for the user to manually enter the link members of SRLG groups for a specific router in the network. The user must also use this command to enter the local interface SRLG membership into the user SRLG database. Use by CSPF of all interface SRLG membership information of a specific router ID may be temporarily disabled by shutting down the node. If this occurs, CSPF will assume these interfaces have no SRLG membership association.

The **no** form of this command will delete all interface entries under the router ID.

Parameters *ip-address* — Specifies the router ID for this system. This must be the router ID configured under the base router instance, the base OSPF instance or the base IS-IS instance.

interface

Syntax **interface** *ip-address* **srlg-group** *group-name* [*group-name*...(up to 5 max)]
no interface *ip-address* [**srlg-group** *group-name*...(up to 5 max)]

Context config>router>mpls>srlg-database>router-id

Description This command allows the operator to manually enter the SRLG membership information for any link in the network, including links on this node, into the user SRLG database.

An interface can be associated with up to 5 SRLG groups for each execution of this command. The operator can associate an interface with up to 64 SRLG groups by executing the command multiple times.

CSPF will not use entered SRLG membership if an interface is not validated as part of a router ID in the routing table.

The **no** form of the command deletes a specific interface entry in this user SRLG database. The **group-name** must already exist in the **config>router>mpls>srlg-group** context.

Default none

Parameters *ip-int-name* — The name of the network IP interface. An interface name cannot be in the form of an IP address.

srlg-group *group-name* — Specifies the SRLG group name. Up to 1024 group names can be defined in the **config>router>mpls** context. The SRLG group names must be identical across all routers in a single domain.

MPLS Interface Commands

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>router>mpls

Description This command specifies MPLS protocol support on an IP interface. No MPLS commands are executed on an IP interface where MPLS is not enabled. An MPLS interface must be explicitly enabled (**no shutdown**).

The **no** form of this command deletes all MPLS commands such as **label-map** which are defined under the interface. The MPLS interface must be shutdown first in order to delete the interface definition. If the interface is not shutdown, the **no interface** *ip-int-name* command does nothing except issue a warning message on the console indicating that the interface is administratively up.

Default **shutdown**

Parameters *ip-int-name* — The name of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 1 to 32 alphanumeric characters.

admin-group

Syntax [**no**] **admin-group** *group-name* [*group-name*...(up to 5 max)]

Context config>router>mpls>interface

Description This command defines admin groups that this interface supports.

This information is advertised as part of OSPF and IS-IS to help CSPF compute constrained LSPs that must include or exclude certain admin groups. An MPLS interface is assumed to belong to all the admin groups unless the 'admin-group' command is issued under the interface config. Once an 'admin-group' command is issued the interface is assumed to belong to only the specifically listed groups for that command.

Each single operation of the admin-group command allows a maximum of 5 groups to be specified at a time. However, a maximum of 32 groups can be specified per inteface through multiple operations.

Default no admin-group

Parameters *group-name* — Name of the group. The group names should be the same across all routers in the MPLS domain.

auto-bandwidth-multipliers

Syntax **auto-bandwidth-multipliers sample-multiplier** *number1* **adjust-multiplier** *number2*
no auto-bandwidth-multipliers

Context config>router>mpls>

Description This command specifies the number of collection intervals in the adjust interval.

Parameters **sample-multiplier** *number1* **—** Specifies the mulitplier for collection intervals in a sample interval.

Values 1 — 511

Default 1

adjust-multiplier *number2* **—** Specifies the number of collection intervals in the adjust interval.

Values 1 — 16383

Default 288

srlg-group

Syntax [**no**] **srlg-group** *group-name* [*group-name*...(up to 5 max)]

Context config>router>mpls>interface

Description This command defines the association of RSVP interface to an SRLG group. An interface can belong to up to 64 SRLG groups. However, each single operation of the **srlg-group** command allows a maximum of 5 groups to be specified at a time.

The **no** form of this command deletes the association of the interface to the SRLG group.

Default none

Parameters *group-name* — Specifies the name of the SRLG group within a virtual router instance up to 32 characters.

te-metric

Syntax **te-metric** *value*
no te-metric

Context config>router>mpls>interface

Description This command configures the traffic engineering metric used on the interface. This metric is in addition to the interface metric used by IGP for the shortest path computation.

This metric is flooded as part of the TE parameters for the interface using an opaque LSA or an LSP. The IS-IS TE metric is encoded as sub-TLV 18 as part of the extended IS reachability TLV. The metric value is encoded as a 24-bit unsigned integer. The OSPF TE metric is encoded as a sub-TLV Type 5 in the Link TLV. The metric value is encoded as a 32-bit unsigned integer.

When the use of the TE metric is enabled for an LSP, CSPF will first prune all links in the network topology which do not meet the constraints specified for the LSP path. Such constraints include bandwidth, admin-groups, and hop limit. Then, CSPF will run an SPF on the remaining links. The shortest path among the all SPF paths will be selected based on the TE metric instead of the IGP metric which is used by default.

The TE metric in CSPF LSP path computation can be configured by entering the command **config>router>mpls>lsp>cspf>use-te-metric**.

Note that the TE metric is only used in CSPF computations for MPLS paths and not in the regular SPF computation for IP reachability.

The **no** form of the command reverts to the default value.

Default no te-metric

The value of the IGP metric is advertised in the TE metric sub-TLV by IS-IS and OSPF.

Parameters *value* — Specifies the metric value.

Values 1 — 16777215

preemption-timer

Syntax **preemption-timer** *seconds*
no preemption-timer

Context config>router>rsvp

Description This parameter configures the time in seconds a 7750 node holds to a reservation for which it triggered the soft pre-emption procedure.

The 7750 pre-empting node starts a separate preemption timer for each pre-empted LSP path. While this timer is on, the node should continue to refresh the Path and Resv for the pre-empted LSP paths. When the preemption timer expires, the node tears down the reservation if the head-end node has not already done so.

A value of zero means the LSP should be pre-empted immediately; hard pre-empted.

The **no** form of this command reverts to the default value.

Default 300

Parameters *seconds* — Specifies the time, in seconds, of the preemption timer.

Values 0 — 1800 seconds

label-map

Syntax [**no**] **label-map** *in-label*

Context config>router>mpls>interface

Description This command is used on transit routers when a static LSP is defined. The static LSP on the ingress router is initiated using the **config router mpls static-lsp** *lsp-name* command. An *in-label* can be associated with either a **pop** or a **swap** action, but not both. If both actions are specified, the last action specified takes effect.

The **no** form of this command deletes the static LSP configuration associated with the *in-label*.

Parameters *in-label* — Specifies the incoming MPLS label on which to match.

Values 32 — 1023

pop

Syntax [**no**] **pop**

Context config>router>mpls>if>label-map

Description This command specifies that the incoming label must be popped (removed). No label stacking is supported for a static LSP. The service header follows the top label. Once the label is popped, the packet is forwarded based on the service header.

The **no** form of this command removes the **pop** action for the *in-label*.

Default none

shutdown

Syntax [**no**] **shutdown**

Context config>router>mpls>if>label-map

Description This command disables the label map definition. This drops all packets that match the specified *in-label* specified in the **label-map** *in-label* command.

The **no** form of this command administratively enables the defined label map action.

Default **no shutdown**

swap

Syntax **swap** {*out-label* **| implicit-null-label**} **nexthop** *ip-address*
no swap {*out-label* **| implicit-null-label**}

Context config>router>mpls>interface>label-map

Description This command swaps the incoming label and specifies the outgoing label and next hop IP address on an LSR for a static LSP.

The **no** form of this command removes the swap action associated with the *in-label*.

Default none

Parameters **implicit-null-label** — Specifies the use of the implicit label value for the outgoing label of the swap operation.

out-label — Specifies the label value to be swapped with the in-label. Label values 16 through 1,048,575 are defined as follows:
Label values 16 through 31 are 7750 SR reserved.
Label values 32 through 1,023 are available for static assignment.
Label values 1,024 through 2,047 are reserved for future use.
Label values 2,048 through 18,431 are statically assigned for services.
Label values 28,672 through 131,071 are dynamically assigned for both MPLS and services.
Label values 131,072 through 1,048,575 are reserved for future use.

Values 16 — 1048575

nexthop *ip-address* **—** The IP address to forward to. If an ARP entry for the next hop exists, then the static LSP will be marked operational. If ARP entry does not exist, software will set the operational status of the static LSP to down and continue to ARP for the configured nexthop. Software will continuously try to ARP for the configured nexthop at a fixed interval.

LSP Commands

lsp

Syntax [**no**] **lsp** *lsp-name* [**bypass-only | p2mp-lsp**]

Context config>router>mpls

Description This command creates an LSP that is signaled dynamically by the 7750 SR OS.

When the LSP is created, the egress router must be specified using the **to** command and at least one **primary** or **secondary** path must be specified. All other statements under the LSP hierarchy are optional. Notre that the maximum number of static configurable LSPs is 4.

LSPs are created in the administratively down (**shutdown**) state.

The **no** form of this command deletes the LSP. All configuration information associated with this LSP is lost. The LSP must be administratively shutdown and unbound from all SDPs before it can be deleted.

Default none

Parameters *lsp-name* — Name that identifies the LSP. The LSP name can be up to 32 characters long and must be unique.

bypass-only — Defines an LSP as a manual bypass LSP exclusively. When a path message for a new LSP requests bypass protection, the PLR first checks if a manual bypass tunnel satisfying the path constraints exists. If one if found, the 7750 selects it. If no manual bypass tunnel is found, the 7750 dynamically signals a bypass LSP in the default behavior. The CLI for this feature includes a knob that provides the user with the option to disable dynamic bypass creation on a per node basis.

p2mp-lsp — Defines an LSP as a point-to-multipoint LSP. The following parameters can be used with a P2MP LSP: adaptive, adspec, cspf, exclude, fast-reroute, from, hop-limit, include, metric, retry-limit, retry-timer, resignal-timer. The following parameters cannot be used with a P2MP LSP: primary, secondary, to.

adaptive

Syntax [**no**] **adaptive**

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This command enables the make-before-break functionality for an LSP or LSP path. When enabled for the LSP, make-before-break will be performed for primary path and all the secondary paths of the LSP.

Default adaptive

adspec

Syntax [**no**] **adspec**

Context config>router>mpls>lsp

Description When enabled, the ADSPEC object will be included in RSVP messages.

Default **no adspec —** No ADSPEC objects are included in RSVP messages.

auto-bandwidth

Syntax [**no**] **auto-bandwidth**

Context config>router>mpls>lsp

Description This command enables automatic adjustments of LSP or SDP bandwidth.

Auto-bandwidth at the LSP level cannot be executed unless cspf and adaptive are configured in the **config>router>mpls>lsp** context.

Auto-bandwidth at the SDP level cannot be executed unless the SDP type is MPLS, the SDP is comprised of only RSVP LSPs, all of the RSVP LSPs have auto-bandwidth enabled and the adjust-up, adjust-down and overflow-limit commands are not present in the auto-bandwidth configuration of any of the RSVP LSPs.

The **no** form of the command disables the automatic adjustments of LSP or SDP bandwidth.

adjust-down

Syntax **adjust-down** *percent* [**bw** *mbps*]
no adjust-down

Context config>router>mpls>lsp>auto-bandwidth

Description This command configures the minimum threshold for decreasing the bandwidth of an LSP based on active measurement of LSP bandwidth.

The **no** form of this command is equivalent to adjust-down 5.

Default no adjust-down

Parameters *percent* — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as a percentage of the current bandwidth, for decreasing the bandwidth of the LSP.

Values 1 — 100

Default 5

mbps — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as an absolute bandwidth (mbps), for decreasing the bandwidth of the LSP.

Values 0 — 100000

Default 0

adjust-up

Syntax **adjust-up** *percent* [**bw** *mbps*]
no adjust-up

Context config>router>mpls>lsp>auto-bandwidth

Description This command configures the minimum threshold for increasing the bandwidth of an LSP based on active measurement of LSP bandwidth.

The **no** form of this command is equivalent to adjust-up 5.

Default no adjust-up

Parameters *percent* — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as a percentage of the current bandwidth, for increasing the bandwidth of the LSP.

1-100

Default 5

mbps — Specifies the minimum difference between the current bandwidth reservation of the LSP and the (measured) maximum average data rate, expressed as an absolute bandwidth (mbps), for increasing the bandwidth of the LSP

Values 0 — 100000

Default 0

max-bandwidth

Syntax **max-bandwidth** *mbps*
no max-bandwidth

Context config>router>mpls>lsp>auto-bandwidth

Description This command configures the maximum bandwidth that auto-bandwidth allocation is allowed to request for an LSP or SDP.

The LSP maximum applies whether the bandwidth adjustment is triggered by normal adjust-timer expiry, the overflow limit having been reached, or manual request or SDP auto-bandwidth adjustment.

The SDP maximum applies to bandwidth adjustment caused by VLL CAC. The SDP maximum bandwidth must be less than or equal to the sum of the max-bandwidth parameters of the LSPs in the SDP.

This command is mandatory at the LSP level if an overflow-limit is configured.

The **no** form of the command means max-bandwidth is infinite (equivalent to 100 Gbps).

Default no max-bandwidth

Parameters *mbps* — Specifies the maximum bandwidth in mbps.

Values 0 — 100000

Default 0

min-bandwidth

Syntax **min-bandwidth** *mbps*
no min-bandwidth

Context config>router>mpls>lsp>auto-bandwidth

Description This command configures the minimum bandwidth that auto-bandwidth allocation is allowed to request for an LSP or SDP.

The LSP minimum applies whether the bandwidth adjustment is triggered by normal adjust-timer expiry or, manual request or SDP auto-bandwidth adjustment.

The **no** form of the command means min-bandwidth is zero.

Default no min-bandwidth

Parameters *mbps* — Specifies the minimum bandwidth in mbps.

Values 0 — 100000

Default 0

monitor-bandwidth

Syntax [**no**] **monitor-bandwidth**

Context config>router>mpls>lsp>auto-bandwidth

Description This command enables the collection and display of auto-bandwidth measurements, but prevents any automatic bandwidth adjustments from taking place, other than those caused by VLL CAC (through an SDP bandwidth change).

This command is mutually exclusive with the **overflow-limit** command.

The **no** form of the command the collection and display of auto-bandwidth measurements.

multipliers

Syntax **multipliers sample-multiplier** *num1* **adjust-multiplier** *num2*
no multipliers

Context config>router>mpls>lsp>auto-bandwidth

Description This command configures the number of collection intervals between measurements of the number of bytes that have been transmitted on the LSP. The byte counts include the layer 2 encapsulation of MPLS packets and represent traffic of all forwarding classes and priorities (in-profile vs, out-of-profile) belonging to the LSP.

The router calculates the average data rate in each sample interval. The maximum of this average data rate over multiple sample intervals is the measured bandwidth input to the auto-bandwidth adjustment algorithms.

The count is not allowed to be set a value greater than adjust-count.

The **no** form of this command instructs the system to take the value from the auto-bandwidth-defaults command.

Default no sample-count

Parameters *number* — The number of collection intervals in a sample interval.

Values 1 — 511

Default 1

overflow-limit

Syntax **overflow-limit** *number* **threshold** *percent* [**bw** *mbps*]
no overflow-limit

Context config>router>mpls>lsp>auto-bandwidth

Description This command configures overflow-triggered auto-bandwidth adjustment. It sets the threshold at which bandwidth adjustment is initiated due to the configured number of overflow samples having been reached, regardless of how much time remains until the adjust interval ends.

A sample interval is counted as an overflow if the average data rate during the sample interval is higher than the currently reserved bandwidth by at least the thresholds configured as part of this command.

If overflow-triggered auto-bandwidth adjustment is successful the overflow count and adjust-timer are reset. If overflow-triggered auto-bandwidth adjustment fails then the overflow count is reset but the adjust-timer continues.

This command is mutually exclusive with the **monitor-bandwidth** command.

This command will fail if the max-bandwidth value at the config>router>mpls>lsp>auto-bandwidth level is not configured or if it is set to infinite (100 Gbps)zero.

The **no** form of this command disables overflow-triggered automatic bandwidth adjustment.

Default no overflow-limit

Parameters *number* — The number of overflow samples that triggers an overflow auto-bandwidth adjustment attempt.

Values 1 — 10

Default none

percent — The minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as a percentage of the current bandwidth, for counting an overflow sample.

Values 1 — 100

Default none

mbps — The minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as an absolute bandwidth (Mbps) relative to the current bandwidth, for counting an overflow sample.

Values 1— 100000

Default 0

class-type

Syntax **class-type** *ct-number*
no class-type

Context config>router>mpls>lsp
config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This command configures the Diff-Serv Class Type (CT) for an LSP, the LSP primary path, or the LSP secondary path. The path level configuration overrides the LSP level configuration. However, only one CT per LSP path will be allowed as per RFC 4124.

The signaled CT of a dynamic bypass is always be CT0 regardless of the CT of the primary LSP path. The setup and hold priorities must be set to default values, i.e., 7 and 0 respectively. This assumes that the operator configured a couple of TE classes, one which combines CT0 and a priority of 7 and the other which combines CTO and a priority of 0. If not, the bypass LSP will not be signaled and will go into the down state.

The operator cannot configure the CT, setup priority, and hold priority of a manual bypass. They are always signaled with CT0 and the default setup and holding priorities.

The signaled CT and setup priority of a detour LSP must match those of the primary LSP path it is associated with.

If the operator changes the CT of an LSP or of an LSP path, or changes the setup and holding priorities of an LSP path, the path will be torn down and retried.

An LSP which does not have the CT explicitly configured will behave like a CT0 LSP when Diff-Serv is enabled.

If the operator configured a combination of a CT and a setup priority and/or a combination of a CT and a holding priroty for an LSP path that are not supported by the user-defined TE classes, the LSP path will be kept in a down state and an error code will be displayed in the show command output for the LSP path.

The **no** form of this command reverts to the default value.

Default no class-type.

Parameters *ct-number* — The Diff-Serv Class Type number.

Values 0 – 7

Default 0

bandwidth

Syntax **bandwidth** *rate-in-mbps*

Context config>router>mpls>lsp>primary-p2mp-instance
config>router>mpls>lsp-template

Description This command specifies the amount of bandwidth to be reserved for the P2MP instance.

Parameters *rate-in-mbps* — specifies the bandwidth, in Mbps.

Values 0 — 100000

cspf

Syntax [**no**] **cspf** [*use-te-metric*]

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This command enables Constrained Shortest Path First (CSPF) computation for constrained-path LSPs. Constrained-path LSPs are the ones that take configuration constraints into account. CSPF is also used to calculate the detour routes when fast-reroute is enabled.

Explicitly configured LSPs where each hop from ingress to egress is specified do not use CSPF. The LSP will be set up using RSVP signaling from ingress to egress.

If an LSP is configured with **fast-reroute** *frr-method* specified but does not enable CSPF, then neither global revertive nor local revertive will be available for the LSP to recover.

Default no cspf

Parameters *use-te-metric* — Specifies to use the use of the TE metric for the purpose of the LSP path computation by CSPF.

exclude

Syntax [**no**] **exclude** *group-name* [*group-name*...(up to 5 max)]

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This command specifies the admin groups to be excluded when an LSP is set up in the primary or secondary contexts. Each single operation of the exclude command allows a maximum of 5 groups to be specified at a time. However, a maximum of 32 groups can be specified per LSP through multiple operations. The admin groups are defined in the **config>router>mpls>admin-group** context.

Use the **no** form of the command to remove the exclude command.

Default no exclude

Parameters *group-name* — Specify the existing group-name to be excluded when an LSP is set up.

fast-reroute

Syntax **fast-reroute** *frr-method*
no fast-reroute

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This command creates a pre-computed detour LSP from each node in the path of the LSP. In case of failure of a link or LSP between two nodes, traffic is immediately rerouted on the pre-computed detour LSP, thus avoiding packet-loss.

When **fast-reroute** is enabled, each node along the path of the LSP tries to establish a detour LSP as follows:

- Each upstream node sets up a detour LSP that avoids only the immediate downstream node, and merges back on to the actual path of the LSP as soon as possible.

  If it is not possible to set up a detour LSP that avoids the immediate downstream node, a detour can be set up to the downstream node on a different interface.
- The detour LSP may take one or more hops (see **hop-limit**) before merging back on to the main LSP path.
- When the upstream node detects a downstream link or node failure, the ingress router switches traffic to a standby path if one was set up for the LSP.

Fast reroute is available only for the primary path. No configuration is required on the transit hops of the LSP. The ingress router will signal all intermediate routers using RSVP to set up their detours. TE must be enabled for fast-reroute to work.

If an LSP is configured with **fast-reroute** *frr-method* specified but does not enable CSPF, then neither global revertive nor local revertive will be available for the LSP to recover.

The **no** form of the **fast-reroute** command removes the detour LSP from each node on the primary path. This command will also remove configuration information about the hop-limit and the bandwidth for the detour routes.

The **no** form of **fast-reroute hop-limit** command reverts to the default value.

Default **no fast-reroute** — When fast-reroute is specified, the default fast-reroute method is one-to-one.

Parameters **Values** **one-to-one** — In the one-to-one technique, a label switched path is established which intersects the original LSP somewhere downstream of the point of link or node failure. For each LSP which is backed up, a separate backup LSP is established.

facility — This option, sometimes called **many-to-one**, takes advantage of the MPLS label stack. Instead of creating a separate LSP for every backed-up LSP, a single LSP is created which serves to backup up a set of LSPs. This LSP tunnel is called a bypass tunnel.

The bypass tunnel must intersect the path of the original LSP(s) somewhere downstream of the point of local repair (PLR). Naturally, this constrains the set of LSPs being backed-up via that bypass tunnel to those that pass through a common downstream node. All LSPs which pass through the PLR and through this common node which do not also use the facilities involved in the bypass tunnel are candidates for this set of LSPs.

bandwidth

Syntax **bandwidth** *rate-in-mbps*
no bandwidth

Context config>router>mpls>lsp>fast-reroute
config>router>mpls>lsp-template>fast-reroute

Description This command is used to request reserved bandwidth on the detour path. When configuring an LSP, specify the traffic rate associated with the LSP.

When configuring fast reroute, allocate bandwidth for the rerouted path. The bandwidth rate does not need to be the same as the bandwidth allocated for the LSP.

Default no bandwidth — Bandwidth is not reserved for a rerouted path.

Parameters *rate-in-mbps* — Specifies the amount of bandwidth in Mbps to be reserved for the LSP path.

hop-limit

Syntax **hop-limit** *limit*
no hop-limit

Context config>router>mpls>lsp>fast-reroute
config>router>mpls>lsp-template>fast-reroute

Description For fast reroute, how many more routers a detour is allowed to traverse compared to the LSP itself. For example, if an LSP traverses four routers, any detour for the LSP can be no more than ten router hops, including the ingress and egress routers.

Default 16

Parameters *limit* — Specify the maximum number of hops.

Values 0 — 255

node-protect

Syntax [**no**] **node-protect**

Context config>router>mpls>lsp>fast-reroute

Description This command enables or disables node and link protection on the specified LSP. Node protection ensures that traffic from an LSP traversing a neighboring router will reach its destination even if the neighboring router fails.

Default node-protect

from

Syntax **from** *ip-address*

Context config>router>mpls>lsp

Description This optional command specifies the IP address of the ingress router for the LSP. When this command is not specified, the system IP address is used. IP addresses that are not defined in the system are allowed. If an invalid IP address is entered, LSP bring-up fails and an error is logged.

If an interface IP address is specified as the **from** address, and the egress interface of the nexthop IP address is a different interface, the LSP is not signaled. As the egress interface changes due to changes in the routing topology, an LSP recovers if the **from** IP address is the system IP address and not a specific interface IP address.

Only one **from** address can be configured.

Default The system IP address

Parameters *ip-address* — This is the IP address of the ingress router. This can be either the interface or the system IP address. If the IP address is local, the LSP must egress through that local interface which ensures local strictness.

Default System IP address

Values System IP or network interface IP addresses

hop-limit

Syntax **hop-limit** *number*
no hop-limit

Context config>router>mpls>lsp
config>router>mpls>lsp>fast-reroute
config>router>mpls>lsp-template

Description This command specifies the maximum number of hops that an LSP can traverse, including the ingress and egress routers. An LSP is not set up if the hop limit is exceeded. This value can be changed dynamically for an LSP that is already set up with the following implications:

If the new value is less than the current number of hops of the established LSP, the LSP is brought down. Software then tries to re-establish the LSP within the new **hop-limit** number. If the new value is equal to or greater than the current number hops of the established LSP, then the LSP is not affected.

The **no** form of this command returns the parameter to the default value.

Default **255**

Parameters *number* — The number of hops the LSP can traverse, expressed as an integer.

Values 2 — 255

Values 0 — 255

ldp-over-rsvp

Syntax **ldp-over-rsvp** [**include** | **exclude**]

Context config>router>mpls>lsp

Description This command specifies if this LSP will be included in LDP over RSVP.

Parameters **include —** Specifies that this LSP will be included in LDP over RSVP.

exclude — Specifies that this LSP will be excluded from LDP over RSVP.

igp-shortcut

Syntax [**no**] **igp-shortcut**

Context config>router>mpls>lsp

Description This command enables the use of a specific RSVP LSP by IS-IS and OSPF routing protocols as a shortcut for resolving IGP routes.

When rsvp-shortcut is enabled at the IGP instance level, all RSVP LSPs originating on this node are eligible by default as long as the destination address of the LSP, as configured in config>router>mpls>lsp>to, corresponds to a router-id of a remote node.

The **no** form of this command disables the use of a specific RSVP LSP by IS-IS and OSPF routing protocols as a shortcut for resolving IGP routes.

Default igp-shortcut

least-fill

Syntax [**no**] **least-fill**

Context config>router>mpls>lsp

Description This command enables the use of the least-fill path selection method for the computation of the path of this LSP.

When MPLS requests the computation of a path for this LSP, CSPF will find all equal cost shortest paths which satisfy the constraints of this path. Then, CSPF identifies the single link in each of these paths which has the least available bandwidth as a percentage of its maximum reservable bandwidth. It then selects the path which has the largest value of this percentage least available bandwidth figure. CSPF identifies the least available bandwidth link in each equal cost path after it has accounted for the bandwidth of the new requested path of this LSP.

CSPF applies the least-fill path selection method to all requests for a path, primary and secondary, of an LSP for which this option is enabled. The bandwidth of the path can be any value, including zero.

CSPF applies the least-fill criterion separately to each pre-emption priority in the base TE. A higher setup priority path can pre-empt lower holding priority paths.

CSPF also applies the least-fill criterion separately to each Diff-Serv TE class if Diff-Serv TE is enabled on this node. A higher setup priority path can pre-empt lower holding priority paths within a Class Type.

MPLS will re-signal and move the LSP to the new path in the following cases:

- Initial LSP path signaling.
- Re-try of an LSP path after failure.
- Make-before-break (MBB) due to pending soft pre-emption of the LSP path.
- MBB due to LSP path configuration change, i.e., a user change to bandwidth parameter of primary or secondary path, or a user enabling of fast-reroute option for the LSP.
- MBB of secondary path due to an update to primary path SRLG.
- MBB due to FRR Global Revertive procedures on the primary path.
- Manual re-signaling of an LSP path or of all LSP paths by the user.

During a manual re-signaling of an LSP path, MPLS will always re-signal the path regardless of whether the new path is exactly the same or different than the current path and regardless or whether the metric of the new path is different or not from that of the current path.

During a timer-based re-signaling of an LSP path which has the least-fill option enabled, MPLS will only re-signal the path if the metric of the new path is different than the one of the current path.

The user deletes a specific node entry in this database by executing the no form of this command.

Default no least-fill. The path of an LSP is randomly chosen among a set of equal cost paths.

ldp-over-rsvp

Syntax [**no**] **ldp-over-rsvp** [**include** | **exclude**]

Context config>router>mpls>lsp

Description This command configures an LSP so that it can be used by the IGP to calculate its SPF tree.

The IGP (OSPF/ISIS) will subsequently provide LDP with all ECMP IGP next-hops and tunnel endpoints that it considers to be the lowest cost path to its destination.

If an IGP calculation and an LDP-over-RSVP indicate the same cost then LDP will always prefer an LDP-over-RSVP tunnel over an IGP route and ECMP between the two types is not considered.

The type and number of tunnels considered by LDP depends on the IGP metrics (the lowest metric between the tunnel endpoint and the target is selected) assuming that each LSP has a TLDP session established between the endpoints.

Enter the command **ldporsvp include** to make the associated LSP available to be used by the LDP-over-RSVP feature.

The no form of the command reverts to default operation.

Default ldporsvp exclude

include

Syntax [**no**] **include** *group-name* [*group-name*...(up to 5max)]

Context config>router>mpls>lsp
config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary
config>router>mpls>lsp-template

Description This command specifies the admin groups to be included when an LSP is set up. Up to 5 groups per operation can be specified, up to 32 maximum.

The **no** form of the command deletes the specified groups in the specified context.

Default no include

Parameters *group-name* — Specifies admin groups to be included when an LSP is set up.

priority

Syntax **priority setup-priority** *hold-priority*
no priority

Context config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This command enables the soft pre-emption procedures for this LSP path. The operator enables the soft pre-emption mechanism on a specific LSP name by explicitly configuring the setup and holding priorities for the primary path at the 7x50 head-end node. The operator can similarly configure priority values for a secondary path for this LSP name. Different values could be used for the primary and for any of the secondary paths. In the absence of explicit user configuration, the setup priority is internally set to the default value of 7 and the holding priority is set to the default value of 0. Note however that valid user-entered values for these two parameters require that the setup priority is numerically lower than or equal to the holding priority, otherwise pre-emption loops can occur.

Pre-emption is effected when a 7x50 pre-empting node processes a new RSVP session reservation and there is not enough available bandwidth on the RSVP interface, or the Class Type (CT) when Diff-Serv is enabled, to satisfy the bandwidth in the Flowspec object while there exist other session reservations for LSP paths with a strictly lower holding priority (numerically higher holding priority value) than the setup priority of the new LSP reservation. If enough available bandwidth is freed on the link or CT to accommodate the new reservation by pre-empting one or more lower priority LSP paths, the pre-empting node allows temporary overbooking of the RSVP interface and honors the new reservation.

The 7x50 pre-empting node will immediately set the 'Preemption pending' flag (0x10) in the IPv4 Sub-Object in the RRO object in the Resv refresh for each of the pre-empted LSP paths. The IPv4 Sub-Object corresponds to the outgoing interface being used by the pre-empting and pre-empted LSP paths. Note however that the bandwidth value in the Flowspec object is not changed. The Resv flag must also be set if the pre-empting node is a merge point for the primary LSP path and the backup bypass LSP or detour LSP and the backup LSP is activated.

When evaluating if enough available bandwidth will be freed, the 7x50 pre-empting node considers the reservations in order from the lowest holding priority (numerically higher holding priority value) to the holding priority just below the setup priority of the new reservation. A new reservation cannot pre-empt a reservation which has a value of the holding priority equal to the new reservation setup priority.

When Diff-Serv is enabled on the pre-empting node and the MAM bandwidth allocation model is used, a new reservation can only pre-empt a reservation in the same Class Type (CT).

LSP paths which were not flagged at the head-end for soft pre-emption will be hard pre-empted. LSP paths with the default holding priority of 0 cannot be pre-empted. LSP paths with zero bandwidth do not pre-empt other LSP paths regardless of the values of the path setup priority and the path holding priority. They can also not be pre-empted.

When evaluating if enough available bandwidth will be freed, the 7x50 pre-empting node considers the reservations in order from the lowest holding priority (numerically higher holding priority) to the holding priority just below the setup priority of the new reservation. There is no specific order in which the reservations in the same holding priority are considered. Furthermore, LSP paths which were not flagged at the head-end for soft pre-emption cannot be pre-empted because their holding priority is set internally to 0.

The 7x50 pre-empting node starts a preemption timer for each of the pre-empted LSP paths. While this timer is on, the node should continue to refresh the Path and Resv for the pre-empted LSP paths. When the preemption timer expires, the node tears down the reservation if the head-end node has not already done so.

A 7x50 head-end node upon receipt of the Resv refresh message with the 'Preemption pending' flag must immediately perform a make-before-break on the affected adaptive CSPF LSP. Both IGP metric and TE metric based CSPF LSPs are included. If an alternative path that excludes the flagged interface is not found, then the LSP is put on a retry in a similar way to the Global Revertive procedure at a 7x50 head-end node. However, the number of retries and the retry timer are governed by the values of the retry-limit and retry-timer parameters: config>router>mpls>lsp>retry-limit; config>router>mpls>lsp>retry-timer.

Note that MPLS will keep the address list of flagged interfaces for a maximum of 60 seconds (not user-configurable) from the time the first Resv message with the ‘Preemption pending’ flag is received. This actually means that MPLS will request CSPF to find a path that excludes the flagged interfaces in the first few retries until success or until 60 seconds have elapsed. Subsequent retries after the 60 seconds will not exclude the flagged interfaces as it is assumed IGP has converged by then and the Unreserved Bandwidth sub-TLV for that priority, or TE Class, in the TE database will show the updated value taking into account the pre-empting LSP path reservation or a value of zero if overbooked.

If the LSP has a configured secondary standby which is operationally UP, the 7x50 will switch the path of the LSP to it and then start the MBB. If no standby path is available and a secondary non-standby is configured, the 7x50 will start the MBB and signal the path of the secondary. The LSP path will be switched to either the secondary or the new primary, whichever comes up first.

The no form of the command reverts the LSP path priority to the default values and results in setting the setup priority to 7, in setting the holding priority to 0, and in clearing the ‘soft preemption desired’ flag in the RRO in the Resv refresh message.

Default no priority.

Parameters *setup-priority* — The priority of the reservation for this session at setup time.

Values 0 — 7 (0 is the highest priority and 7 is the lowest priority.)

Default 7 — This session does not pre-empt any other session.

holding-priority — The priority of the reservation for this session at pre-emption action.

Values 0 — 7 (0 is the highest priority and 7 is the lowest priority.)

Default 0 — This session does not get pre-empted by any other session.

main-ct-retry-limit

Syntax **main-ct-retry-limit number**
no main-ct-retry-limit

Context config>router>mpls>lsp

Description This command configures the maximum number of retries the LSP primary path should be retried with the LSP Diff-Serv main Class Type (CT).

When an unmapped LSP primary path goes into retry, it uses the main CT until the number of retries reaches the value of the new main-ct-retry-limit parameter. If the path did not come up, it must start using the backup CT at that point in time. By default, this parameter is set to infinite value. The new main-ct-retry-limit parameter has no effect on an LSP primary path which retries due to a failure event.

An unmapped LSP primary path is a path which has never received a Resv in response to the first Path message sent. This can occur when performing a “shut/no-shut” on the LSP or LSP primary path or when the node reboots. An unmapped LSP primary path goes into retry if the retry timer expired or the head-end node received a PathErr message before the retry timer expired.

If the user entered a value of the main-ct-retry-limit parameter that is greater than the value of the LSP retry-limit, the number of retries will still stop when the LSP primary path reaches the value of the LSP retry-limit. In other words, the meaning of the LSP retry-limit parameter is not changed and always represents the upper bound on the number of retries. The unmapped LSP primary path behavior applies to both CSPF and non-CSPF LSPs.

The **no** form of this command sets the parameter to the default value of zero (0) which means the LSP primary path will retry forever.

Default no main-ct-retry-limit

Parameters *number* — The number of times MPLS will attempt to re-establish the LSP primary path using the Diff-Serv main CT. Allowed values are integers in the range of zero (0) to 10,000, where zero indicates to retry infinitely.

Values 0-1000, integer

metric

Syntax **metric** *metric*

Context config>router>mpls>lsp

Description This command specifies the metric for this LSP which is used to select an LSP among a set of LSPs which are destined to the same egress router. The LSP with the lowest metric will be selected.

In LDP-over-RSVP, LDP performs a lookup in the Routing Table Manager (RTM) which provides the next hop to the destination PE and the advertising router (ABR or destination PE itself). If the advertising router matches the targeted LDP peer, LDP then performs a second lookup for the advertising router in the Tunnel Table Manager (TTM). This lookup returns the best RSVP LSP to use to forward packets for an LDP FEC learned through the targeted LDP session. The lookup returns the LSP with the lowest metric. If multiple LSPs have the same metric, then the result of the lookup will be to select the first one available in the TTM.

Default 1

Parameters *metric* — Specifies the metric for this LSP which is used to select an LSP among a set of LSPs which are destined to the same egress router.

Values 1 — 65535

to

Syntax **to** *ip-address*

Context config>router>mpls>lsp

Description This command specifies the system IP address of the egress router for the LSP. This command is mandatory to create an LSP.

An IP address for which a route does not exist is allowed in the configuration. If the LSP signaling fails because the destination is not reachable, an error is logged and the LSP operational status is set to down.

The **to** *ip-address* ***must*** be the system IP address of the egress router. If the **to** address does not match the SDP address, the LSP is not included in the SDP definition.

Default No default

Parameters *ip-address* — The system IP address of the egress router.

vprn-auto-bind

Syntax **vprn-auto-bind** [**include** | **exclude**]

Context config>router>mpls>lsp

Description This command determines whether the associated names LSP can be used or no as part of the auto-bind feature for VPRN services. By default a names LSP is available for inclusion to used for the auto-bind feature.

By configuring the command vprn-auto-bind exclude, the associated LSP will not be used by the auto-bind feature within VPRN services.

The **no** form of the command resets the flag backto the default value.

Default include

Parameters **include —** Allows an associated LSPto be used by auto-bin for vprn services

exclude — Disables the use of the associated LSP to be used with the auto-bind feature for VPRN services.

retry-limit

Syntax **retry-limit** *number*
no retry-limit

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This optional command specifies the number of attempts software should make to re-establish the LSP after it has failed LSP. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made and the LSP path is put into the **shutdown** state.

Use the config router **mpls lsp** *lsp-name* **no shutdown** command to bring up the path after the retry-limit is exceeded.

For P2MP LSP, all S2Ls must attempt to retry-limit before client application must be informed of failure.

The **no** form of this command revert the parameter to the default value.

Default 0 (no limit, retries forever)

Parameters *number* — The number of times software will attempt to re-establish the LSP after it has failed. Allowed values are integers in the range of 0 to 10000 where 0 indicates to retry forever.

Values 0 — 10000

retry-timer

Syntax **retry-timer** *seconds*
no retry-timer

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This command configures the time, in seconds, for LSP re-establishment attempts after it has failed.

For P2MP LSP, all S2Ls must attempt to retry-limit before client application must be informed of failure.

The **no** form of this command reverts to the default value.

Default **30**

Parameters *seconds* — The amount of time, in seconds, between attempts to re-establish the LSP after it has failed. Allowed values are integers in the range of 1 to 600.

Values 1 — 600

rsvp-resv-style

Syntax **rsvp-resv-style** [*se* | *ff*]

Context config>router>mpls>lsp

Description This command specifies the RSVP reservation style, shared explicit (se) or fixed filter (ff). A reservation style is a set of control options that specify a number of supported parameters. The style information is part of the LSP configuration.

Default **se**

Parameters *ff* — Fixed filter is single reservation with an explicit scope. This reservation style specifies an explicit list of senders and a distinct reservation for each of them. A specific reservation request is created for data packets from a particular sender. The reservation scope is determined by an explicit list of senders.

se — Shared explicit is shared reservation with a limited scope. This reservation style specifies a shared reservation environment with an explicit reservation scope. This reservation style creates a single reservation over a link that is shared by an explicit list of senders. Because each sender is explicitly listed in the RESV message, different labels can be assigned to different sender-receiver pairs, thereby creating separate LSPs.

shutdown

Syntax [**no**] **shutdown**

Context config>router>mpls>lsp
config>router>mpls>lsp-template

Description This command disables the existing LSP including the primary and any standby secondary paths.

To shutdown only the primary enter the **config router mpls lsp** *lsp-name* **primary** *path-name* **shutdown** command.

To shutdown a specific standby secondary enter the **config router mpls lsp** *lsp-name* **secondary** *path-name* **shutdown** command. The existing configuration of the LSP is preserved.

Use the **no** form of this command to restart the LSP. LSPs are created in a shutdown state. Use this command to administratively bring up the LSP.

Default **shutdown**

lsp-template

Syntax **[no] lsp-template** *lsp-template-name* **p2mp-lsp**

Context config>router>mpls>

Description This command creates a template construct that can be referenced by client application where dynamic LSP creation is required. ‘p2mp-lsp’ keyword is mandatory to be consistent with LSP structure and future P2P support.

The **no** form of command should delete LSP template. LSP template must not be allowed to be deleted if a client application is using it.

Default none

Parameters *lsp-template-name* — Name to identify LSP template. Any LSP template name and LSP name must not be same.

lsp-name-rule

Syntax **[no] lsp-name-rule {suffix-client-id | suffix-mpls-id}**

Context config>router>mpls>lsp-template

Description This command is used to select the criteria used for naming an LSP. LSP template must be shutdown to modify this option.

The **no** form of command should set the lsp-name-rule to the default value i.e. suffix-client-id.

Default **suffix-client-id**

Parameters **{suffix-client-id | suffix-mpls-id}**

default-path

Syntax **[no] default-path** *path-name*

Context config>router>mpls>lsp-template

Description This command creates a default path binding that must be applied while using TE constraints. A default path binding must be provided before LSP template can be used for signaling LSP. LSP template must be shutdown to modify default-path binding. Open issue: Default TE parameters - include and exclude must be moved under default-path.

The **no** form of command should delete path binding.

Default **none**

Parameters *path-name*

Primary and Secondary Path Commands

primary

Syntax **primary** *path-name*
no primary

Context config>router>mpls>lsp

Description This command specifies a preferred path for the LSP. This command is optional only if the **secondary** *path-name* is included in the LSP definition. Only one primary path can be defined for an LSP.

Some of the attributes of the LSP such as the bandwidth, and hop-limit can be optionally specified as the attributes of the primary path. The attributes specified in the **primary path** *path-name* command, override the LSP attributes.

The **no** form of this command deletes the association of this *path-name* from the LSP *lsp-name*. All configurations specific to this primary path, such as record, bandwidth, and hop limit, are deleted. The primary path must be shutdown first in order to delete it. The **no primary** command will not result in any action except a warning message on the console indicating that the primary path is administratively up.

Default none

Parameters *path-name* — The case-sensitive alphanumeric name label for the LSP path up to 32 characters in length.

secondary

Syntax [**no**] **secondary** *path-name*

Context config>router>mpls>lsp

Description This command specifies an alternative path that the LSP uses if the primary path is not available. This command is optional and is not required if the **config router mpls lsp** *lsp-name* **primary** *path-name* command is specified. After the switch over from the primary to the secondary, the software continuously tries to revert to the primary path. The switch back to the primary path is based on the **retry-timer** interval.

Up to eight secondary paths can be specified. All the secondary paths are considered equal and the first available path is used. The software will not switch back among secondary paths.

Software starts the signaling of all non-standby secondary paths at the same time. Retry counters are maintained for each unsuccessful attempt. Once the retry limit is reached on a path, software will not attempt to signal the path and administratively shuts down the path. The first successfully established path is made the active path for the LSP.

The **no** form of this command removes the association between this *path-name* and *lsp-name*. All specific configurations for this association are deleted. The secondary path must be shutdown first in order to delete it. The **no secondary** *path-name* command will not result in any action except a warning message on the console indicating that the secondary path is administratively up.

Default none

Parameters *path-name* — The case-sensitive alphanumeric name label for the LSP path up to 32 characters in length.

adaptive

Syntax [**no**] **adaptive**

Context config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This command enables the make-before-break functionality for an LSP or a primary or secondary LSP path. When enabled for the LSP, make-before-break will be performed for primary path and all the secondary paths of the LSP.

Default adaptive

backup-class-type

Syntax **backup-class-type ct-number**
no backup-class-type

Context config>router>mpls>lsp>primary

Description This command enables the use of the Diff-Serv backup Class-Type (CT), instead of the Diff-Serv main CT, to signal the LSP primary path when it fails and goes into retry. The Diff-Serv main CT is configured at the LSP level or at the primary path level using the following commands:

config>router>mpls>lsp>class-type *ct-number*

config>router>mpls>lsp>primary>class-type *ct-number*

When a LSP primary path retries due a failure, for example, it fails after being in the UP state, or undergoes any type of Make-Before-Break (MBB), MPLS will retry a new path for the LSP using the main CT. If the first attempt failed, the head-end node performs subsequent retries using the backup CT. This procedure must be followed regardless if the currently used CT by this path is the main or backup CT. This applies to both CSPF and non-CSPF LSPs.

The triggers for using the backup CT after the first retry attempt are:

1. A local interface failure or a control plane failure (hello timeout etc.).
2. Receipt of a PathErr message with a notification of a FRR protection becoming active downstream and/or Receipt of a Resv message with a 'Local-Protection-In-Use' flag set. This invokes the FRR Global Revertive MBB.
3. Receipt of a PathErr message with error code=25 ("Notify") and sub-code=7 ("Local link maintenance required") or a sub-code=8 ("Local node maintenance required"). This invokes the TE Graceful Shutdown MBB.

4. Receipt of a Resv refresh message with the ‘Preemption pending’ flag set or a PathErr message with error code=34 ("Reroute") and a value=1 ("Reroute request soft preemption"). This invokes the soft preemption MBB.
5. Receipt of a ResvTear message.
6. A configuration change MBB.
7. The user executing the clear>router>mpls>lsp command.

When an unmapped LSP primary path goes into retry, it uses the main CT until the number of retries reaches the value of the new **main-ct-retry-limit** parameter. If the path did not come up, it must start using the backup CT at that point in time. By default, this parameter is set to infinite value. The new main-ct-retry-limit parameter has no effect on an LSP primary path which retries due to a failure event.

An unmapped LSP primary path is a path which has never received a Resv in response to the first Path message sent. This can occur when performing a ‘shut/no-shut’ on the LSP or LSP primary path or when the node reboots. An unmapped LSP primary path goes into retry if the retry timer expired or the head-end node received a PathErr message before the retry timer expired.

When the re-signal timer expires, CSPF will try to find a path with the main CT. The head-end node must re-signal the LSP even if the new path found by CSPF is identical to the existing one since the idea is to restore the main CT for the primary path. A path with main CT is not found, the LSP remains on its current primary path using the backup CT.

When the user performs a manual re-signal of the primary path, CSPF will try to find a path with the main CT. The head-end node must re-signal the LSP as in current implementation.

The **no** form of this command disables the use of the Diff-Serv backup CT.

Default no backup-class-type

Parameters *ct-number* — The Diff-Serv Class Type number. One or more system forwarding classes can be mapped to a CT.

Values 0-7, integer

bandwidth

Syntax **bandwidth** *rate-in-mbps*
no bandwidth

Context config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary
config>router>mpls>lsp-template>fast-reroute

Description This command specifies the amount of bandwidth to be reserved for the LSP path.

The **no** form of this command resets bandwidth parameters (no bandwidth is reserved).

Default **no bandwidth** (bandwidth setting in the global LSP configuration)

Parameters *rate-in-mbps* — The amount of bandwidth reserved for the LSP path in Mbps. Allowed values are integers in the range of 1 to 100000.

Values 0 — 100000

exclude

Syntax [**no**] **exclude** *group-name* [*group-name*...(up to 5 max)]

Context config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This command specifies the admin groups to be excluded when an LSP is set up. . Up to 5 groups per operation can be specified, up to 32 maximum. The admin groups are defined in the **config>router>mpls>admin-group** context.

Use the **no** form of the command to remove the exclude command.

Default no exclude

Parameters *group-name* — Specifies the existing group-name to be excluded when an LSP is set up.

hop-limit

Syntax **hop-limit** *number*
no hop-limit

Context config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This optional command overrides the **config router mpls lsp** *lsp-name* **hop-limit** command. This command specifies the total number of hops that an LSP traverses, including the ingress and egress routers.

This value can be changed dynamically for an LSP that is already set up with the following implications:

If the new value is less than the current hops of the established LSP, the LSP is brought down. MPLS then tries to re-establish the LSP within the new hop-limit number. If the new value is equal or more than the current hops of the established LSP then the LSP will be unaffected.

The **no** form of this command reverts the values defined under the LSP definition using the **config router mpls lsp** *lsp-name* **hop-limit** command.

Default **no hop-limit**

Parameters *number* — The number of hops the LSP can traverse, expressed as an integer.

Values 2 — 255

record

Syntax [**no**] **record**

Context config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This command enables recording of all the hops that an LSP path traverses. Enabling **record** increases the size of the PATH and RESV refresh messages for the LSP since this information is carried end-to-end along the path of the LSP. The increase in control traffic per LSP may impact scalability.

The **no** form of this command disables the recording of all the hops for the given LSP. There are no restrictions as to when the **no** command can be used. The **no** form of this command also disables the **record-label** command.

Default **record**

record-label

Syntax [**no**] **record-label**

Context config>router>mpls>lsp>primary
config>router>mpls>lsp>secondary

Description This command enables recording of all the labels at each node that an LSP path traverses. Enabling the **record-label** command will also enable the **record** command if it is not already enabled.

The **no** form of this command disables the recording of the hops that an LSP path traverses.

Default **record-label**

srlg

Syntax [**no**] **srlg**

Context config>router>mpls>lsp>secondary

Description This command enables the use of the SRLG constraint in the computation of a secondary path for an LSP at the head-end LER.

When this feature is enabled, CSPF includes the SRLG constraint in the computation of the secondary LSP path. This requires that the primary LSP already be established and is up since the head-end LER needs the most current ERO computed by CSPF for the primary path. CSPF would return the list of SRLG groups along with the ERO during primary path CSPF computation. At a subsequent establishment of a secondary path with the SRLG constraint, the MPLS/RSVP task will query again CSPF providing the list of SLRG group numbers to be avoided. CSPF prunes all links with interfaces which belong to the same SRLGs as the interfaces included in the ERO of the primary path. If CSPF finds a path, the secondary is setup. If not, MPLS/RSVP will keep retrying the requests to CSPF.

If CSPF is not enabled on the LSP name, then a secondary path of that LSP which has the SRLG constraint included will be shut down and a specific failure code will indicate the exact reason for the failure in **show>router>mpls>lsp>path>detail** output.

At initial primary LSP path establishment, if primary does not come up or primary is not configured, SRLG secondary will not be signaled and will put to down state. A specific failure code will indicate the exact reason for the failure in **show>router>mpls>lsp>path>detail** output. However, if a non-SRLG secondary path was configured, such as a secondary path with the SRLG option disabled, MPLS/RSVP task will signal it and the LSP use it.

As soon as the primary path is configured and successfully established, MPLS/RSVP moves the LSP to the primary and signals all SRLG secondary paths.

Any time the primary path is re-optimized, has undergone MBB, or has come back up after being down, MPLS/RSVP task checks with CSPF if the SRLG secondary should be re-signaled. If MPLS/RSVP finds that current secondary path is no longer SRLG disjoint, for example, it became ineligible, it puts it on a delayed MBB immediately after the expiry of the retry timer. If MBB fails at the first try, the secondary path is torn down and the path is put on retry.

At the next opportunity the primary goes down, the LSP will use the path of an eligible SRLG secondary if it is UP. If all secondary eligible SLRG paths are Down, MPLS/RSVP will use a non SRLG secondary if configured and UP. If while the LSP is using a non SRLG secondary, an eligible SRLG secondary came back up, MPLS/RSVP will not switch the path of the LSP to it. As soon as primary is re-signaled and comes up with a new SLRG list, MPLS/RSVP will re-signal the secondary using the new SRLG list.

A secondary path which becomes ineligible as a result of an update to the SRLG membership list of the primary path will have the ineligibility status removed on any of the following events:

8. A successful MBB of the standby SRLG path which makes it eligible again.
9. The standby path goes down. MPLS/RSVP puts the standby on retry at the expiry of the retry timer. If successful, it becomes eligible. If not successful after the retry-timer expired or the number of retries reached the number configured under the retry-limit parameter, it is left down.
10. The primary path goes down. In this case, the ineligible secondary path is immediately torn down and will only be re-signaled when the primary comes back up with a new SRLG list.

Once primary path of the LSP is setup and is operationally up, any subsequent changes to the SRLG group membership of an interface the primary path is using would not be considered until the next opportunity the primary path is re-signaled. The primary path may be re-signaled due to a failure or to a make-before-break operation. Make-before-break occurs as a result of a global revertive operation, a timer based or manual re-optimization of the LSP path, or an operator change to any of the path constraints.

One an SRLG secondary path is setup and is operationally UP, any subsequent changes to the SRLG group membership of an interface the secondary path is using would not be considered until the next opportunity secondary path is re-signaled. The secondary path is re-signaled due to a failure, to a re-signaling of the primary path, or to a make before break operation. Make-before break occurs as a result of a timer based or manual re-optimization of the secondary path, or an operator change to any of the path constraints of the secondary path, including enabling or disabling the SRLG constraint itself.

Also, the user-configured include/exclude admin group statements for this secondary path are also checked together with the SRLG constraints by CSPF

The **no** form of the command reverts to the default value.

Default no srlg

standby

Syntax [**no**] **standby**

Context config>router>mpls>lsp>secondary

Description The secondary path LSP is normally signaled once the primary path LSP fails. The **standby** keyword ensures that the secondary path LSP is signaled and maintained indefinitely in a hot-standby state. When the primary path is re-established then the traffic is switched back to the primary path LSP.

The **no** form of this command specifies that the secondary LSP is signaled when the primary path LSP fails.

Default none

path-preference

Syntax [**no**] **path-preference** *value*

Context config>router>mpls>lsp>secondary

Description This command enables use of path preference among configured standby secondary paths per LSP. If all standby secondary paths have a default path-preference value then a non-standby secondary path will remain the active path while a standby secondary is available. A standby secondary path configured with highest priority (lowest path-preference value) must be made the active path when the primary is not in use. Path preference can be configured on standby secondary path.

The **no** form of this command resets the path-preference to the default value.

Default 255

Parameters *value* — Specifies an alternate path for the LSP if the primary path is not available,

1–255

LSP Path Commands

hop

Syntax **hop** *hop-index ip-address* {**strict | loose**}
no hop *hop-index*

Context config>router>mpls>path

Description This command specifies the IP address of the hops that the LSP should traverse on its way to the egress router. The IP address can be the interface IP address or the system IP address. If the system IP address is specified then the LSP can choose the best available interface.

Optionally, the LSP ingress and egress IP address can be included as the first and the last hop. A hop list can include the ingress interface IP address, the system IP address, and the egress IP address of any of the hops being specified.

The **no** form of this command deletes hop list entries for the path. All the LSPs currently using this path are affected. Additionally, all services actively using these LSPs are affected. The path must be shutdown first in order to delete the hop from the hop list. The **no hop** *hop-index* command will not result in any action except a warning message on the console indicating that the path is administratively up.

Default none

Parameters *hop-index* — The hop index is used to order the hops specified. The LSP always traverses from the lowest hop index to the highest. The hop index does not need to be sequential.

Values 1 — 1024

ip-address — The system or network interface IP address of the transit router. The IP address can be the interface IP address or the system IP address. If the system IP address is specified then the LSP can choose the best available interface. A hop list can also include the ingress interface IP address, the system IP address, and the egress IP address of any of the specified hops.

loose — This keyword specifies that the route taken by the LSP from the previous hop to this hop can traverse through other routers. Multiple hop entries with the same IP address are flagged as errors. Either the **loose** *or* **strict** keyword must be specified.

strict — This keyword specifies that the LSP must take a direct path from the previous hop router to this router. No transit routers between the previous router and this router are allowed. If the IP address specified is the interface address, then that is the interface the LSP must use. If there are direct parallel links between the previous router and this router and if system IP address is specified, then any one of the available interfaces can be used by the LSP. The user must ensure that the previous router and this router have a direct link. Multiple hop entries with the same IP address are flagged as errors. Either the **loose** *or* **strict** keyword must be specified.

path

Syntax [**no**] **path** *path-name*

Context config>router>mpls

Description This command creates the path to be used for an LSP. A path can be used by multiple LSPs. A path can specify some or all hops from ingress to egress and they can be either **strict** or **loose**. A path can also be empty (no *path-name* specified) in which case the LSP is set up based on IGP (best effort) calculated shortest path to the egress router. Paths are created in a **shutdown** state. A path must be shutdown before making any changes (adding or deleting hops) to the path. When a path is shutdown, any LSP using the path becomes operationally down.

To create a strict path from the ingress to the egress router, the ingress and the egress routers must be included in the path statement.

The **no** form of this command deletes the path and all its associated configuration information. All the LSPs that are currently using this path will be affected. Additionally all the services that are actively using these LSPs will be affected. A path must be **shutdown** and unbound from all LSPs using the path before it can be deleted. The **no path** *path-name* command will not result in any action except a warning message on the console indicating that the path may be in use.

Parameters *path-name* — Specify a unique case-sensitive alphanumeric name label for the LSP path up to 32 characters in length.

shutdown

Syntax [**no**] **shutdown**

Context config>router>mpls>path

Description This command disables the existing LSPs using this path. All services using these LSPs are affected. Binding information, however, is retained in those LSPs. Paths are created in the **shutdown** state.

The **no** form of this command administratively enables the path. All LSPs, where this path is defined as primary or defined as standby secondary, are (re)established.

Default **shutdown**

Static LSP Commands

static-lsp

Syntax [**no**] **static-lsp** *lsp-name*

Context config>router>mpls

Description This command is used to configure a static LSP on the ingress router. The static LSP is a manually set up LSP where the nexthop IP address and the outgoing label (push) must be specified.

The **no** form of this command deletes this static LSP and associated information.

The LSP must be shutdown first in order to delete it. If the LSP is not shut down, the **no static-lsp** *lsp-name* command does nothing except generate a warning message on the console indicating that the LSP is administratively up.

Parameters *lsp-name* — Name that identifies the LSP.

Values Up to 32 alphanumeric characters.

push

Syntax **push** {*label* **| implicit-null-label**} **nexthop** *ip-address*
no push {*out-label* **| implicit-null-label**}

Context config>router>mpls>static-lsp

Description This command specifies the label to be pushed on the label stack and the next hop IP address for the static LSP.

The **no** form of this command removes the association of the label to push for the static LSP.

Parameters **implicit-null-label** **—** Specifies the use of the implicit label value for the push operation.

label — The label to push on the label stack. Label values 16 through 1,048,575 are defined as follows:

Label values 16 through 31 are 7750 SR reserved.
Label values 32 through 1,023 are available for static assignment.
Label values 1,024 through 2,047 are reserved for future use.
Label values 2,048 through 18,431 are statically assigned for services.
Label values 28,672 through 131,071 are dynamically assigned for both MPLS and services.
Label values 131,072 through 1,048,575 are reserved for future use.

Values 16 — 1048575

nexthop *ip-address* **—** This command specifies the IP address of the next hop towards the LSP egress router. If an ARP entry for the next hop exists, then the static LSP is marked operational. If ARP entry does not exist, software sets the operational status of the static LSP to down and continues to ARP for the configured nexthop. Software continuously tries to ARP for the configured nexthop at a fixed interval.

shutdown

Syntax [**no**] **shutdown**

Context config>router>mpls>static-lsp

Description This command is used to administratively disable the static LSP.

The **no** form of this command administratively enables the static LSP.

Default **shutdown**

to

Syntax **to** *ip-address*

Context config>router>mpls>static-lsp

Description This command specifies the system IP address of the egress router for the static LSP. When creating an LSP this command is required. For LSPs that are used as transport tunnels for services, the **to** IP address ***must*** be the system IP address. If the **to** address does not match the SDP address, the LSP is not included in the SDP definition.

Parameters *ip-address* — The system IP address of the egress router.

Default none

Point-to-Multipoint MPLS (P2MP) Commands

p2mp-id

Syntax **p2mp-id** *id*

Context config>router>mpls>lsp

Description This command configures the identifier of an RSVP P2MP LSP. An RSVP P2MP LSP is fully identified by the combination of: <P2MP ID, tunnel ID, extended tunnel ID> part of the P2MP session object, and <tunnel sender address, LSP ID> fields in the p2mp sender_template object.

The **p2mp-id** is a 32-bit identifier used in the session object that remains constant over the life of the P2MP tunnel. It is unique within the scope of the ingress LER.

The **no** form restores the default value of this parameter.

Default 0

Parameters *id* — Specifies a P2MP identifier.

Values 0 — 65535

primary-p2mp-instance

Syntax [**no**] **primary-p2mp-instance** *instance-name*

Context config>router>mpls>lsp

Description This command creates the primary instance of a P2MP LSP. The primary instance of a P2MP LSP is modeled as a set of root-to-leaf (S2L) sub-LSP's. The root, for example a head-end node triggers signaling using one path message per S2L path. The leaf sub-LSP paths are merged at branching points.

Default none

Parameters *instance-name* — Specifies a name that identifies the P2MP LSP instance. The instance name can be up to 32 characters long and must be unique.

s2l-path

Syntax [**no**] **s2l-path** *path-name* **to** *ip-address*

Context config>router>mpls>lsp>primary-inst

Description This command creates a root-to-leaf (S2L) sub-LSP path for the primary instance of a P2MP LSP. The primary instance of a P2MP LSP is modeled as a set of root-to-leaf (S2L) sub-LSPs. The root, for example, head-end node, triggers signaling using one path message per S2L path. The leaf sub-LSP paths are merged at branching points.

Each S2L sub-LSP is signaled in a separate path message. Each leaf node will respond with its own RESV message. A branch LSR node will forward the path message of each S2L sub-LSP to the downstream LSR without replicating it. It will also forward the RESV message of each S2L sub-LSP to the upstream LSR without merging it with the RESV messages of other S2L sub-LSPs of the same P2MP LSP. The same is done for subsequent refreshes of the path and RESV states.

The S2L paths can be empty paths or can specify a list of explicit hops. The path name must exist and must have been defined using the **config>router>mpls>path** command. The same path name can be re-used by more than one S2L of the primary P2MP instance. However, the **to** keyword must have a unique argument per S2L as it corresponds to the address of the egress LER node.

Default none

Parameters *path-name* — Specifies the name of the path which consists of up to 32 alphanumeric characters.

to *ip-address* **—** Specifies the system IP address of the egress router.

p2mp-resignal-timer

Syntax **p2mp-resignal-timer** *minutes*
no p2mp-resignal-timer

Context config>router>mpls

Description This command configures the re-signal timer for a P2MP LSP instance. MPLS will request CSPF to re-compute the whole set of S2L paths of a given active P2MP instance each time the P2MP re-signal timer expires. The P2MP re-signal timer is configured separately from the P2P LSP parameter. MPLS performs a global MBB and moves each S2L sub-LSP in the instance into its new path using a new P2MP LSP ID if the global MBB is successful, regardless of the cost of the new S2L path.

The **no** form of this command disables the timer-based re-signaling of P2MP LSPs on this system.

Parameters *minutes* — Specifies the time MPLS waits before attempting to re-signal the P2MP LSP instance.

Values 60 — 10080

RSVP Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context config>router>rsvp
config>router>rsvp>interface

Description This command disables the RSVP protocol instance or the RSVP-related functions for the interface. The RSVP configuration information associated with this interface is retained. When RSVP is administratively disabled, all the RSVP sessions are torn down. The existing configuration is retained.

The **no** form of this command administratively enables RSVP on the interface.

Default **shutdown**

RSVP Commands

rsvp

Syntax [**no**] **rsvp**

Context config>router

Description This command enables the context to configure RSVP protocol parameters. RSVP is not enabled by default and must be explicitely enabled (**no shutdown**).

RSVP is used to set up LSPs. RSVP should be enabled on all router interfaces that participate in signaled LSPs.

The **no** form of this command deletes this RSVP protocol instance and removes all configuration parameters for this RSVP instance. To suspend the execution and maintain the existing configuration, use the **shutdown** command. RSVP must be shutdown before the RSVP instance can be deleted. If RSVP is not shutdown, the **no rsvp** command does nothing except issue a warning message on the console indicating that RSVP is still administratively enabled.

Default no shutdown

diffserv-te

Syntax **diffserv-te** [**mam | rdm**]
no diffserv-te

Context config>router>rsvp

Description This command enabled Diff-Serv Traffic Engineering on the node.

When this command is enabled, IS-IS and OSPF will start advertising available bandwidth for each TE class configured under the diffserv-te node. This command will only have effect if the operator has already enabled traffic engineering at the IS-IS and/or OSPF routing protocol levels:

config>router>isis>traffic-engineering

and/or:

config>router>ospf>traffic-engineering

IGP will advertize for each RSVP interface in the system the available bandwidth in each TE class in the unreserved bandwidth TE parameter for that class. In addition, IGP will continue to advertize the existing Maximum Reservable Link Bandwidth TE parameter to mean the maximum bandwidth that can be booked on a given interface by all classes. The value advertized is adjusted with the link **subscription** *percentage* factor configured in the **config>router>rsvp>interface** context.

The user configures the following parameters for the operation of Diff-Serv:

- Definition of TE classes, TE Class = {Class Type (CT), LSP priority}.
- Mapping of the system forwarding classes to the Diff-Serv Class Type (CT).

- Configuration of the percentage of RSVP interface bandwidth each CT shares, i.e., the Bandwidth Constraint (BC).

When Diff-Serv TE is enabled, the system will automatically enable the Max Allocation Model (MAM) Admission Control Policy. MAM represents the bandwidth constraint model for the admission control of an LSP reservation to a link. This is the only Admission Control Policy supported in this release.

Each CT shares a percentage of the Maximum Reservable Link Bandwidth via the user configured Bandwidth Constraint (BC) for this CT. The Maximum Reservable Link Bandwidth is the link bandwidth multiplied by the RSVP interface subscription factor.

The sum of all BC values across all CTs will not exceed the Maximum Reservable Link Bandwidth. In other words, the following rule is enforced:

SUM (BCc) =< Max-Reservable-Bandwidth, 0 <= c <= 7

An LSP of class-type CTc, setup priority p, holding priority h (h=<p), and bandwidth B is admitted into a link if the following condition is satisfied:

B <= Unreserved Bandwidth for TE-Class[i]

where TE-Class [i] maps to < CTc , p > in the definition of the TE classes on the node. The bandwidth reservation is effected at the holding priority, i.e., in TE-class [j] = <CTc, h>. Thus, the reserved bandwidth for CTc and the unreserved bandwidth for the TE classes using CTc are updated as follows:

Reserved(CTc) = Reserved(CTc) + B

Unreserved TE-Class [j] = BCc - SUM (Reserved(CTc,q)) for 0<= q <= h

Unreserved TE-Class [i] = BCc - SUM (Reserved(CTc,q)) for 0<= q <= p

The same is done to update the unreserved bandwidth for any other TE class making use of the same CTc. These new values are advertised to the rest of the network at the next IGP-TE flooding.

The Russian Doll Model (RDM) LSP admission control policy allows bandwidth sharing across Class Types. It provides a hierarchical model by which the reserved bandwidth of a CT is the sum of the reserved bandwidths of the numerically equal and higher CTs.

The RDM model is defined using the following equations:

SUM (Reserved (CTc)) <= BCb,

where the SUM is across all values of c in the range b <= c <= (MaxCT - 1), and BCb is the bandwidth constraint of CTb.

BC0= Max-Reservable-Bandwidth, so that

SUM (Reserved(CTc)) <= Max-Reservable-Bandwidth,

where the SUM is across all values of c in the range 0 <= c <= (MaxCT - 1).

When Diff-Serv is disabled on the node, this model degenerates into a single default CT internally with eight pre-emption priorities and a non-configurable BC equal to the Maximum Reservable Link Bandwidth. This would behave exactly like CT0 with eight pre-emption priorities and BC= Maximum Reservable Link Bandwidth if Diff-Serv was enabled.

The enabling or disabling of Diff-Serv TE on the system requires the RSVP and MPLS protocol be shutdown.

The **no** form of this command reverts to the default value.

Default no diffserv-te

Parameters **mam** — Defines the default admission control policy for Diff-Serv LSPs.

rdm — Defines Russian doll model for the admission control policy of Diff-Serv LSPs.

class-type-bw

Syntax **class-type-bw ct0** *%-link-bandwidth* **ct1***%-link-bandwidth* **ct2***%-link-bandwidth* **ct3***%-link-bandwidth* **ct4***%-link-bandwidth* **ct5***%-link-bandwidth* **ct6***%-link-bandwidth* **ct7***%-link-band-width*
no class-type-bw

Context config>router>rsvp>diffserv-te
config>router>rsvp>interface

Description This command configures the percentage of RSVP interface bandwidth each CT shares, for example, the Bandwidth Constraint (BC).

The absolute value of the CT share of the interface bandwidth is derived as the percentage of the bandwidth advertised by IGP in the Maximum Reservable Link Bandwidth TE parameter, for example, the link bandwidth multiplied by the RSVP interface **subscription** *percentage* parameter.

Note this configuration also exists at RSVP interface level and the interface specific configured value overrides the global configured value. The BC value can be changed at any time.

The RSVP interface **subscription** *percentage* parameter is configured in the **config>router>rsvp>interface** context.

The operator can specify the Bandwidth Constraint (BC) for a CT which is not used in any of the TE class definition but that does not get used by any LSP originating or transiting this node.

When Diff-Serv is disabled on the node, this model degenerates into a single default CT internally with eight pre-emption priorities and a non configurable BC equal to the Maximum Reservable Link Bandwidth. This would behave exactly like CT0 with eight pre-emption priorities and BC= Maximum Reservable Link Bandwidth if Diff-Serv was enabled.

The **no** form of this command reverts to the default value.

Parameters **ct0** (**ct1**/**ct2**/ — **ct7**) % *link-bandwidth* — The Diff-Serv Class Type number. One or more system forwading classes can be mapped to a CT.

Values 0 — 100 %

Default 0

fc

Syntax **fc** *fc-name* **class-type** *ct-number*
no fc fc-name

Context config>router>rsvp>diffserv-te

Description This command maps one or more system forwarding classes to a Diff-Serv Class Type (CT).

The default mapping is shown in the following table.

FC ID	FC Name	FC Designation	Class Type (CT)
7	Network Control	NC	7
6	High-1	H1	6
5	Expedited	EF	5
4	High-2	H2	4
3	Low-1	L1	3
2	Assured	AF	2
1	Low-2	L2	1
0	Best Effort	BE	0

The **no** form of this command reverts to the default mapping for the forwarding class name.

Parameters

class-type *ct-number* **—** The Diff-Serv Class Type number. One or more system forwading classes can be mapped to a CT.

Values 0 — 7

te-class

Syntax

te-class *te-class-number* **class-type** *ct-number* **priority** *priority*
no te-class te-class-number

Context

config>router>rsvp>diffserv-te

Description

This command configures a traffic engineering class. A TE class is defined as:

TE Class = {Class Type (CT), LSP priority}

Eight TE classes are supported. There is no default TE class once Diff-Serv is enabled. The user has to explicitly define each TE class.

When when Diff-Serv is disabled there will be an internal use of the default CT (CT0) and eight pre-emption priorities as shown in the following table.

Class Type (CT internal)	LSP Priority
0	7
0	6
0	5

Class Type (CT internal)	LSP Priority	(Continued)
0	4	
0	3	
0	2	
0	1	
0	0	

The **no** form of this command deletes the TE class.

Parameters **te-class** *te-class-number* **—** The traffic engineering class number.

Values 0 — 7

class-type *ct-number* **—** The Diff-Serv Class Type number. One or more system forwading classes can be mapped to a CT.

Values 0 — 7

priority *priority* **—** The LSP priority.

Values 0 — 7

graceful-shutdown

Syntax [**no**] **graceful-shutdown**

Context config>router>rsvp
config>router>rsvp>interface

Description This command initiates a graceful shutdown of the specified RSVP interface or all RSVP interfaces on the node if applied at the RSVP level. These are referred to as maintenance interface and maintenance node, respectively.

To initiate a graceful shutdown the maintenance node generates a PathErr message with a specific error sub-code of Local Maintenance on TE Link required for each LSP that is exiting the maintenance interface.

The node performs a single make-before-break attempt for all adaptive CSPF LSPs it originates and LSP paths using the maintenance interfaces. If an alternative path for an affected LSP is not found, then the LSP is maintained on its current path. The maintenance node also tears down and re-signals any detour LSP path using listed maintenance interfaces as soon as they are not active.

The maintenance node floods an IGP TE LSA/LSP containing Link TLV for the links under graceful shutdown with Traffic Engineering metric set to 0xffffffff and Unreserved Bandwidth parameter set to zero (0).

A head-end LER node, upon receipt of the PathErr message performs a single make-before-break attempt on the affected adaptive CSPF LSP. If an alternative path is not found, then the LSP is maintained on its current path.

A node does not take any action on the paths of the following originating LSPs after receiving the PathErr message:

a. An adaptive CSPF LSP for which the PathErr indicates a node address in the address list and the node corresponds to the destination of the LSP. In this case, there are no alternative paths which can be found.

b. An adaptive CSPF LSP whose path has explicit hops defined using the listed maintenance interface(s)/node(s).

c. A CSPF LSP with the adaptive option disabled and which current path is over the listed maintenance interfaces in the PathErr message. These are not subject to make-before-break.

d. A non CSPF LSP which current path is over the listed maintenance interfaces in the PathErr message.

The head-end LER node upon receipt of the updates IPG TE LSA/LSP for the maintenance interfaces updates the TE database. This information will be used at the next scheduled CSPF computation for any LSP which path may traverse any of the maintenance interfaces.

The **no** form of the command disables the graceful shutdown operation at the RSVP interface level or at the RSVP level. The configured TE parameters of the maintenance links are restored and the maintenance node floods the links.

Default none

implicit-null-label

Syntax [**no**] **implicit-null-label**
implicit-null-label

Context config>router>rsvp

Description This command enables the use of the implicit null label.

Signalling the IMPLICIT NULL label value for all RSVP LSPs can be enabled for which this node is the egress LER. RSVP must be shutdown before being able to change this configuration option.

The egress LER does not signal the implicit null label value on P2MP RSVP LSPs. However, the Penultimate Hop Popping (PHP) node can honor a resv message with the label value set to the implicit null.

The **no** form of this command disables the signaling of the implicit null label.

Default no implicit-null-label

keep-multiplier

Syntax [**no**] **keep-multiplier** *number*
no keep-multiplier

Context config>router>rsvp

Description The **keep-multiplier** *number* is an integer used by RSVP to declare that a reservation is down or the neighbor is down.

The **no** form of this command reverts to the default value.

Default 3

Parameters *number* — The **keep-multiplier** value.

Values 1 — 255

refresh-reduction-over-bypass

Syntax **refresh-reduction-over-bypass** [**enable** | **disable**]

Context config>router>rsvp

Description This command enables the refresh reduction capabilities over all bypass tunnels originating on this 7750 PLR node or terminating on this 7750 Merge Point (MP) node.

By default, this is disabled. Since a bypass tunnel may merge with the primary LSP path in a node downstream of the next-hop, there is no direct interface between the PLR and the MP node and it is possible the latter will not accept summary refresh messages received over the bypass.

When disabled, the node as a PLR or MP will not set the "Refresh-Reduction-Capable" bit on RSVP messages pertaining to LSP paths tunneled over the bypass. It will also not send Message-ID in RSVP messages. This effectively disables summary refresh.

Default disable

rapid-retransmit-time

Syntax **rapid-retransmit-time** *hundred-milliseconds*
no rapid-retransmit-time

Context config>router>rsvp

Description This command defines the value of the Rapid Retransmission Interval. It is used in the re-transmission mechanism to handle unacknowledged message_id objects and is based on an exponential back-off timer.

Re-transmission interval of a RSVP message with the same message_id = 2 * rapid-retransmit-time interval of time.

The node stops re-transmission of unacknowledged RSVP messages:

- If the updated back-off interval exceeds the value of the regular refresh interval.

- If the number of re-transmissions reaches the value of the **rapid-retry-limit** parameter, whichever comes first.

The Rapid Retransmission Interval must be smaller than the regular refresh interval configured in **config>router>rsvp>refresh-time**.

The **no** form of this command reverts to the default value.

Default 5

Parameters *hundred-milliseconds* — Specifies the rapid retransmission interval.

Values 1 – 100, in units of 100 msec.

rapid-retry-limit

Syntax **rapid-retry-limit** *number*
no rapid-retry-limit

Context config>router>rsvp

Description This command is used to define the value of the Rapid Retry Limit. This is used in the retransmission mechanism based on an exponential backoff timer in order to handle unacknowledged message_id objects. The RSVP message with the same message_id is retransmitted every 2 * rapid-retransmit-time interval of time. The node will stop retransmission of unacknowledged RSVP messages whenever the updated backoff interval exceeds the value of the regular refresh interval or the number of retransmissions reaches the value of the rapid-retry-limit parameter, whichever comes first.

The **no** form of this command reverts to the default value.

Default 3

Parameters *number* — Specifies the value of the Rapid Retry Limit.

Values 1 – 6, integer values

refresh-time

Syntax **refresh-time** *seconds*
no refresh-time

Context config>router>rsvp

Description The **refresh-time** controls the interval, in seconds, between the successive Path and Resv refresh messages. RSVP declares the session down after it misses **keep-multiplier** *number* consecutive refresh messages.

The **no** form of this command reverts to the default value.

Default 30 seconds

Parameters *seconds* — The refresh time in seconds.

Values 1 — 65535

te-threshold-update

Syntax **te-threshold-update**
no te-threshold-update

Context config>router>rsvp

Description This command is used to control threshold-based IGP TE updates. The **te-threshold-update** command must enable IGP TE update based only on bandwidth reservation thresholds per interface and must block IGP TE update on bandwidth changes for each reservation. Threshold levels can be defined using the **te-up-threshold** and **te-down-threshold** commands at the global RSVP or per-interface level.

The **no** form of this command should reset te-threshold-update to the default value and disable threshold based update.

Default no te-threshold-update

on-cac-failure

Syntax **on-cac-failure**
no on-cac-failure

Context config>router>rsvp>te-threshold-update

Description This command is used to enable a CAC failure-triggered IGP update.

The **no** form of this command should reset on-cac-failure to the default value and disable the CAC failure-triggered IGP update.

Default no on-cac-failure

update-timer

Syntax **update-timer** *seconds*
no update-timer

Context config>router>rsvp>te-threshold-update

Description This command is to control timer-based IGP TE updates. Timer-based IGP updates can be enabled by specifying a non-zero time value. Default value of update-timer is 0.

The **no** form of this command should reset update-timer to the default value and disable timer-based IGP update.

Default no update-timer (time - 0 seconds)

Parameters *seconds* — The time in seconds.

Values 0-300

te-up-threshold

Syntax **te-up-threshold** *threshold-level* [*threshold-level*...(up to 16 max)]

Context config>router>rsvp
config>router>rsvp>interface

Description This command configures the specific threshold levels per node and per interface. Threshold levels are for reserved bandwidth per interface. The **te-threshold-update** command is used to enable or disable threshold-based IGP TE updates. Any reserved bandwidth change per interface is compared with all the threshold levels and trigger an IGP TE update if a defined threshold level is crossed in either direction (LSP setup or teardown). Threshold-based updates must be supported with both ISIS and OSPF. A minimum of one and a maximum of 16 threshold levels must be supported.

Threshold levels configured per node is inherited by all configured RSVP interfaces. Threshold levels defined under the RSVP interface is used to trigger IGP updates if non-default threshold levels are configured.

The **no** form of this command resets te-up-threshold to its default value.

Default 0 15 30 45 60 75 80 85 90 95 96 97 98 99 100

Parameters *threshold-level* — Integer value

Values 0 — 100

te-down-threshold

Syntax **te-down-threshold** *threshold-level* [*threshold-level*...(up to 16 max)]

Context config>router>rsvp
config>router>rsvp>interface

Description This command configures the specific threshold levels per node and per interface. Threshold levels are for reserved bandwidth per interface. The **te-threshold-update** command is used to enable or disable threshold-based IGP TE updates. Any reserved bandwidth change per interface is compared with all the threshold levels and trigger an IGP TE update if a defined threshold level is crossed in either direction (LSP setup or teardown). Threshold-based updates must be supported with both ISIS and OSPF. A minimum of one and a maximum of 16 threshold levels is supported.

Threshold levels configured per node is inherited by all configured RSVP interfaces. Threshold levels defined under the RSVP interface is used to trigger IGP updates if non-default threshold levels are configured.

The **no** form of this command resets te-down-threshold to its default value.

Default 100 99 98 97 96 95 90 85 80 75 60 45 30 15 0

Parameters *threshold-level* — Integer value

Values 0 — 100

Interface Commands

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>router>rsvp

Description This command enables RSVP protocol support on an IP interface. No RSVP commands are executed on an IP interface where RSVP is not enabled.

The **no** form of this command deletes all RSVP commands such as **hello-interval** and **subscription**, which are defined for the interface. The RSVP interface must be **shutdown** it can be deleted. If the interface is not shut down, the **no interface** *ip-int-name* command does nothing except issue a warning message on the console indicating that the interface is administratively up.

Default **shutdown**

Parameters *ip-int-name* — The name of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 1 — 32 alphanumeric characters.

authentication-key

Syntax **authentication-key** [*authentication-key* **|** *hash-key*] [**hash | hash2**]
no authentication-key

Context config>router>rsvp>interface

Description his command specifies the authentication key to be used between RSVP neighbors to authenticate RSVP messages. Authentication uses the MD-5 message-based digest.

When enabled on an RSVP interface, authentication of RSVP messages operates in both directions of the interface.

A 7750 node maintains a security association using one authentication key for each interface to a neighbor. The following items are stored in the context of this security association:

- The HMAC-MD5 authentication algorithm.
- Key used with the authentication algorithm.
- Lifetime of the key. The user-entered key is valid until the user deletes it from the interface.
- Source Address of the sending system.
- Latest sending sequence number used with this key identifier.

A 7750 RSVP sender transmits an authenticating digest of the RSVP message, computed using the shared authentication key and a keyed-hash algorithm. The message digest is included in an integrity object which also contains a flags field, a key identifier field, and a sequence number field. The

RSVP sender complies to the procedures for RSVP message generation in RFC 2747, *RSVP Cryptographic Authentication*.

A RSVP receiver uses the key together with the authentication algorithm to process received RSVP messages.

When a PLR node switches the path of the LSP to a bypass LSP, it does not send the Integrity object in the RSVP messages sent over the bypass tunnel. If the PLR receives an RSVP message with an Integrity object, it will perform the digest verification for the key of the interface over which the packet was received. If this fails, the packet is dropped. If the received RSVP message is a RESV message and does not have an Integrity object, then the PLR node will accept it only if it originated from the MP node.

A 7750 MP node will accept RSVP messages received over the bypass tunnel with and without the Integrity object. If an Integrity object is present, the proper digest verification for the key of the interface over which the packet was received is performed. If this fails, the packet is dropped.

The MD5 implementation does not support the authentication challenge procedures in RFC 2747.

The **no** form of this command disables authentication.

Default **no authentication-key** - The authentication key value is the null string.

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 16 characters in length (unencrypted). If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

hash-key — The hash key. The key can be any combination of up 33 alphanumeric characters. If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

bfd-enable

Syntax [**no**] **bfd-enable**

Context config>router>rsvp>interface

Description This command enables the use of bi-directional forwarding (BFD) to control the state of the associated RSVP interface. This causes RSVP to register the interface with the BFD session on that interface.

The user configures the BFD session parameters, such as, **transmit-interval**, **receive-interval**, and **multiplier**, under the IP interface in the **config>router> interface>bfd** context.

Note that it is possible that the BFD session on the interface was started because of a prior registration with another protocol, for example, OSPF or IS-IS.

The registration of an RSVP interface with BFD is performed at the time of neighbor gets its first session. This means when this node sends or receives a new Path message over the interface. If however the session did not come up, due to not receiving a Resv for a new path message sent after the maximum number of re-tries, the LSP is shutdown and the node de-registers with BFD. In general, the registration of RSVP with BFD is removed as soon as the last RSVP session is cleared.

The registration of an RSVP interface with BFD is performed independent of whether RSVP hello is enabled on the interface or not. However, hello timeout will clear all sessions towards the neighbor and RSVP de-registers with BFD at clearing of the last session.

Note that an RSVP session is associated with a neighbor based on the interface address the path message is sent to. If multiple interfaces exist to the same node, then each interface is treated as a separate RSVP neighbor. The user will have to enable BFD on each interface and RSVP will register with the BFD session running with each of those neighbors independently

Similarly the disabling of BFD on the interface results in removing registration of the interface with BFD.

When a BFD session transitions to DOWN state, the following actions are triggered. For RSVP signaled LSPs, this triggers activation of FRR bypass/detour backup (PLR role), global revertive (head-end role), and switchover to secondary if any (head-end role) for affected LSPs with FRR enabled. It triggers switchover to secondary if any and scheduling of re-tries for signaling the primary path of the non-FRR affected LSPs (head-end role).

The **no** form of this command removes BFD from the associated RSVP protocol adjacency.

Default no bfd-enable

hello-interval

Syntax **hello-interval** *milli-seconds*
no hello-interval

Context config>router>rsvp>interface

Description This command configures the time interval between RSVP hello messages.

RSVP hello packets are used to detect loss of RSVP connectivity with the neighboring node. Hello packets detect the loss of neighbor far quicker than it would take for the RSVP session to time out based on the refresh interval. After the loss of the of number keep-multiplier consecutive hello packets, the neighbor is declared to be in a down state.

The **no** form of this command reverts to the default value of the hello-interval. To disable sending hello messages, set the value to zero.

Default **3000** milliseconds

Parameters *milli-seconds* — Specifies the RSVP hello interval in milliseconds, in multiples of 1000. A 0 (zero) value disables the sending of RSVP hello messages.

Values 0 — 60000 milliseconds (in multiples of 1000)

implicit-null-label

Syntax **implicit-null-label** [**enable** | **disable**]
no implicit-null-label

Context config>router>rsvp>interface

Description This command enables the use of the implicit null label over a specific RSVP interface.

All LSPs for which this node is the egress LER and for which the path message is received from the previous hop node over this RSVP interface will signal the implicit null label. This means that if the egress LER is also the merge-point (MP) node, then the incoming interface for the path refresh message over the bypass dictates if the packet will use the implicit null label or not. The same for a 1-to-1 detour LSP.

The user must shutdown the RSVP interface before being able to change the implicit null configuration option.

The **no** form of this command returns the RSVP interface to use the RSVP level configuration value.

Default disable

Parameters **enable —** This parameter enables the implicit null label.

disable — This parameter disables the implicit null label.

refresh-reduction

Syntax [**no**] **refresh-reduction**

Context config>router>rsvp>interface

Description This command enables the use of the RSVP overhead refresh reduction capabilities on this RSVP interface.

When this option is enabled, a 7750 node will enable support for three capabilities. It will accept bundles RSVP messages from its peer over this interface, it will attempt to perform reliable RSVP message delivery to its peer, and will use summary refresh messages to refresh path and resv states. The reliable message delivery must be explicitly enabled by the user after refresh reduction is enabled. The other two capabilities are enabled immediately.

A bundle message is intended to reduce overall message handling load. A bundle message consists of a bundle header followed by one or more bundle sub-messages. A sub-message can be any regular RSVP message except another bundle message. A 7750 node will only process received bundled RSVP messages but will not generate them.

When reliable message delivery is supported by both the node and its peer over the RSVP interface, an RSVP message is sent with a message_id object. A message_id object can be added to any RSVP message when sent individually or as a sub-message of a bundled message.

if the sender sets the ack_desired flag in the message_id object, the receiver acknowledges the receipt of the RSVP message by piggy-backing a message_ack object to the next RSVP message it sends to its peer. Alternatively, an ACK message can also be used to send the message_ack object. In both cases, one or many message_ack objects could be included in the same message.

The 7750 supports the sending of separate ACK messages only but is capable of processing received message_ack objects piggy-backed to hop-by-hop RSVP messages, such as path and resv.

The 7750 sets the ack_desired flag only in non refresh RSVP messages and in refresh messages which contain new state information.

A retransmission mechanism based on an exponential backoff timer is supported in order to handle unacknowledged message_id objects. The RSVP message with the same message_id is retransmitted every 2 * rapid-retransmit-time interval of time. The rapid-retransmit-time is referred to as the rapid retransmission interval as it must be smaller than the regular refresh interval configured in the **config>router>rsvp>refresh-time** context. There is also a maximum number of retransmissions of an unacknowledged RSVP message rapid-retry-limit. The node will stop retransmission of unacknowledged RSVP messages whenever the updated backoff interval exceeds the value of the regular refresh interval or the number of retransmissions reaches the value of the rapid-retry-limit parameter, whichever comes first. These two parameters are configurable globally on a system in the **config>router>rsvp** context.

Refresh summary consists of sending a summary refresh message containing a message_id list object. The fields of this object are populated each with the value of the message_identifier field in the message_id object of a previously sent individual path or resv message. The summary refresh message is sent every refresh regular interval as configured by the user using the refresh-time command in the **config>router>rsvp** context. The receiver checks each message_id object against the saved path and resv states. If a match is found, the state is updated as if a regular path or resv refresh message was received from the peer. If a specific message_identifier field does not match, then the node sends a message_id_nack object to the originator of the message.

The above capabilities are referred to collectively as “refresh overhead reduction extensions”. When the refresh-reduction is enabled on an RSVP interface, the node indicates this to its peer by setting a “refresh-reduction-capable” bit in the flags field of the common RSVP header. If both peers of an RSVP interface set this bit, all the above three capabilities can be used. Furthermore, the node monitors the settings of this bit in received RSVP messages from the peer on the interface. As soon as this bit is cleared, the router stops sending summary refresh messages. If a peer did not set the “refresh-reduction-capable” bit, a node does not attempt to send summary refresh messages.

However, if the peer did not set the “refresh-reduction-capable” bit, a node, with refresh reduction enabled and reliable message delivery enabled, will still attempt to perform reliable message delivery with this peer. If the peer does not support the message_id object, it returns an error message “unknown object class”. In this case, the node retransmits the RSVP message without the message_id object and reverts to using this method for future messages destined to this peer.

The **no** form of the command reverts to the default value.

Default no refresh-reduction

reliable-delivery

Syntax [**no**] **reliable-delivery**

Context config>router>rsvp>interface>refresh-reduction

Description This command enables reliable delivery of RSVP messages over the RSVP interface. When refresh-reduction is enabled on an interface and reliable-delivery is disabled, then the router will send a message_id and not set ACK desired in the RSVP messages over the interface. Thus 7750 does not expect an ACK and but will accept it if received. The node will also accept message ID and reply with an ACK when requested. In this case, if the neighbor set the “refresh-reduction-capable” bit in the flags field of the common RSVP header, the node will enter summary refresh for a specific message_id it sent regardless if it received an ACK or not to this message from the neighbor.

Finally, when ‘reliable-delivery’ option is enabled on any interface, RSVP message pacing is disabled on all RSVP interfaces of the system, for example, the user cannot enable the msg-pacing option in the **config>router>rsvp** context, and error message is returned in CLI. Conversely, when the msg-pacing option is enabled, the user cannot enable the reliable delivery option on any interface on this system. An error message will also generated in CLI after such an attempt.

The **no** form of the command reverts to the default value.

Default no reliable-delivery

subscription

Syntax **subscription** *percentage*
no subscription

Context config>router>rsvp>interface

Description This command configures the percentage of the link bandwidth that RSVP can use for reservation and sets a limit for the amount of over-subscription or under-subscription allowed on the interface.

When the **subscription** is set to zero, no new sessions are permitted on this interface. If the *percentage* is exceeded, the reservation is rejected and a log message is generated.

The **no** form of this command reverts the *percentage* to the default value.

Default **100**

Parameters *percentage* — The percentage of the interface's bandwidth that RSVP allows to be used for reservations.

Values 0 — 1000

te-up-threshold

Syntax **te-up-threshold** *threshold-level* [*threshold-level*...(up to 16 max)]
no te-up-threshold

Context config>router>rsvp
config>router>rsvp>interface

Description This command configures the specific threshold levels per node and per interface. Threshold levels are for reserved bandwidth per interface. The **te-threshold-update** command is used to enable or disable threshold-based IGP TE updates. Any reserved bandwidth change per interface is compared with all the threshold levels and trigger an IGP TE update if a defined threshold level is crossed in either direction (LSP setup or teardown). Threshold-based updates must be supported with both ISIS and OSPF. A minimum of one and a maximum of 16 threshold levels must be supported.

Threshold levels configured per node is inherited by all configured RSVP interfaces. Threshold levels defined under the RSVP interface is used to trigger IGP updates if non-default threshold levels are configured.

The **no** form of this command resets the default value.

Default 0 15 30 45 60 75 80 85 90 95 96 97 98 99 100

Parameters *threshold-level* — Integer value

Values 0 — 100

te-down-threshold

Syntax **te-down-threshold** *threshold-level* [*threshold-level*...(up to 16 max)]
no te-down-threshold

Context config>router>rsvp
config>router>rsvp>interface

Description This command configures the specific threshold levels per node and per interface. Threshold levels are for reserved bandwidth per interface. The **te-threshold-update** command is used to enable or disable threshold-based IGP TE updates. Any reserved bandwidth change per interface is compared with all the threshold levels and trigger an IGP TE update if a defined threshold level is crossed in either direction (LSP setup or teardown). Threshold-based updates is supported with both ISIS and OSPF. A minimum of one and a maximum of 16 threshold levels is supported.

Threshold levels configured per node is inherited by all configured RSVP interfaces. Threshold levels defined under the RSVP interface must be used to trigger IGP updates if non-default threshold levels are configured.

The **no** form of this command resets the default value.

Default 100 99 98 97 96 95 90 85 80 75 60 45 30 15 0

Parameters *threshold-level* — Integer value

Values 0 — 100

Message Pacing Commands

msg-pacing

Syntax [**no**] **msg-pacing**

Context config>router>rsvp

Description This command enables RSVP message pacing in which the specified number of RSVP messages, specified in the **max-burst** command, are sent in a configured interval, specified in the **period** command. A count is kept of the messages that were dropped because the output queue for the interface used for message pacing was full.

Default **no msg-pacing**

max-burst

Syntax **max-burst** *number*
no max-burst

Context config>router>rsvp>msg-pacing

Description This command specifies the maximum number of RSVP messages that are sent in the specified period under normal operating conditions.

Default 650

Values 10 — 1000 in increments of 10

period

Syntax **period** *milli-seconds*
no period

Context config>router>rsvp>msg-pacing

Description This command specifies the time interval, in milliseconds, when the router can send the specified number of RSVP messages which is specified in the **max-burst** command.

Default 100

Values 10 — 1000 milliseconds in increments of 10 milliseconds

Show Commands

admin-group

Syntax **admin-group** *group-name*

Context show>router>mpls

Description This command displays MPLS administrative group information.

Parameters *group-name* — Specify a group name up to 32 characters.

Output **MPLS Administrative Group Output Fields —** The following table describes MPLS administrative group output fields.

Label	Description
Group Name	The name of the group. The name identifies the administrative group within a virtual router instance.
Group Value	The unique group value associated with the administrative group. If the value displays -1, then the group value for this entry has not been set.
No. of Groups	The total number of configured admin groups within the virtual router instance.

Sample Output

```
A:ALA-1# show router mpls admin-group
=================================================
MPLS Administrative Groups
=================================================
Group Name                          Group Value
-------------------------------------------------
green                               15
red                                 25
yellow                              20
-------------------------------------------------
No. of Groups: 3
=================================================
A:ALA-1#
```

bypass-tunnel

Syntax **bypass-tunnel** [**to** *ip-address*] [**protected-lsp** [*lsp-name*]] [**dynamic | manual | p2mp**] [**detail**]

Context show>router>mpls

Description If fast reroute is enabled on an LSP and the facility method is selected, instead of creating a separate LSP for every LSP that is to be backed up, a single LSP is created which serves as a backup for a set of LSPs. Such an LSP tunnel is called a bypass tunnel.

Parameters *ip-address* — Specify the IP address of the egress router.

lsp-name — Specify the name of the LSP protected by the bypass tunnel.

dynamic — Displays dynamically assigned labels for bypass protection.

manual — Displays manually assigned labels for bypass protection.

detail — Displays detailed information.

p2mp — Displays P2MP bypass tunnel information.

Output **MPLS Bypass Tunnel Output Fields —** The following table describes MPLS bypass tunnel output fields.

`To`	The system IP address of the egress router.
`State`	The LSP's administrative state.
`Out I/F`	Specifies the name of the network IP interface.
`Out Label`	Specifies the incoming MPLS label on which to match.
`Reserved BW (Kbps)`	Specifies the amount of bandwidth in megabits per second (Mbps) reserved for the LSP.

Sample Output

```
*A:SRU4>show>router>mpls# bypass-tunnel
===============================================================================
MPLS Bypass Tunnels
===============================================================================
Legend :  m - Manual      d - Dynamic      p - P2mp
===============================================================================
To               State  Out I/F        Out Label     Reserved   Protected  Type
                                                     BW (Kbps)  LSP Count
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
*A:SRU4>show>router>mpls#


*A:Dut-B# show router mpls bypass-tunnel detail
==============================================================================
MPLS Bypass Tunnels (Detail)
```

```
===============================================================================
bypass-link10.10.104.4
-------------------------------------------------------------------------------
To              : 10.10.101.4        State               : Up
Out I/F         : 1/1/2:1            Out Label           : 129994
Up Time         : 0d 00:02:33        Active Time         : n/a
Reserved BW     : 0 Kbps             Protected LSP Count : 1
Type            : Dynamic
SetupPriority   : 7                  Hold Priority       : 0
Class Type      : 0
Actual Hops     :
    10.10.101.2     -> 10.10.101.4
===============================================================================
*A:Dut-B#


*A:Dut-B# show router mpls bypass-tunnel detail
===============================================================================
MPLS Bypass Tunnels (Detail)
-------------------------------------------------------------------------------
bypass-link10.10.104.4
-------------------------------------------------------------------------------
To              : 10.10.101.4        State               : Up
Out I/F         : 1/1/2:1            Out Label           : 129994
Up Time         : 0d 00:02:33        Active Time         : n/a
Reserved BW     : 0 Kbps             Protected LSP Count : 1
Type            : Dynamic
SetupPriority   : 7                  Hold Priority       : 0
Class Type      : 0
Actual Hops     :
    10.10.101.2     -> 10.10.101.4
===============================================================================
*A:Dut-B#
```

interface

Syntax **interface** [*ip-int-name* **|** *ip-address*] [**label-map** *label*]
interface [*ip-int-name* **|** *ip-address*] **statistics**

Context show>router>mpls

Description This command displays MPLS interface information.

Parameters *ip-int-name* — The name of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-address — The system or network interface IP address.

label-map *label* — The MPLS label on which to match.

Values 32 — 1048575

statistics — Displays IP address and the number of packets and octets sent and received on an interface-basis.

Output **MPLS Interface Output Fields —** The following table describes MPLS interface output fields.

Label	Description
`Interface`	The interface name.
`Port-id`	The port ID displayed in the *slot/mda/port* format.
`Adm`	Specifies the administrative state of the interface.
`Opr`	Specifies the operational state of the interface.
`Te-metric`	Specifies the traffic engineering metric used on the interface.
`Srlg Groups`	Specifies the shared risk loss group (SRLG) name(s).
`Interfaces`	The total number of interfaces.
`Transmitted`	Displays the number of packets and octets transmitted from the interface.
`Received`	Displays the number of packets and octets received.
`In Label`	Specifies the ingress label.
`In I/F`	Specifies the ingress interface.
`Out Label`	Specifies the egress label.
`Out I/F`	Specifies the egress interface.
`Next Hop`	Specifies the next hop IP address for the static LSP.
`Type`	Specifies whether the label value is statically or dynamically assigned.

Sample Output

```
*A:SRU4>config>router>mpls# show router mpls interface
===============================================================================
MPLS Interfaces
===============================================================================
Interface                          Port-id          Adm    Opr    TE-metric
-------------------------------------------------------------------------------
system                             system           Up     Up     None
  Admin Groups                     None
  Srlg Groups                      None
aps-1                              aps-1            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      3410
aps-2                              aps-2            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      3420
aps-3                              aps-3            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      3430
sr4-1                              1/1/4            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      3440
ess-7-1                            3/2/4            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      45100
ess-7-2                            3/2/5            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      45110
...
g7600                              3/1/2            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      41.80
m160                               3/2/1            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      420.40
-------------------------------------------------------------------------------
Interfaces : 35
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls#  show router mpls interface "hubA"
===============================================================================
MPLS Interface : hubA
===============================================================================
Interface                          Port-id          Adm    Opr    TE-metric
-------------------------------------------------------------------------------
hubA                               3/2/8            Up     Up     None
  Admin Groups                     None
  Srlg Groups                      44.200
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:SRU4>config>router>mpls#



*A:SRU4>config>router>mpls#  show router mpls interface "hubA" label-map 203
===============================================================================
MPLS Interface : hubA (Label-Map 203)
```

```
===============================================================================
In Label  In I/F     Out Label Out I/F    Next Hop          Type      Adm  Opr
-------------------------------------------------------------------------------
203       3/2/8      403       1/1/9      11.22.10.3        Static    Up   Up
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls# show router mpls interface statistics
===============================================================================
MPLS Interface (statistics)
===============================================================================
Interface      : aps-1
  Transmitted  : Pkts - 76554                Octets - 7930285
  Received     : Pkts - 17068                Octets - 3626842

Interface      : aps-2
  Transmitted  : Pkts - 0                    Octets - 0
  Received     : Pkts - 1311                 Octets - 219888

Interface      : aps-3
  Transmitted  : Pkts - 0                    Octets - 0
  Received     : Pkts - 3                    Octets - 234

Interface      : sr4-1
  Transmitted  : Pkts - 0                    Octets - 0
  Received     : Pkts - 0                    Octets - 0

Interface      : ess-7-1
  Transmitted  : Pkts - 113537               Octets - 15058332
  Received     : Pkts - 13193                Octets - 1091492

Interface      : ess-7-2
  Transmitted  : Pkts - 166133               Octets - 22762482
  Received     : Pkts - 16672                Octets - 1368464

Interface      : ess-7-3
  Transmitted  : Pkts - 122934               Octets - 11033246
  Received     : Pkts - 12256                Octets - 1026826
...

Interface      : m160
  Transmitted  : Pkts - 17188024             Octets - 2183076528
  Received     : Pkts - 677745               Octets - 59367236
===============================================================================
*A:SRU4>config>router>mpls#
```

label

Syntax **label** *start-label* [*end-label* | *in-use* | **owner**]

Context show>router>mpls

Description Displays MPLS labels exchanged.

Parameters *start-label* — The label value assigned at the ingress router.

end-label — The label value assigned for the egress router.

in-use — The number of in-use labels displayed.

Output **MPLS Label Output Fields —** The following table describes MPLS label output fields.

Label	Description
`Label`	Displays the value of the label being displayed.
`Label Type`	Specifies whether the label value is statically or dynamically assigned.
`Label Owner`	The label owner.
`In-use labels in entire range`	The total number of labels being used by RSVP.

Sample Output

```
*A:SRU4>config>router>mpls#    show router mpls label 202
=================================================================
MPLS Label 202
=================================================================
Label               Label Type          Label Owner
-----------------------------------------------------------------
202                 static-lsp          STATIC
-----------------------------------------------------------------
In-use labels in entire range                       : 5057
=================================================================
*A:SRU4>config>router>mpls#
```

label-range

Syntax **label-range**

Context show>router>mpls

Description This command displays the MPLS label range.

Output **MPLS Label Range Output —** The following table describes the MPLS label range output fields.

Label	Description
`Label Type`	Displays the information about **static-lsp**, **static-svc**, and **dynamic** label types.
`Start Label`	The label value assigned at the ingress router.
`End Label`	The label value assigned for the egress router.
`Aging`	The number of labels released from a service which are transitioning back to the label pool. Labels are aged 15 seconds.
`Total Available`	The number of label values available.

Sample Output

```
*A:SRU4>config>router>mpls# show router mpls label-range
===============================================================================
Label Ranges
===============================================================================
Label Type      Start Label     End Label       Aging          Total Available
-------------------------------------------------------------------------------
Static-lsp      32              1023            -              736
Static-svc      2048            18431           -              16384
Dynamic         32768           131071          258            93232
===============================================================================
*A:SRU4>config>router>mpls#
```

lsp

Syntax **lsp** *lsp-name* [**status** {**up|down**}] [**from** *ip-address* **| to** *ip-address*] [**detail**]
lsp {**transit** | **terminate**} [**status** {**up** | **down**}] [**from** *ip-address* **| to** *ip-address* **| lsp-name** *name*] [**detail**]
lsp count
lsp *lsp-name* **activepath**
lsp *lsp-name* **path** [*path-name*] [**status** {**up** |**down**}] [**detail**]
lsp [*lsp-name*] **path** [*path-name*] **mbb**

Context show>router>mpls

Description This command displays LSP details.

Parameters **lsp** *lsp-name* — The name of the LSP used in the path.

status up — Displays an LSP that is operationally up.

status down — Displays an LSP that is operationally down.

from *ip-address* — Displays the IP address of the ingress router for the LSP.

to *ip-address* — Displays the IP address of the egress router for the LSP.

transit — Displays the number of static LSPs that transit through the router.

terminate — Displays the number of static LSPs that terminate at the router.

lsp *count* — Displays the total number of LSPs.

activepath — Displays the present path being used to forward traffic.

mbb — Displays make-before-break (MBB) information.

detail — Displays detailed information.

Output **MPLS LSP Output —** The following table describes MPLS LSP output fields.

Label	Description
`LSP Name`	The name of the LSP used in the path.
`To`	The system IP address of the egress router for the LSP.

Label	Description (Continued)
`Adm State`	`Down` — The path is administratively disabled.
	`Up` — The path is administratively enabled.
`Oper State`	`Down` — The path is operationally down.
	`Up` — The path is operationally up.
`Oper State`	`Down` — The path is operationally down.
	`Up` — The path is operationally up.
`LSPs`	The total number of LSPs configured.
`From`	The IP address of the ingress router for the LSP.
`LSP Up Time`	The length of time the LSP has been operational.
`Transitions`	The number of transitions that have occurred for the LSP.
`Retry Limit`	The number of attempts that the software should make to re-establish the LSP after it has failed.
`Signaling`	Specifies the signaling style.
`Hop Limit`	The maximum number of hops that an LSP can traverse, including the ingress and egress routers.
`Fast Reroute/ FastFail Config`	`enabled` — Fast reroute is enabled. In the event of a failure, traffic is immediately rerouted on the pre-computed detour LSP, thus minimizing packet loss.
	`disabled` — There is no detour LSP from each node on the primary path.
`ADSPEC`	`enabled` — The LSP will include advertising data (ADSPEC) objects in RSVP messages.
	`disabled` — The LSP will not include advertising data (ADSPEC) objects in RSVP messages.
`Primary`	The preferred path for the LSP.
`Secondary`	The alternate path that the LSP will use if the primary path is not available.
`Bandwidth`	The amount of bandwidth in megabits per second (Mbps) reserved for the LSP path.
`LSP Up Time`	The total time in increments that the LSP path has been operational.
`LSP Tunnel ID`	The value which identifies the label switched path that is signaled for this entry.
`To`	The IP address of the egress router for the LSP.

Label	Description (Continued)
LSP Down Time	The total time in increments that the LSP path has not been operational.
Path Changes	The number of path changes this LSP has had. For every path change (path down, path up, path change), a corresponding syslog/trap (if enabled) is generated.
Retry Timer	The time, in seconds, for LSP re-establishment attempts after an LSP failure.
Resv Style	`se` — Specifies a shared reservation environment with a limited reservation scope. This reservation style creates a single reservation over a link that is shared by an explicit list of senders.
	`ff` — Specifies a shared reservation environment with an explicit reservation scope. Specifies an explicit list of senders and a distinct reservation for each of them.
Negotiated MTU	The size of the maximum transmission unit (MTU) that is negotiated during establishment of the LSP.
FR Hop Limit	The total number of hops a detour LSP can take before merging back onto the main LSP path.
LastResignalAttempt	Displays the system up time when the last attempt to resignal this LSP was made.
MBB Type	Displays an enumerated integer that specifies the type of make-before-break (MBB). If none displays then there is no MBB in progress or no last MBB.
MBB State	Displays the state of the most recent invocation of the make-before-break functionality.
End at	Displays the system up time when the last MBB ended.
Old Metric	Displays the cost of the traffic engineered path for the LSP path prior to MBB.
NextRetryIn	Displays the amount of time remaining, in seconds, before the next attempt is made to retry the in-progress MBB.
RetryAttempt	Displays the number attempts for the MBB is in progress.
Failure Code	Displays the reason code for in-progress MBB failure. A value of **none** indicates that no failure has occurred.
Failure Node	Displays the IP address of the node in the LSP path at which the in-progress MBB failed. When no failure has occurred, this value is **none**.

Sample Output

```
*A:SRU4>config>router>mpls# show router mpls lsp
```

```
===============================================================================
MPLS LSPs (Originating)
===============================================================================
LSP Name                          To                  Fastfail     Adm   Opr
                                                      Config
-------------------------------------------------------------------------------
to_110_20_1_1_cspf                110.20.1.1          No           Up    Up
to_110_20_1_2_cspf                110.20.1.2          No           Up    Dwn
to_110_20_1_3_cspf                110.20.1.3          No           Up    Up
to_110_20_1_4_cspf                110.20.1.4          No           Up    Dwn
to_110_20_1_5_cspf                110.20.1.5          No           Up    Up
to_110_20_1_6_cspf                110.20.1.6          No           Up    Dwn
to_110_20_1_110_cspf              110.20.1.110        No           Up    Up
to_10_8_100_15_cspf               10.8.100.15         No           Up    Dwn
to_10_20_1_20_cspf                10.20.1.20          No           Up    Up
to_10_20_1_22_cspf                10.20.1.22          No           Up    Up
to_10_100_1_1_cspf                10.100.1.1          No           Up    Dwn
to_110_20_1_1_cspf_2              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_3              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_4              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_5              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_6              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_7              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_8              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_9              110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_10             110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_11             110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_12             110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_13             110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_14             110.20.1.1          No           Up    Up
to_110_20_1_1_cspf_15             110.20.1.1          No           Up    Up
...
-------------------------------------------------------------------------------
LSPs : 201
===============================================================================
*A:SRU4>config>router>mpls#
```

Label	Description
Autobandwidth	Enabled – Auto-bandwidth adjustment is enabled on this LSP. Disabled – Auto-bandwidth adjustment is disabled on this LSP.
Auto BW Min	The minimum bandwidth of the LSP that auto-bandwidth can request
Auto BW Max	The maximum bandwidth of the LSP that auto-bandwidth can request
AB Up Thresh	The percent threshold for increasing LSP bandwidth followed by absolute threshold in ().
AB Down Thresh	The percent threshold for decreasing LSP bandwidth followed by absolute threshold in ().
AB Adj Time	The configured adjust-count times the collection-interval.
AB Sample Time	The configured sample-count times the collection-interval.

Label	Description
AB Last Adj	The system time of the last auto-bandwidth adjustment and the cause: (M) manual (T) normal expiry of adjust-timer (O) overflow (C) VLL CAC
AB Next Adj	The system time when the adjust-timer will expire next [or the remaining adjust-count, if this is not possible].
AB Max AvgR*	The maximum average data rate in any sample interval of the current adjust interval
AB Lst AvgR*	The average data rate measured in the sample interval that ended most recently
AB Oflow Lmt	The configured value of the auto-bandwidth overflow-limit
AB Oflow Count	The number of overflow samples since the last reset
Init BW	The configured bandwidth of the primary path (and used at original establishment of the LSP)
Current BW	The current bandwidth reserved along the primary path

```
*A:SRU4>config>router>mpls#  show router mpls lsp detail
===============================================================================
MPLS LSPs (Originating) (Detail)
===============================================================================
-------------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------------
LSP Name    : to_110_20_1_1_cspf
LSP Type    : RegularLsp                       LSP Tunnel ID  : 1
From        : 110.20.1.4
Adm State   : Up                               Oper State     : Up
LSP Up Time : 0d 01:47:49                      LSP Down Time  : 0d 00:00:00
Transitions : 11                               Path Changes   : 11
Retry Limit : 0                                Retry Timer    : 30 sec
Signaling   : RSVP                             Resv. Style    : SE
Hop Limit   : 255                              Negotiated MTU : 1500
Adaptive    : Enabled                          ClassType      : 0
FastReroute : Disabled                         Oper FR        : Disabled
CSPF        : Enabled                          ADSPEC         : Disabled
Metric      : 0                                Use TE metric  : Disabled
Include Grps:                                  Exclude Grps   :
None                                           None
Least Fill  : Disabled
LdpOverRsvp : Enabled                          VprnAutoBind   : Enabled
IGP Shortcut: Enabled
Oper Metric : 1001

Primary(a)  : to_110_20_1_1                    Up Time        : 0d 01:47:49
Bandwidth   : 0 Mbps
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------------
```

```
LSP Name    : to_10_100_1_1_cspf_20
LSP Type    : RegularLsp                      LSP Tunnel ID  : 201
From        : 110.20.1.4
Adm State   : Up                              Oper State     : Down
LSP Up Time : 0d 00:00:00                     LSP Down Time  : 0d 13:30:49
Transitions : 0                               Path Changes   : 0
Retry Limit : 0                               Retry Timer    : 30 sec
Signaling   : RSVP                            Resv. Style    : SE
Hop Limit   : 255                             Negotiated MTU : 0
Adaptive    : Enabled                         ClassType      : 0
FastReroute : Disabled                        Oper FR        : Disabled
CSPF        : Enabled                         ADSPEC         : Disabled
Metric      : 0                               Use TE metric  : Disabled
Include Grps:                                 Exclude Grps   :
None                                          None
Least Fill  : Disabled
LdpOverRsvp : Enabled                         VprnAutoBind   : Enabled
IGP Shortcut: Enabled
Oper Metric : 65535

Primary     : to_10_100_1_1                   Down Time      : 0d 13:30:49
Bandwidth   : 0 Mbps
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls# show router mpls lsp path detail
===============================================================================
MPLS LSP  Path  (Detail)
===============================================================================
Legend :
    @ - Detour Available              # - Detour In Use
    b - Bandwidth Protected           n - Node Protected
    s - Soft Preemption
===============================================================================
-------------------------------------------------------------------------------
LSP to_110_20_1_1_cspf Path to_110_20_1_1
-------------------------------------------------------------------------------
LSP Name    : to_110_20_1_1_cspf                Path LSP ID : 12856
From        : 110.20.1.4                        To          : 110.20.1.1
Adm State   : Up                                Oper State  : Up
Path Name   : to_110_20_1_1                     Path Type   : Primary
Path Admin  : Up                                Path Oper   : Up
OutInterface: 3/2/1                             Out Label   : 336302
Path Up Time: 0d 01:43:19                       Path Dn Time: 0d 00:00:00
Retry Limit : 0                                 Retry Timer : 30 sec
RetryAttempt: 0                                 NextRetryIn : 0 sec
SetupPriori*: 7                                 Hold Priori*: 0
Preference  : n/a
Bandwidth   : No Reservation                    Oper Bw     : 0 Mbps
Hop Limit   : 255                               Class Type  : 0
Backup CT   : None
MainCT Retry: n/a                               MainCT Retry: 0
    Rem     :                                       Limit   :
Oper CT     : 0
Record Route: Record                            Record Label: Record
Oper MTU    : 1500                              Neg MTU     : 1500
Adaptive    : Enabled                           Oper Metric : 1001
Include Grps:                                   Exclude Grps:
None                                          None
Path Trans  : 13                                CSPF Queries: 56
```

```
Failure Code: noError                           Failure Node: n/a
ExplicitHops:
    No Hops Specified
Actual Hops :
    10.100.30.4(110.20.1.4)                     Record Label    : N/A
 -> 10.100.30.20(10.20.1.20)                    Record Label    : 336302
 -> 10.100.14.1(110.20.1.1)                     Record Label    : 126325
ComputedHops:
    10.100.30.4     -> 10.100.30.20    -> 10.100.14.1
ResigEligib*: False
LastResignal: n/a                               CSPF Metric : 1001
Last MBB    :
 MBB Type   : TimerBasedResignal                MBB State   : Fail
 Ended At   : 03/04/2010 08:53:40               Old Metric  : 0
-------------------------------------------------------------------------------
...
LSP to_10_100_1_1_cspf_20 Path to_10_100_1_1
-------------------------------------------------------------------------------
LSP Name    : to_10_100_1_1_cspf_20             Path LSP ID : 40960
From        : 110.20.1.4                        To          : 10.100.1.1
Adm State   : Up                                Oper State  : Down
Path Name   : to_10_100_1_1                     Path Type   : Primary
Path Admin  : Up                                Path Oper   : Down
OutInterface: n/a                               Out Label   : n/a
Path Up Time: 0d 00:00:00                       Path Dn Time: 0d 13:26:06
Retry Limit : 0                                 Retry Timer : 30 sec
RetryAttempt: 1612                              NextRetryIn : 19 sec
SetupPriori*: 7                                 Hold Priori*: 0
Preference  : n/a
Bandwidth   : No Reservation                    Oper Bw     : 0 Mbps
Hop Limit   : 255                               Class Type  : 0
Backup CT   : None
MainCT Retry: Infinite                          MainCT Retry: 0
    Rem     :                                       Limit   :
Oper CT     : None
Record Route: Record                            Record Label: Record
Oper MTU    : 0                                 Neg MTU     : 0
Adaptive    : Enabled                           Oper Metric : 65535
Include Grps:                                   Exclude Grps:
None                                          None
Path Trans  : 0                                 CSPF Queries: 0
Failure Code: noCspfRouteOwner                  Failure Node: 110.20.1.4
ExplicitHops:
    No Hops Specified
Actual Hops :
    No Hops Specified
ComputedHops:
    No Hops Specified
ResigEligib*: False
LastResignal: n/a                               CSPF Metric : 0
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls#   show router mpls lsp "to_110_20_1_1_cspf"
===============================================================================
MPLS LSPs (Originating)
===============================================================================
LSP Name                          To                    Fastfail     Adm   Opr
                                                        Config
```

```
-------------------------------------------------------------------------------
to_110_20_1_1_cspf                 110.20.1.1          No           Up    Up
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls#   show router mpls lsp "to_110_20_1_1_cspf" detail
===============================================================================
MPLS LSPs (Originating) (Detail)
===============================================================================
-------------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------------
LSP Name    : to_110_20_1_1_cspf
LSP Type    : RegularLsp                      LSP Tunnel ID  : 1
From        : 110.20.1.4
Adm State   : Up                              Oper State     : Up
LSP Up Time : 0d 01:47:02                     LSP Down Time  : 0d 00:00:00
Transitions : 11                              Path Changes   : 11
Retry Limit : 0                               Retry Timer    : 30 sec
Signaling   : RSVP                            Resv. Style    : SE
Hop Limit   : 255                             Negotiated MTU : 1500
Adaptive    : Enabled                         ClassType      : 0
FastReroute : Disabled                        Oper FR        : Disabled
CSPF        : Enabled                         ADSPEC         : Disabled
Metric      : 0                               Use TE metric  : Disabled
Include Grps:                                 Exclude Grps   :
None                                          None
Least Fill  : Disabled
LdpOverRsvp : Enabled                         VprnAutoBind   : Enabled
IGP Shortcut: Enabled
Oper Metric : 1001

Primary(a)  : to_110_20_1_1                   Up Time        : 0d 01:47:02
Bandwidth   : 0 Mbps
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls# show router mpls lsp detail to 110.20.1.2
===============================================================================
MPLS LSPs (Originating) (Detail)
===============================================================================
-------------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------------
LSP Name    : to_110_20_1_2_cspf
LSP Type    : RegularLsp                      LSP Tunnel ID  : 2
From        : 110.20.1.4
Adm State   : Up                              Oper State     : Up
LSP Up Time : 0d 00:01:26                     LSP Down Time  : 0d 00:00:00
Transitions : 529                             Path Changes   : 529
Retry Limit : 0                               Retry Timer    : 30 sec
Signaling   : RSVP                            Resv. Style    : SE
Hop Limit   : 255                             Negotiated MTU : 9206
Adaptive    : Enabled                         ClassType      : 0
FastReroute : Disabled                        Oper FR        : Disabled
CSPF        : Enabled                         ADSPEC         : Disabled
Metric      : 0                               Use TE metric  : Disabled
```

```
Include Grps:                                Exclude Grps    :
None                                         None
Least Fill  : Disabled
LdpOverRsvp : Enabled                        VprnAutoBind    : Enabled
IGP Shortcut: Enabled
Oper Metric : 65535

Primary(a)  : to_110_20_1_2                  Up Time         : 0d 00:01:26
Bandwidth   : 0 Mbps
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------------
LSP Name    : to_110_20_1_2_cspf_20
LSP Type    : RegularLsp                     LSP Tunnel ID  : 49
From        : 110.20.1.4
Adm State   : Up                             Oper State     : Up
LSP Up Time : 0d 00:41:15                    LSP Down Time  : 0d 00:00:00
Transitions : 431                            Path Changes   : 431
Retry Limit : 0                              Retry Timer    : 30 sec
Signaling   : RSVP                           Resv. Style    : SE
Hop Limit   : 255                            Negotiated MTU : 1500
Adaptive    : Enabled                        ClassType      : 0
FastReroute : Disabled                       Oper FR        : Disabled
CSPF        : Enabled                        ADSPEC         : Disabled
Metric      : 0                              Use TE metric  : Disabled
Include Grps:                                Exclude Grps   :
None                                         None
Least Fill  : Disabled
LdpOverRsvp : Enabled                        VprnAutoBind   : Enabled
IGP Shortcut: Enabled
Oper Metric : 66536

Primary(a)  : to_110_20_1_2                  Up Time        : 0d 00:41:15
Bandwidth   : 0 Mbps
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls#    show router mpls lsp count
===============================================================================
MPLS LSP Count
===============================================================================
                    Originate           Transit             Terminate
-------------------------------------------------------------------------------
Static LSPs         0                   136                 0
Dynamic LSPs        140                 421                 1620
Detour LSPs         0                   0                   0
P2MP S2Ls           0                   0                   0
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls# show router mpls lsp path mbb
===============================================================================
MPLS LSP Paths
===============================================================================
-------------------------------------------------------------------------------
LSP to_110_20_1_1_cspf Path to_110_20_1_1
-------------------------------------------------------------------------------
```

```
LastResignal: n/a                                CSPF Metric : 1001
Last MBB    :
 MBB Type   : TimerBasedResignal                 MBB State   : Fail
 Ended At   : 03/04/2010 09:23:58                Old Metric  : 0
-------------------------------------------------------------------------------
LSP to_110_20_1_2_cspf Path to_110_20_1_2
-------------------------------------------------------------------------------
LastResignal: 03/04/2010 09:23:58                CSPF Metric : 65535
-------------------------------------------------------------------------------
LSP to_110_20_1_3_cspf Path to_110_20_1_3
-------------------------------------------------------------------------------
LastResignal: n/a                                CSPF Metric : 1001
Last MBB    :
 MBB Type   : TimerBasedResignal                 MBB State   : Fail
 Ended At   : 03/04/2010 09:23:58                Old Metric  : 0
-------------------------------------------------------------------------------
LSP to_110_20_1_4_cspf Path to_110_20_1_4
-------------------------------------------------------------------------------
LastResignal: n/a                                CSPF Metric : 0
-------------------------------------------------------------------------------
LSP to_110_20_1_5_cspf Path to_110_20_1_5
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
LastResignal: n/a                                CSPF Metric : 0
-------------------------------------------------------------------------------
LSP to_10_100_1_1_cspf_19 Path to_10_100_1_1
-------------------------------------------------------------------------------
LastResignal: n/a                                CSPF Metric : 0
-------------------------------------------------------------------------------
LSP to_10_100_1_1_cspf_20 Path to_10_100_1_1
-------------------------------------------------------------------------------
LastResignal: n/a                                CSPF Metric : 0
===============================================================================
*A:SRU4>config>router>mpls#

In Prog MBB :
 MBB Type   : SoftPreemption                     NextRetryIn : 19 sec
 Started At : 12/08/2008 22:21:11                RetryAttempt: 0
 FailureCode: noError                            Failure Node: n/a
==============================================================================
*A:Dut-B#


*A:SRU4>config>router>mpls# show router mpls lsp transit
===============================================================================
MPLS LSPs (Transit)
===============================================================================
Legend :  @ - Active Detour
===============================================================================
From            To              In I/F   Out I/F  State LSP Name
-------------------------------------------------------------------------------
110.20.1.5      10.20.1.22      3/2/1    3/2/7    Up    to_10_20_1_22_cspf::to*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_3::*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_4::*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_2::*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_20:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_18:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_19:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_17:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_16:*
```

```
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_15:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_13:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_14:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_12:*
110.20.1.5      10.20.1.20      3/2/7    3/2/1    Up    to_10_20_1_20_cspf_10:*
...
110.20.1.3      10.20.1.22      aps-1    3/2/7    Up    to_10_20_1_22_cspf_6::*
110.20.1.3      10.20.1.22      aps-1    3/2/7    Up    to_10_20_1_22_cspf::to*
110.20.1.3      10.20.1.22      aps-1    3/2/7    Up    to_10_20_1_22_cspf_9::*
-------------------------------------------------------------------------------
LSPs : 520
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>config>router>mpls#
*A:SRU4>config>router>mpls# show router mpls lsp terminate
===============================================================================
MPLS LSPs (Terminate)
===============================================================================
Legend :  @ - Active Detour
===============================================================================
From            To              In I/F   Out I/F  State LSP Name
-------------------------------------------------------------------------------
110.20.1.5      110.20.1.4      3/2/1    n/a      Up    b4-1::b4-1
110.20.1.5      110.20.1.4      3/2/7    n/a      Up    gsr::gsr
10.20.1.22      110.20.1.4      3/2/7    n/a      Up    gsr2_t10
110.20.1.6      110.20.1.4      3/2/3:10 n/a      Up    1::2
110.20.1.6      110.20.1.4      3/2/3:3  n/a      Up    1::stby
110.20.1.6      110.20.1.4      3/2/3:10 n/a      Up    2::2
110.20.1.6      110.20.1.4      3/2/3:6  n/a      Up    2::stby
110.20.1.6      110.20.1.4      3/2/3:10 n/a      Up    3::2
110.20.1.6      110.20.1.4      3/2/3:6  n/a      Up    3::stby
...
110.20.1.3      110.20.1.4      aps-1    n/a      Up    to_110_20_1_4_cspf_20:*
110.20.1.3      110.20.1.4      aps-1    n/a      Up    to_110_20_1_4_cspf_4::*
-------------------------------------------------------------------------------
LSPs : 1603
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls# show router mpls lsp terminate detail
===============================================================================
MPLS LSPs (Terminate) (Detail)
===============================================================================
-------------------------------------------------------------------------------
LSP b4-1::b4-1
-------------------------------------------------------------------------------
From                 : 110.20.1.5           To            : 110.20.1.4
State                : Up
SetupPriority        : 7                    Hold Priority : 0
Class Type           : 0
In Interface         : 3/2/1                In Label      : 131071
Previous Hop         : 10.100.30.20
-------------------------------------------------------------------------------
LSP gsr::gsr
-------------------------------------------------------------------------------
From                 : 110.20.1.5           To            : 110.20.1.4
State                : Up
SetupPriority        : 7                    Hold Priority : 0
Class Type           : 0
```

```
In Interface         : 3/2/7               In Label      : 128547
Previous Hop         : 160.60.60.2
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
From                 : 110.20.1.3          To            : 110.20.1.4
State                : Up
SetupPriority        : 7                   Hold Priority : 0
Class Type           : 0
In Interface         : aps-1               In Label      : 130409
Previous Hop         : 104.104.0.3
===============================================================================
*A:SRU4>config>router>mpls#
```

lsp-egress-stats

Syntax **lsp-egress-stats**
lsp-egress-stats *lsp-name*

Context show>router>mpls

Description This command displays MPLS LSP egress statistics information.

lsp-ingress-stats

Syntax **lsp-ingress-stats**
lsp-ingress-stats *ip-address* **lsp** *lsp-name*

Context show>router>mpls

Description This command displays MPLS LSP ingress statistics information.

p2mp-info

Syntax **p2mp-info** [**type** {**originate** | **transit** | **terminate**}] [**s2l-endpoint** *ip-address*]

Context show>router>mpls

Description This command displays P2MP cross-connect information.

Parameters **type —** Specifies the P2MP type.

Values **originate** — Specifies to display the static LSPs that originate at this virtual router.
transit — Specifies to display the static LSPs that transit through this virtual router.
terminate — Specifies to display the static LSPs that terminate at this virtual router.

Sample Output

```
*A:SetupCLI# show router mpls p2mp-info
```

```
=======================================================================
MPLS P2MP Cross Connect Information
=======================================================================
-----------------------------------------------------------------------
S2L 3::1
-----------------------------------------------------------------------
Source IP Address    : 200.0.0.61           Tunnel ID     : 4
P2MP ID              : 255                  Lsp ID        : 49152
S2L Name             : 3::1                 To            : 200.0.0.63
In Interface         : 1/1/1:1              In Label      : 131070
Num. of S2ls         : 1
-----------------------------------------------------------------------
S2L 3::2
-----------------------------------------------------------------------
Source IP Address    : 200.0.0.61           Tunnel ID     : 4
P2MP ID              : 255                  Lsp ID        : 49152
S2L Name             : 3::2                 To            : 200.0.0.65
Out Interface        : 2/1/1:2              Out Label     : 131071
Num. of S2ls         : 2
-----------------------------------------------------------------------
S2L 3::2
-----------------------------------------------------------------------
Source IP Address    : 200.0.0.61           Tunnel ID     : 4
P2MP ID              : 255                  Lsp ID        : 49152
S2L Name             : 3::2                 To            : 200.0.0.66
Out Interface        : 2/1/1:2              Out Label     : 131071
Num. of S2ls         : 2
-----------------------------------------------------------------------
P2MP Cross-connect instances : 3
=======================================================================
*A:SetupCLI#
```

p2mp-lsp

Syntax **p2mp-lsp** [*lsp-name*] [**detail**]
p2mp-lsp [*lsp-name*] **p2mp-instance** [*p2mp-instance-name*] [**mbb**]
p2mp-lsp [*lsp-name*] **p2mp-instance** [*p2mp-instance-name*] **s2l** [*s2l-name* [**to** *s2l-to-address*]] [**status** {**up** | **down**}] [**detail**]
p2mp-lsp [*lsp-name*] **p2mp-instance** [*p2mp-instance-name*] **s2l** [*s2l-name* [**to** *s2l-to-address*]] **mbb**

Context show>router>mpls

Description This command displays MPLS P2MP LSP information.

Parameters *lsp-name* — Specifies the name of the LSP used in the path.

p2mp-instance[*p2mp-instance-name* **—** Specifies the administrative name for the P2MP instance which must be unique within a virtual router instance.

mbb — Specifies to display make-before-break (MBB) information.

s2l — Specifies the source-to-leaf (S2L) name.

to *s2l-to-address* **—**

status — Displays the status of the p2mp LSP.

Values up — Displays the total time that this S2l has been operational.
down — Displays the total time that this S2l has not been operational.

Sample Output

```
A:ALU-25# show router mpls p2mp-lsp lsp_1
========================================================================
MPLS LSPs (Originating)
========================================================================
LSP Name                     To/P2MP ID            Fastfail     Adm   Opr
                                                     Config
------------------------------------------------------------------------
lsp_1                            18                  Yes          Up    Up
------------------------------------------------------------------------
LSPs : 1
========================================================================
A:ALU-25#

A:ALU-25# show router mpls p2mp-lsp Test_p2mp detail
========================================================================
MPLS P2MP LSPs (Originating) (Detail)
========================================================================
------------------------------------------------------------------------
Type : Originating
------------------------------------------------------------------------
LSP Name    : lsp_1                             LSP Tunnel ID  : 1
From       : 10.10.1.1                       P2MP ID       : 18
Adm State   : Up                                Oper State     : Down
LSP Up Time : 0d 00:00:00                       LSP Down Time  : 0d 20:39:48
Transitions : 0                                 Path Changes   : 0
Retry Limit : 0                                 Retry Timer    : 30 sec
Signaling   : RSVP                              Resv. Style    : FF
Hop Limit   : 255                               Adaptive       : Enabled
FastReroute : Disabled                          Oper FR        : Disabled
FR Method   : Facility                          FR Hop Limit   : 45
FR Bandwidth: 0 Mbps                            FR Node Protect: Disabled
FR Object   : Enabled
CSPF        : Disabled                          ADSPEC         : Disabled
Metric      : 1                                 Use TE metric  : Disabled
Include Grps:                                   Exclude Grps   :
None                                            None

P2MPinstance:Test_p2mp                          p2mp-inst-type : primary

S2L Name    :Test-s2l1                          To             : 10.20.1.6
S2L Name    :Test-s2l2                          To             : 10.20.1.5
S2L Name    :Test-s2l3                          To             : 10.20.1.4
------------------------------------------------------------------------
A:ALU-25#

A:ALU-25# show router mpls p2mp-lsp Test_p2mp
========================================================================
MPLS P2MP Instance (Originating)
========================================================================
------------------------------------------------------------------------
Type : Originating
------------------------------------------------------------------------
LSP Name    : lsp_1                             LSP Tunnel ID  : 1
```

```
P2MP ID      : 18                               Path LSP ID     : 18
Adm State    : Up                               Oper State      : Down

P2MPinstance:Test_p2mp                          p2mp-inst-type : primary
Inst Name    : lsp_1                            P2MP Inst ID    : 1
Adm State    : Up                               Oper State      : Down
Inst Up Time: 0d 00:00:00                       Inst Down Time : 0d 20:39:48
Hop Limit    : 255                              Adaptive        : Enabled
Record Route: Record                            Record Label    : Record
Include Grps:                                   Exclude Grps    :
None                                            None
Bandwidth    : 0 Mbps                           Oper Bw         : 0 Mbps

S2L Name     :Test-s2l1                         To              : 10.20.1.6
S2L Name     :Test-s2l2                         To              : 10.20.1.5
S2L Name     :Test-s2l3                         To              : 10.20.1.4
-------------------------------------------------------------------------
A:ALU-25#
```

Note that the normal output is in detailed format only. There is no separate detail format.

```
A:ALU-52# show router mpls p2mp-lsp [p2mp-lsp-name] p2mp-instance [p2mp-inst-name]
=========================================================================
MPLS P2MP Instance (Originating)
=========================================================================
-------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------
LSP Name     : lsp_1                            LSP Tunnel ID  : 1
P2MP ID      : 18                               Path LSP ID     : 18
Adm State    : Up                               Oper State      : Down

P2MPinstance:Test_p2mp                          p2mp-inst-type : primary
Inst Name    : lsp_1                            P2MP Inst ID    : 1
Adm State    : Up                               Oper State      : Down
Inst Up Time: 0d 00:00:00                       Inst Down Time : 0d 20:39:48
Hop Limit    : 255                              Adaptive        : Enabled
Record Route: Record                            Record Label    : Record
Include Grps:                                   Exclude Grps    :
None                                            None
Bandwidth    : 0 Mbps                           Oper Bw         : 0 Mbps

S2L Name     :Test-s2l1                         To              : 10.20.1.6
S2L Name     :Test-s2l2                         To              : 10.20.1.5
S2L Name     :Test-s2l3                         To              : 10.20.1.4
-------------------------------------------------------------------------
A:ALU-52#


A:ALU-52# show router mpls p2mp-lsp [p2mp-lsp-name] p2mp-instance [p2mp-inst-name]
mbb
=========================================================================
MPLS P2MP Instance (Originating)
=========================================================================
-------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------
LSP Name     : lsp_1                            LSP Tunnel ID  : 1
P2MP ID      : 18                               Path LSP ID     : 18
Adm State    : Up                               Oper State      : Down
```

```
P2MPinstance:Test_p2mp                          p2mp-inst-type : primary
Inst Name    : lsp_1                            P2MP Inst ID   : 1
Adm State    : Up                               Oper State     : Down
Inst Up Time: 0d 00:00:00                       Inst Down Time : 0d 20:39:48
Hop Limit    : 255                              Adaptive       : Enabled
Record Route: Record                            Record Label   : Record
Include Grps:                                   Exclude Grps   :
None                                            None
Bandwidth    : 0 Mbps                           Oper Bw        : 0 Mbps
Last MBB     :
MBB type     :                                  Mbb State      :
ended at     :                                  Old Metric     :
In Prog MBB :
MBB type     :                                  Next Retry In  :
Started at  :                                   Retry Attempt  :
Failure code:                                   Failure Node   :

S2L Name     :Test-s2l1                         To             : 10.20.1.6
S2l Admin    :                                  S2l Oper       :
Failure code:                                   Failure Node   : 10.12.1.1

S2L Name     :Test-s2l1           To             : 10.20.1.6
S2l Admin    :                                  S2l Oper       :
Failure code:                                   Failure Node   : 10.12.1.1
-------------------------------------------------------------------------
A:ALU-52#


A:ALU-52# show router mpls p2mp-lsp [p2mp-lsp-name] p2mp-instance [p2mp-inst-name]
s2l [s2l-name]
=========================================================================
MPLS S2Ls (Originating)
=========================================================================
S2L Name                           To             Next Hop     Adm   Opr
-------------------------------------------------------------------------
Test-s2l1                          10.20.1.6      10.10.1.2    Up    Up
-------------------------------------------------------------------------
LSPs : 1
=========================================================================
A:ALU-52#


A:ALU-52# show router mpls p2mp-lsp [p2mp-lsp-name] p2mp-instance [p2mp-inst-name]
s2l [s2l-name] detail
=========================================================================
MPLS S2Ls (Originating) (Detail)
=========================================================================
-------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------
LSP Name     : lsp_1                            LSP Tunnel ID  : 1
P2MP ID      : 18                               Path LSP ID    : 18
Adm State    : Up                               Oper State     : Down

P2MP Primary Instance:
Inst Name    : lsp_1                            P2MP Inst ID   : 1
Adm State    : Up                               Oper State     : Down

S2L Name     : Test-s2l1                        To             : 10.20.1.6
Adm State    : Up                               Oper State     : Down
```

```
OutInterface: 1/1/1                             Out Label      : 131071
S2L Up Time : 0d 00:00:00                       S2L Down Time  : 0d 20:39:48
Transitions : 0                                 Path Changes   : 0
Retry Limit : 0                                 Retry Timer    : 30 sec
RetryAttempt: 0                                 NextRetryIn    : 0 sec
Bandwidth   : No Reservation                    Oper Bw        : 0 Mbps
Hop Limit   : 255                               Adaptive       : Enabled
Record Route: Record                            Record Label   : Record
Oper MTU    : 1496                              Neg MTU        : 1496
FastReroute : Disabled                          Oper FR        : Disabled
FR Method   : Facility                          FR Hop Limit   : 45
FR Bandwidth: 0 Mbps                            FR Node Protect: Disabled
FR Object   : Enabled
CSPF        : Disabled                          ADSPEC         : Disabled
Metric      : 1                                 Use TE metric  : Disabled
Include Grps:                                   Exclude Grps   :
None                                            None
CSPF Queries: 9
Failure Code: noError                           Failure Node   : n/a
ExplicitHops:
    No Hops Specified
Actual Hops :
    10.10.1.1(10.20.1.1) @                      Record Label   : N/A
 -> 10.10.1.2(10.20.1.2)                        Record Label   : 131071
ComputedHops:
    10.10.1.1       -> 10.10.1.2
LastResignal: n/a                               CSPF Metric    : 1000
-------------------------------------------------------------------------
A:ALU-52#
```

srlg-database

Syntax **srlg-database** [**router-id** *ip-address*] [**interface** *ip-address*]

Context show>router>mpls

Description This command displays MPLS SRLG database information.

Parameters **router-id** *ip-address* **—** Specifies a 32-bit integer uniquely identifying the router in the Autonomous System. By convention to ensure uniqueness, this may default to the value of one of the router's IPv4 host addresses, represented as a 32-bit unsigned integer, if IPv4 is configured on the router. The router-id can be either the local one or some remote router.

interface *ip-address* **—** Specifies the IP address of the interface.

path

Syntax **path** [*path-name*] [*lsp-binding*]

Context show>router>mpls

Description This command displays MPLS paths.

Parameters *path-name* — The unique name label for the LSP path.

lsp-binding — Keyword to display binding information.

Output **MPLS Path Output —** The following table describes MPLS Path output fields.

Label	Description
Path Name	The unique name label for the LSP path.
Adm	Down — The path is administratively disabled.
	Up — The path is administratively enabled.
Hop Index	The value used to order the hops in a path.
IP Address	The IP address of the hop that the LSP should traverse on the way to the egress router.
Strict/Loose	Strict — The LSP must take a direct path from the previous hop router to the next router.
	Loose — The route taken by the LSP from the previous hop to the next hop can traverse through other routers.
LSP Name	The name of the LSP used in the path.
Binding	Primary — The preferred path for the LSP.
	Secondary — The standby path for the LSP.
Paths	Total number of paths configured.

Sample Output

```
*A:SRU4>config>router>mpls# show router mpls path
===============================================================================
MPLS Path:
===============================================================================
Path Name                          Adm  Hop Index   IP Address        Strict/Loose
-------------------------------------------------------------------------------
to_110_20_1_1                      Up   no hops     n/a               n/a

to_110_20_1_2                      Up   no hops     n/a               n/a

to_110_20_1_3                      Up   no hops     n/a               n/a

to_110_20_1_4                      Up   no hops     n/a               n/a

to_110_20_1_5                      Up   no hops     n/a               n/a
```

```
to_110_20_1_6                   Up   no hops     n/a              n/a

to_110_20_1_110                 Up   no hops     n/a              n/a

to_10_8_100_15                  Up   no hops     n/a              n/a

to_10_20_1_20                   Up   no hops     n/a              n/a

to_10_20_1_22                   Up   no hops     n/a              n/a

to_10_100_1_1                   Up   no hops     n/a              n/a
------------------------------------------------------------------------------
Paths : 11
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls# show router mpls path lsp-binding
===============================================================================
MPLS Path:
===============================================================================
Path Name                       Opr  LSP Name                        Binding
-------------------------------------------------------------------------------
to_110_20_1_1                   Up   to_110_20_1_1_cspf              Primary
                                Up   to_110_20_1_1_cspf_2            Primary
                                Up   to_110_20_1_1_cspf_3            Primary
Up   to_110_20_1_1_cspf_16           Primary
                                Up   to_110_20_1_1_cspf_17           Primary
                                Up   to_110_20_1_1_cspf_18           Primary
                                Up   to_110_20_1_1_cspf_19           Primary
                                Up   to_110_20_1_1_cspf_20           Primary
to_110_20_1_2                   Up   to_110_20_1_2_cspf              Primary
                                Up   to_110_20_1_2_cspf_2            Primary
                                Up   to_110_20_1_2_cspf_3            Primary
                                Up   to_110_20_1_2_cspf_4            Primary
                                Up   to_110_20_1_2_cspf_5            Primary
...
to_10_100_1_1                   Down to_10_100_1_1_cspf              Primary
                                Down to_10_100_1_1_cspf_2            Primary
                                Down to_10_100_1_1_cspf_3            Primary
                                Down to_10_100_1_1_cspf_4            Primary
                                Down to_10_100_1_1_cspf_5            Primary
                                Down to_10_100_1_1_cspf_6            Primary
Down to_10_100_1_1_cspf_13           Primary
                                Down to_10_100_1_1_cspf_14           Primary
                                Down to_10_100_1_1_cspf_15           Primary
                                Down to_10_100_1_1_cspf_16           Primary
                                Down to_10_100_1_1_cspf_17           Primary
                                Down to_10_100_1_1_cspf_18           Primary
                                Down to_10_100_1_1_cspf_19           Primary
                                Down to_10_100_1_1_cspf_20           Primary
-------------------------------------------------------------------------------
Paths : 11
===============================================================================
*A:SRU4>config>router>mpls#
```

srlg-group

Syntax **srlg-group** [*group-name*]

Context show>router>mpls

Description This command displays MPLS SRLG groups

Parameters *group-name* — Specifies the name of the SRLG group within a virtual router instance.

Output **MPLS SRLG Group Output —** The following table describes MPLS SRLG group output fields

Label	Description
Group Name	Displays the name of the SRLG group within a virtual router instance.
Group Value	Displays the group value associated with this SRLG group.
Interface	Displays the interface where the SRLG groups is associated.
No. of Groups	Displays the total number of SRLG groups associated with the output.

Sample Output

```
*A:SRU4>config>router>mpls# show router mpls srlg-group
===============================================================================
MPLS Srlg Groups
===============================================================================
Group Name                      Group Value   Interfaces
-------------------------------------------------------------------------------
1432                            1432          srl-1
1433                            1433          srl-3
1434                            1434          aps-8
1435                            1435          aps-9
2410                            2410          srr-1
2411                            2411          srr-2
2412                            2412          srr-3
3410                            3410          aps-1
3420                            3420          aps-2
3430                            3430          aps-3
3440                            3440          sr4-1
41.80                           4180          g7600
41104                           41104         germ-1
415.70                          41570         gsr1
420.40                          42040         m160
422.60                          42260         gsr2
44.200                          44200         hubA
45100                           45100         ess-7-1
45110                           45110         ess-7-2
45120                           45120         ess-7-3
4651                            4651          src-1.1
4652                            4652          src-1.2
4653                            4653          src-1.3
4654                            4654          src-1.4
4655                            4655          src-1.5
4656                            4656          src-1.6
4657                            4657          src-1.7
4658                            4658          src-1.8
```

```
4659                             4659          src-1.9
4660                             4660          src-1.10
-------------------------------------------------------------------------------
No. of Groups: 30
===============================================================================
*A:SRU4>config>router>mpls#


*A:SRU4>config>router>mpls# show router mpls srlg-group "1432"
===============================================================================
MPLS Srlg Groups
===============================================================================
Group Name                       Group Value   Interfaces
-------------------------------------------------------------------------------
1432                             1432          srl-1
-------------------------------------------------------------------------------
No. of Groups: 1
===============================================================================
*A:SRU4>config>router>mpls#
```

static-lsp

Syntax **static-lsp** [*lsp-name*]
static-lsp {**transit** | **terminate**}
static-lsp count

Context show>router>mpls

Description This command displays MPLS static LSP information.

Output **MPLS Static LSP Output —** The following table describes MPLS static LSP output fields.

Label	Description
Lsp Name	The name of the LSP used in the path.
To	The system IP address of the egress router for the LSP.
Next Hop	The system IP address of the next hop in the LSP path.
In I/F	The ingress interface.
Out Label	The egress interface.
Out I/F	The egress interface.
Adm	Down — The path is administratively disabled.
	Up — The path is administratively enabled.
Opr	Down — The path is operationally down.
	Up — The path is operationally up.
LSPs	The total number of static LSPs.

Sample Output

```
A:ALA-12# show router mpls static-lsp
===============================================================================
MPLS Static LSPs (Originating)
===============================================================================
Lsp Name          To              Next Hop        Out Label Out I/F   Adm  Opr
-------------------------------------------------------------------------------
NYC_SJC_customer2 100.20.1.10     10.10.1.4       1020      1/1/1     Up   Up
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
A:ALA-12#


*A:SRU4>config>router>mpls# show router mpls static-lsp transit
===============================================================================
MPLS Static LSPs (Transit)
===============================================================================
In Label     In Port      Out Label    Out Port     Next Hop            Adm   Opr
-------------------------------------------------------------------------------
240          aps-1        440          1/1/10       11.22.11.3          Up    Up
241          aps-1        441          1/1/10       11.22.11.3          Up    Up
242          aps-1        442          1/1/10       11.22.11.3          Up    Up
243          aps-1        443          1/1/10       11.22.11.3          Up    Up
244          aps-1        444          1/1/10       11.22.11.3          Up    Up
245          aps-1        445          1/1/10       11.22.11.3          Up    Up
246          aps-1        446          1/1/10       11.22.11.3          Up    Up
247          aps-1        447          1/1/10       11.22.11.3          Up    Up
248          aps-1        448          1/1/10       11.22.11.3          Up    Up
249          aps-1        449          1/1/10       11.22.11.3          Up    Up
250          aps-1        450          1/1/10       11.22.11.3          Up    Up
251          aps-1        451          1/1/10       11.22.11.3          Up    Up
252          aps-1        452          1/1/10       11.22.11.3          Up    Up
253          aps-1        453          1/1/10       11.22.11.3          Up    Up
...
207          3/2/8        407          1/1/9        11.22.10.3          Up    Up
208          3/2/8        408          1/1/9        11.22.10.3          Up    Up
209          3/2/8        409          1/1/9        11.22.10.3          Up    Up
-------------------------------------------------------------------------------
LSPs : 256
===============================================================================
*A:SRU4>config>router>mpls#

A:ALA-12# show router mpls static-lsp terminate
===============================================================================
MPLS Static LSPs (Terminate)
===============================================================================
In Label     In I/F       Out Label    Out I/F      Next Hop            Adm   Opr
-------------------------------------------------------------------------------
1021         1/1/1        n/a          n/a          n/a                 Up    Up
-------------------------------------------------------------------------------
LSPs : 1
===============================================================================
A:ALA-12#
```

statistics-summary

Syntax **statistics-summary**

Context show>router>mpls>statistics-summary

Description This command displays the number of LSP statistics configured.

Sample Output

```
*A:SRU4>config>router>mpls# show router mpls statistics-summary
===============================================================================
Statistics Summary
===============================================================================
LSP egress statistics                : 0
LSP ingress statistics               : 0
===============================================================================
*A:SRU4>config>router>mpls#
```

status

Syntax **status**

Context show>router>mpls

Description This command displays MPLS operation information.

Output **MPLS Status Output —** The following table describes MPLS status output fields.

Label	Description
`Admin Status`	`Down` — MPLS is administratively disabled. `Up` — MPLS is administratively enabled.
`Oper Status`	`Down` — MPLS is operationally down. `Up` — MPLS is operationally up.
`LSP Counts`	`Static LSPs` — Displays the count of static LSPs that originate, transit, and terminate on or through the router. `Dynamic LSPs` — Displays the count of dynamic LSPs that originate, transit, and terminate on or through the router. `Detour LSPs` — Displays the count of detour LSPs that originate, transit, and terminate on or through the router.
`FR Object`	`Enabled` — Specifies that Fast reroute object is signaled for the LSP. `Disabled` — Specifies that Fast reroute object is not signaled for the LSP.
`Resignal Timer`	`Enabled` — Specifies that the resignal timer is enabled for the LSP. `Disabled` — Specifies that the resignal timer is disabled for the LSP.
`Hold Timer`	Displays the amount of time that the ingress node holds before programming its data plane and declaring the LSP up to the service module.

Sample Output

```
*A:SRU4>config>router>mpls# show router mpls status
===============================================================================
MPLS Status
===============================================================================
Admin Status       : Up                 Oper Status        : Up
Oper Down Reason   : n/a
FR Object          : Enabled            Resignal Timer     : 30 minutes
Hold Timer         : 1 seconds          Next Resignal      : 13 minutes
Srlg Frr           : Enabled            Srlg Frr Strict    : Enabled
Dynamic Bypass     : Enabled            User Srlg Database : Disabled
```

```
Least Fill Min Thd.: 5 percent          LeastFill ReoptiThd: 10 percent
Short. TTL Prop Lo*: Enabled            Short. TTL Prop Tr*: Enabled

P2mp Resignal Timer: Disabled           P2mp Next Resignal : N/A
Sec FastRetryTimer : Disabled           Static LSP FR Timer: 30 seconds

LSP Counts          Originate           Transit             Terminate
-------------------------------------------------------------------------------
Static LSPs         0                   136                 0
Dynamic LSPs        140                 499                 1626
Detour LSPs         0                   0                   0
P2MP S2Ls           0                   0                   0
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>config>router>mpls#
```

Show RSVP Commands

interface

Syntax **interface** [*ip-int-name* | *ip-address*] **statistics** [**detail**]

Context show>router>rsvp

Description This command shows RSVP interfaces.

ip-int-name — The name of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-address — The system or network interface IP address.

statistics — Displays IP address and the number of packets sent and received on an interface-basis.

detail — Displays detailed information.

Output **RSVP Interface Output —** The following table describes RSVP interface output fields.

Label	Description
`Interface`	The name of the IP interface.
`Total Sessions`	The total number of RSVP sessions on this interface. This count includes sessions that are active as well as sessions that have been signaled but a response has not yet been received.
`Active Sessions`	The total number of active RSVP sessions on this interface.
`Total BW (Mbps)`	The amount of bandwidth in megabits per second (Mbps) available to be reserved for the RSVP protocol on the interface.
`Resv BW (Mbps)`	The amount of bandwidth in mega-bits per seconds (Mbps) reserved on this interface. A value of zero (0) indicates that no bandwidth is reserved.
`Adm`	`Down` – The RSVP interface is administratively disabled.
	`Up` – The RSVP interface is administratively enabled.
`Bfd`	`Yes` – BFD is enabled on the RSVP interface.
	`No` – BFD is disabled on the RSVP interface.
`Opr`	`Down` – The RSVP interface is operationally down.
	`Up` – The RSVP interface is operationally up.
`Port ID`	Specifies the physical port bound to the interface.

Label	Description (Continued)
`Active Resvs`	The total number of active RSVP sessions that have reserved bandwidth.
`Subscription`	Specifies the percentage of the link bandwidth that RSVP can use for reservation. When the value is zero (0), no new sessions are permitted on this interface.
`Port Speed`	Specifies the speed for the interface.
`Unreserved BW`	Specifies the amount of unreserved bandwidth.
`Reserved BW`	Specifies the amount of bandwidth in megabits per second (Mbps) reserved by the RSVP session on this interface. A value of zero (0) indicates that no bandwidth is reserved.
`Total BW`	Specifies the amount of bandwidth in megabits per second (Mbps) available to be reserved for the RSVP protocol on this interface.
`Aggregate`	Aggregate messages are used to pack multiple RSVP messages into a single packet to reduce the network overhead. When the value is true, RSVP negotiates with each neighbor and gets consensus before sending aggregate messages.
`Hello Interval`	Specifies the length of time, in seconds, between the hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network. When the value is zero (0), the sending of hello messages is disabled.
`Refresh Time`	Specifies the interval between the successive Path and Resv refresh messages. RSVP declares the session down after it misses ((keep-multiplier + 0.5) * 1.5 * refresh-time)) consecutive refresh messages.
`Hello Timeouts`	The total number of hello messages that timed out on this RSVP interface.
`Neighbors`	The IP address of the RSVP neighbor.
`Sent`	The total number of error free RSVP packets that have been transmitted on the RSVP interface.
`Recd`	The total number of error free RSVP packets received on the RSVP interface.
`Total Packets`	The total number of RSVP packets, including errors, received on the RSVP interface.
`Bad Packets`	The total number of RSVP packets with errors transmitted on the RSVP interface.
`Paths`	The total number of RSVP PATH messages received on the RSVP interface.
`Path Errors`	The total number of RSVP PATH ERROR messages transmitted on the RSVP interface.

Label	Description (Continued)
Path Tears	The total number of RSVP PATH TEAR messages received on the RSVP interface.
Resvs	The total number of RSVP RESV messages received on the RSVP interface.
Resv Confirms	The total number of RSVP RESV CONFIRM messages received on the RSVP interface.
Resv Errors	Total RSVP RESV ERROR messages received on RSVP interface.
Resv Tears	Total RSVP RESV TEAR messages received on RSVP interface.
Refresh Summaries	Total RSVP RESV summary refresh messages received on interface.
Refresh Acks	Total RSVP RESV acknowledgement messages received when refresh reduction is enabled on the RSVP interface.
Bundle Packets	Total RSVP RESV bundled packets received on the RSVP interface.
Hellos	Total RSVP RESV HELLO REQ messages received on the interface.

Sample Output

```
*A:SRU4>show>router>rsvp# interface
===============================================================================
RSVP Interfaces
===============================================================================
Interface                        Total    Active    Total BW  Resv BW   Adm Opr
                                 Sessions Sessions  (Mbps)    (Mbps)
-------------------------------------------------------------------------------
system                           -        -         -         -         Up  Up
aps-1                            0        0         6012      0         Up  Up
aps-2                            0        0         6010      0         Up  Up
aps-3                            0        0         6010      0         Up  Up
sr4-1                            0        0         6010      0         Up  Up
ess-7-1                          9        9         100       0         Up  Up
ess-7-2                          7        7         100       0         Up  Up
ess-7-3                          4        4         100       0         Up  Up
ess-7-4                          0        0         800       0         Up  Up
ess-7-5                          0        0         800       0         Up  Up
ess-7-6                          0        0         800       0         Up  Up
hubA                             0        0         100       0         Up  Up
germ-1                           0        0         1000      0         Up  Up
src-1.1                          3        3         100       0         Up  Up
src-1.2                          2        2         100       0         Up  Up
src-1.3                          3        3         100       0         Up  Up
src-1.4                          5        5         100       0         Up  Up
...
g7600                            0        0         1000      0         Up  Up
m160                             481      481       1000      82        Up  Up
-------------------------------------------------------------------------------
Interfaces : 35
===============================================================================
*A:SRU4>show>router>rsvp#
```

```
*A:SRU4>show>router>rsvp# interface statistics
===============================================================================
RSVP Interface (statistics)
===============================================================================
-------------------------------------------------------------------------------
Interface system
-------------------------------------------------------------------------------
Interface                    : Up
Total Packets        (Sent) : 0                      (Recd.): 0
Bad Packets          (Sent) : 0                      (Recd.): 0
Paths                (Sent) : 0                      (Recd.): 0
Path Errors          (Sent) : 0                      (Recd.): 0
Path Tears           (Sent) : 0                      (Recd.): 0
Resvs                (Sent) : 0                      (Recd.): 0
Resv Confirms        (Sent) : 0                      (Recd.): 0
Resv Errors          (Sent) : 0                      (Recd.): 0
Resv Tears           (Sent) : 0                      (Recd.): 0
Refresh Summaries    (Sent) : 0                      (Recd.): 0
Refresh Acks         (Sent) : 0                      (Recd.): 0
Bundle Packets       (Sent) : 0                      (Recd.): 0
Hellos               (Sent) : 0                      (Recd.): 0
Auth Errors          (Sent) : 0                      (Recd.): 0
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Interface m160
-------------------------------------------------------------------------------
Interface                    : Up
Total Packets        (Sent) : 883643                 (Recd.): 3052503
Bad Packets          (Sent) : 0                      (Recd.): 0
Paths                (Sent) : 592153                 (Recd.): 373610
Path Errors          (Sent) : 464                    (Recd.): 30716
Path Tears           (Sent) : 29563                  (Recd.): 3480
Resvs                (Sent) : 93970                  (Recd.): 2518660
Resv Confirms        (Sent) : 0                      (Recd.): 0
Resv Errors          (Sent) : 136815                 (Recd.): 54115
Resv Tears           (Sent) : 13338                  (Recd.): 71922
Refresh Summaries    (Sent) : 0                      (Recd.): 0
Refresh Acks         (Sent) : 0                      (Recd.): 0
Bundle Packets       (Sent) : 0                      (Recd.): 0
Hellos               (Sent) : 17340                  (Recd.): 0
Auth Errors          (Sent) : 0                      (Recd.): 0
===============================================================================
*A:SRU4>show>router>rsvp#


*A:SRU4>show>router>rsvp# interface "sr4-1" statistics
===============================================================================
RSVP Interface : sr4-1 (statistics)
===============================================================================
-------------------------------------------------------------------------------
Interface sr4-1
-------------------------------------------------------------------------------
Interface                    : Up
Total Packets        (Sent) : 33100                  (Recd.): 20405
Bad Packets          (Sent) : 0                      (Recd.): 0
Paths                (Sent) : 0                      (Recd.): 1833
Path Errors          (Sent) : 1783                   (Recd.): 9
Path Tears           (Sent) : 0                      (Recd.): 1157
Resvs                (Sent) : 76                     (Recd.): 0
Resv Confirms        (Sent) : 0                      (Recd.): 0
```

```
Resv Errors          (Sent) : 0                    (Recd.): 0
Resv Tears           (Sent) : 1                    (Recd.): 0
Refresh Summaries    (Sent) : 4                    (Recd.): 33
Refresh Acks         (Sent) : 1520                 (Recd.): 4
Bundle Packets       (Sent) : 0                    (Recd.): 0
Hellos               (Sent) : 29716                (Recd.): 17369
Auth Errors          (Sent) : 0                    (Recd.): 0
===============================================================================
*A:SRU4>show>router>rsvp#

*A:SRU4>show>router>rsvp#  interface detail
===============================================================================
RSVP Interfaces (Detailed)
===============================================================================
-------------------------------------------------------------------------------
Interface : system
-------------------------------------------------------------------------------
Interface         : system
Port ID           : system
Admin State       : Up                     Oper State        : Up
Active Sessions   : 0                      Active Resvs      : 0
Total Sessions    : 0
Subscription      : 100 %                  Port Speed        : 0 Mbps
Total BW          : 0 Mbps                 Aggregate         : Dsabl
Hello Interval    : 3000 ms                Hello Timeouts    : 0
Authentication    : Disabled
Auth Rx Seq Num   : n/a                    Auth Key Id       : n/a
Auth Tx Seq Num   : n/a                    Auth Win Size     : n/a
Refresh Reduc.    : Enabled                Reliable Deli.    : Disabled
Bfd Enabled       : No                     Graceful Shut.    : Disabled
ImplicitNullLabel : Disabled*

Percent Link Bandwidth for Class Types*
Link Bw CT0       : 100                    Link Bw CT4       : 0
Link Bw CT1       : 0                      Link Bw CT5       : 0
Link Bw CT2       : 0                      Link Bw CT6       : 0
Link Bw CT3       : 0                      Link Bw CT7       : 0

Bandwidth Constraints for Class Types (Kbps)
BC0               : 0                      BC4               : 0
BC1               : 0                      BC5               : 0
BC2               : 0                      BC6               : 0
BC3               : 0                      BC7               : 0

Bandwidth for TE Class Types (Kbps)
TE0->  Resv. Bw   : 0                      Unresv. Bw        : 0
TE1->  Resv. Bw   : 0                      Unresv. Bw        : 0
TE2->  Resv. Bw   : 0                      Unresv. Bw        : 0
TE3->  Resv. Bw   : 0                      Unresv. Bw        : 0
TE4->  Resv. Bw   : 0                      Unresv. Bw        : 0
TE5->  Resv. Bw   : 0                      Unresv. Bw        : 0
TE6->  Resv. Bw   : 0                      Unresv. Bw        : 0
TE7->  Resv. Bw   : 0                      Unresv. Bw        : 0

IGP Update
Up Thresholds(%)    : 0 15 30 45 60 75 80 85 90 95 96 97 98 99 100  *
Down Thresholds(%) : 100 99 98 97 96 95 90 85 80 75 60 45 30 15 0  *
IGP Update Pending : No
Next Update         : N/A
No Neighbors.
-------------------------------------------------------------------------------
```

```
Interface : m160
-------------------------------------------------------------------------------
Interface         : m160
Port ID           : 3/2/1
Admin State       : Up                   Oper State        : Up
Active Sessions   : 218                  Active Resvs      : 0
Total Sessions    : 517
Subscription      : 1000 %               Port Speed        : 100 Mbps
Total BW          : 1000 Mbps            Aggregate         : Dsabl
Hello Interval    : 3000 ms              Hello Timeouts    : 0
Authentication    : Disabled
Auth Rx Seq Num   : n/a                  Auth Key Id       : n/a
Auth Tx Seq Num   : n/a                  Auth Win Size     : n/a
Refresh Reduc.    : Enabled              Reliable Deli.    : Disabled
Bfd Enabled       : No                   Graceful Shut.    : Disabled
ImplicitNullLabel : Disabled*

Percent Link Bandwidth for Class Types*
Link Bw CT0       : 100                  Link Bw CT4       : 0
Link Bw CT1       : 0                    Link Bw CT5       : 0
Link Bw CT2       : 0                    Link Bw CT6       : 0
Link Bw CT3       : 0                    Link Bw CT7       : 0

Bandwidth Constraints for Class Types (Kbps)
BC0               : 1000000              BC4               : 0
BC1               : 0                    BC5               : 0
BC2               : 0                    BC6               : 0
BC3               : 0                    BC7               : 0

Bandwidth for TE Class Types (Kbps)
TE0->  Resv. Bw   : 0                    Unresv. Bw        : 1000000
TE1->  Resv. Bw   : 0                    Unresv. Bw        : 1000000
TE2->  Resv. Bw   : 0                    Unresv. Bw        : 1000000
TE3->  Resv. Bw   : 0                    Unresv. Bw        : 1000000
TE4->  Resv. Bw   : 0                    Unresv. Bw        : 1000000
TE5->  Resv. Bw   : 0                    Unresv. Bw        : 1000000
TE6->  Resv. Bw   : 0                    Unresv. Bw        : 1000000
TE7->  Resv. Bw   : 0                    Unresv. Bw        : 1000000

IGP Update
Up Thresholds(%)   : 0 15 30 45 60 75 80 85 90 95 96 97 98 99 100  *
Down Thresholds(%) : 100 99 98 97 96 95 90 85 80 75 60 45 30 15 0  *
IGP Update Pending : No
Next Update        : N/A
Neighbors      : 10.100.30.20
* indicates inherited values
===============================================================================
*A:SRU4>show>router>rsvp#
```

neighbor

Syntax **neighbor** [*ip-address*] [**detail**]

Context show>router>rsvp

Description This command shows neighbor information.

Parameters *ip-address* — Displays RSVP information about the specified IP address.

detail — Displays detailed information.

session

Syntax **session** *session-type* [**from** *ip-address* **| to** *ip-address***| lsp-name** *name*] [**status** {**up | down**}] [**detail**]

Context show>router>rsvp

Description This command shows RSVP session information.

Parameters **session** *session-type* — Specifies the session type.

Values originate, transit, terminate, detour, detour-transit, detour-terminate, bypass-tunnel

from *ip-address* — Specifies the IP address of the originating router.

to *ip-address* — Specifies the IP address of the egress router.

lsp-name *name* — Specifies the name of the LSP used in the path.

status up — Specifies to display a session that is operationally up.

status down — Specifies to display a session that is operationally down.

detail — Displays detailed information.

Output **RSVP Session Output —** The following table describers RSVP session output fields.

Label	Description
`From`	The IP address of the originating router.
`To`	The IP address of the egress router.
`Tunnel ID`	The IP address of the tunnel's ingress node supporting this RSVP session.
`LSP ID`	The ID assigned by the agent to this RSVP session.
`Name`	The administrative name assigned to the RSVP session by the agent.
`State`	`Down` — The operational state of this RSVP session is down. `Up` — The operational state of this RSVP session is up.

Sample Output

```
*A:SRU4>show>router>rsvp#   session
===============================================================================
RSVP Sessions
===============================================================================
From            To              Tunnel LSP   Name                          State
                                ID     ID
-------------------------------------------------------------------------------
```

```
110.20.1.5      110.20.1.4      18     27648 b4-1::b4-1                   Up
110.20.1.5      110.20.1.4      1      37902 gsr::gsr                     Up
110.20.1.5      10.20.1.22      11     53760 to_10_20_1_22_cspf::to_10_2* Up
110.20.1.4      10.20.1.20      146    17920 to_10_20_1_20_cspf_3::to_10* Up
110.20.1.4      10.20.1.20      145    34816 to_10_20_1_20_cspf_2::to_10* Up
110.20.1.4      10.20.1.20      147    45056 to_10_20_1_20_cspf_4::to_10* Up
110.20.1.4      10.20.1.20      148    6656  to_10_20_1_20_cspf_5::to_10* Up
110.20.1.4      10.20.1.20      149    58880 to_10_20_1_20_cspf_6::to_10* Up
110.20.1.4      10.20.1.20      150    13312 to_10_20_1_20_cspf_7::to_10* Up
110.20.1.4      10.20.1.20      152    40448 to_10_20_1_20_cspf_9::to_10* Up
110.20.1.4      10.20.1.20      154    27648 to_10_20_1_20_cspf_11::to_1* Up
110.20.1.4      10.20.1.20      155    12288 to_10_20_1_20_cspf_12::to_1* Up
110.20.1.4      10.20.1.20      151    46080 to_10_20_1_20_cspf_8::to_10* Up
110.20.1.4      10.20.1.20      153    512   to_10_20_1_20_cspf_10::to_1* Up
110.20.1.4      10.20.1.22      164    62464 to_10_20_1_22_cspf_2::to_10* Up
110.20.1.4      10.20.1.20      156    37888 to_10_20_1_20_cspf_13::to_1* Up
110.20.1.4      10.20.1.20      157    24064 to_10_20_1_20_cspf_14::to_1* Up
110.20.1.4      10.20.1.20      158    19968 to_10_20_1_20_cspf_15::to_1* Up
110.20.1.4      10.20.1.20      161    59904 to_10_20_1_20_cspf_18::to_1* Up
...
110.20.1.3      110.20.1.4      54     23088 to_110_20_1_4_cspf_4::to_11* Up
-------------------------------------------------------------------------------
Sessions : 1976
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>show>router>rsvp#


A:ALA-12# show router rsvp session lsp-name A_C_2::A_C_2 status up
===============================================================================
RSVP Sessions
===============================================================================
From            To              Tunnel LSP   Name                         State
                                ID     ID
-------------------------------------------------------------------------------
10.20.1.1       10.20.1.3       2      40    A_C_2::A_C_2                 Up
-------------------------------------------------------------------------------
Sessions : 1
===============================================================================
A:ALA-12#


*A:SRU4>show>router>rsvp#   session detail
===============================================================================
RSVP Sessions (Detailed)
===============================================================================
-------------------------------------------------------------------------------
LSP : b4-1::b4-1
-------------------------------------------------------------------------------
From            : 110.20.1.5            To              : 110.20.1.4
Tunnel ID       : 18                    LSP ID          : 27648
Style           : FF                    State           : Up
Session Type    : Terminate
In Interface    : 3/2/1                 Out Interface   : n/a
In Label        : 131071                Out Label       : n/a
Previous Hop    : 10.100.30.20          Next Hop        : n/a
SetupPriority   : 7                     Hold Priority   : 0
Class Type      : 0
SubGrpOrig ID   : 0                     SubGrpOrig Addr: 0.0.0.0
P2MP ID         : 0
```

```
Path Recd      : 7497                  Path Sent      : 0
Resv Recd      : 0                     Resv Sent      : 1757

Summary messages:
SPath Recd     : 0                     SPath Sent     : 0
SResv Recd     : 0                     SResv Sent     : 0
-------------------------------------------------------------------------------
LSP : gsr::gsr
-------------------------------------------------------------------------------
From           : 110.20.1.5            To             : 110.20.1.4
Tunnel ID      : 1                     LSP ID         : 37902
Style          : FF                    State          : Up
Session Type   : Terminate
In Interface   : 3/2/7                 Out Interface  : n/a
In Label       : 128547                Out Label      : n/a
Previous Hop   : 160.60.60.2           Next Hop       : n/a
SetupPriority  : 7                     Hold Priority  : 0
Class Type     : 0
SubGrpOrig ID  : 0                     SubGrpOrig Addr: 0.0.0.0
P2MP ID        : 0

Path Recd      : 5225                  Path Sent      : 0
Resv Recd      : 0                     Resv Sent      : 1741

Summary messages:
SPath Recd     : 0                     SPath Sent     : 0
SResv Recd     : 0                     SResv Sent     : 0
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
From           : 110.20.1.3            To             : 110.20.1.4
Tunnel ID      : 54                    LSP ID         : 23088
Style          : SE                    State          : Up
Session Type   : Terminate
In Interface   : aps-1                 Out Interface  : n/a
In Label       : 130409                Out Label      : n/a
Previous Hop   : 104.104.0.3           Next Hop       : n/a
SetupPriority  : 7                     Hold Priority  : 0
Class Type     : 0
SubGrpOrig ID  : 0                     SubGrpOrig Addr: 0.0.0.0
P2MP ID        : 0

Path Recd      : 1                     Path Sent      : 0
Resv Recd      : 0                     Resv Sent      : 1

Summary messages:
SPath Recd     : 840                   SPath Sent     : 0
SResv Recd     : 0                     SResv Sent     : 850
===============================================================================
*A:SRU4>show>router


*A:Dut-B# show router rsvp session detour detail
==============================================================================
RSVP Sessions (Detailed)
==============================================================================
LSP : tof919::1_detour
------------------------------------------------------------------------------
From           : 10.20.1.2             To             : 10.20.1.4
Tunnel ID      : 919                   LSP ID         : 15441
Style          : SE                    State          : Up
```

```
Session Type   : Originate (Detour)
In Interface   : n/a                    Out Interface  : 1/1/2:1
In Label       : n/a                    Out Label      : 129865
Previous Hop   : n/a                    Next Hop       : 10.10.101.4
SetupPriority  : 4                      Hold Priority  : 4
Class Type     : 5
SugGrpOrig ID  : 0                      SubGrpOrig Addr: 0.0.0.0
P2MP ID        : 0

Path Recd      : 0                      Path Sent      : 106
Resv Recd      : 113                    Resv Sent      : 0

Summary messages:
SPath Recd     : 0                      SPath Sent     : 0
SResv Recd     : 0                      SResv Sent     : 0
===============================================================================
*A:Dut-B#


*A:Dut-C# show router mpls lsp transit detail
===============================================================================
MPLS LSPs (Transit) (Detail)
-------------------------------------------------------------------------------
LSP tof1::sec2
-------------------------------------------------------------------------------
From                 : 10.20.1.2             To             : 10.20.1.4
State                : Up
SetupPriority        : 5                     Hold Priority : 5
Class Type           : 5
In Interface         : lag-1:0               In Label       : 131068
Out Interface        : 2/1/2                 Out Label      : 131068
Previous Hop         : 10.10.12.2            Next Hop       : 10.10.11.4
Reserved BW          : 1000 Kbps
===============================================================================
*A:Dut-C#


*A:Dut-B# show router rsvp session detour-terminate detail
===============================================================================
RSVP Sessions (Detailed)
===============================================================================
LSP : tof878::1_detour
-------------------------------------------------------------------------------
From           : 10.20.1.2              To             : 10.20.1.4
Tunnel ID      : 878                    LSP ID         : 14929
Style          : SE                     State          : Up
Session Type   : Terminate (Detour)
In Interface   : lag-1:0                Out Interface  : 1/1/2:8
In Label       : 131069                 Out Label      : 127951
Previous Hop   : 10.10.12.3             Next Hop       : 10.10.108.4
SetupPriority  : 4                      Hold Priority  : 4
Class Type     : 5
SugGrpOrig ID  : 0                      SubGrpOrig Addr: 0.0.0.0
P2MP ID        : 0

Path Recd      : 128                    Path Sent      : 0
Resv Recd      : 125                    Resv Sent      : 124

Summary messages:
SPath Recd     : 0                      SPath Sent     : 0
SResv Recd     : 0                      SResv Sent     : 0
```

```
===============================================================================
*A:Dut-B#

*A:Dut-B# show router rsvp session bypass-tunnel detail
===============================================================================
RSVP Sessions (Detailed)
===============================================================================
LSP : bypass-link10.10.108.4
-------------------------------------------------------------------------------
From            : 10.20.1.2             To              : 10.10.109.4
Tunnel ID       : 4003                  LSP ID          : 6
Style           : FF                    State           : Up
Session Type    : Bypass Tunnel
In Interface    : n/a                   Out Interface   : 1/1/2:9
In Label        : n/a                   Out Label       : 124069
Previous Hop    : n/a                   Next Hop        : 10.10.109.4
SetupPriority   : 7                     Hold Priority   : 0
Class Type      : 0
SugGrpOrig ID   : 0                     SubGrpOrig Addr: 0.0.0.0
P2MP ID         : 0

Path Recd       : 0                     Path Sent       : 3
Resv Recd       : 4                     Resv Sent       : 0

Summary messages:
SPath Recd      : 0                     SPath Sent      : 0
SResv Recd      : 0                     SResv Sent      : 0
===============================================================================
*A:Dut-B#


*A:Dut-B# show router rsvp session detour detail
===============================================================================
RSVP Sessions (Detailed)
-------------------------------------------------------------------------------
LSP : tof919::1_detour
-------------------------------------------------------------------------------
From            : 10.20.1.2             To              : 10.20.1.4
Tunnel ID       : 919                   LSP ID          : 15441
Style           : SE                    State           : Up
Session Type    : Originate (Detour)
In Interface    : n/a                   Out Interface   : 1/1/2:1
In Label        : n/a                   Out Label       : 129865
Previous Hop    : n/a                   Next Hop        : 10.10.101.4
SetupPriority   : 4                     Hold Priority   : 4
Class Type      : 5
SugGrpOrig ID   : 0                     SubGrpOrig Addr: 0.0.0.0
P2MP ID         : 0

Path Recd       : 0                     Path Sent       : 106
Resv Recd       : 113                   Resv Sent       : 0

Summary messages:
SPath Recd      : 0                     SPath Sent      : 0
SResv Recd      : 0                     SResv Sent      : 0
===============================================================================
*A:Dut-B#


*A:Dut-B# show router rsvp session detour-transit detail
===============================================================================
```

```
RSVP Sessions (Detailed)
-------------------------------------------------------------------------------
LSP : tof919::1_detour
-------------------------------------------------------------------------------
From           : 10.20.1.2              To             : 10.20.1.4
Tunnel ID      : 919                    LSP ID         : 15441
Style          : SE                     State          : Up
Session Type   : Transit (Detour)
In Interface   : lag-1:0                Out Interface  : 1/1/2:6
In Label       : 131071                 Out Label      : 127952
Previous Hop   : 10.10.12.3             Next Hop       : 10.10.106.4
SetupPriority  : 4                      Hold Priority  : 4
Class Type     : 5
SugGrpOrig ID  : 0                      SubGrpOrig Addr: 0.0.0.0
P2MP ID        : 0

Path Recd      : 119                    Path Sent      : 123
Resv Recd      : 121                    Resv Sent      : 120

Summary messages:
SPath Recd     : 0                      SPath Sent     : 0
SResv Recd     : 0                      SResv Sent     : 0
===============================================================================
*A:Dut-B#


*A:Dut-B# show router rsvp session detour-terminate detail
===============================================================================
RSVP Sessions (Detailed)
-------------------------------------------------------------------------------
LSP : tof878::1_detour
-------------------------------------------------------------------------------
From           : 10.20.1.2              To             : 10.20.1.4
Tunnel ID      : 878                    LSP ID         : 14929
Style          : SE                     State          : Up
Session Type   : Terminate (Detour)
In Interface   : lag-1:0                Out Interface  : 1/1/2:8
In Label       : 131069                 Out Label      : 127951
Previous Hop   : 10.10.12.3             Next Hop       : 10.10.108.4
SetupPriority  : 4                      Hold Priority  : 4
Class Type     : 5
SugGrpOrig ID  : 0                      SubGrpOrig Addr: 0.0.0.0
P2MP ID        : 0

Path Recd      : 128                    Path Sent      : 0
Resv Recd      : 125                    Resv Sent      : 124

Summary messages:
SPath Recd     : 0                      SPath Sent     : 0
SResv Recd     : 0                      SResv Sent     : 0
===============================================================================
*A:Dut-B#


*A:Dut-B# show router rsvp session bypass-tunnel detail
===============================================================================
RSVP Sessions (Detailed)
-------------------------------------------------------------------------------
LSP : bypass-link10.10.108.4
-------------------------------------------------------------------------------
From           : 10.20.1.2              To             : 10.10.109.4
```

```
Tunnel ID      : 4003                 LSP ID         : 6
Style          : FF                   State          : Up
Session Type   : Bypass Tunnel
In Interface   : n/a                  Out Interface  : 1/1/2:9
In Label       : n/a                  Out Label      : 124069
Previous Hop   : n/a                  Next Hop       : 10.10.109.4
SetupPriority  : 7                    Hold Priority  : 0
Class Type     : 0
SugGrpOrig ID  : 0                    SubGrpOrig Addr: 0.0.0.0
P2MP ID        : 0

Path Recd      : 0                    Path Sent      : 3
Resv Recd      : 4                    Resv Sent      : 0

Summary messages:
SPath Recd     : 0                    SPath Sent     : 0
SResv Recd     : 0                    SResv Sent     : 0
===============================================================================
*A:Dut-B#
```

statistics

Syntax **statistics**

Context show>router>rsvp

Description This command displays global statistics in the RSVP instance.

Output **RSVP Statistics Output —** The following table describes RSVP statistics output fields.

Label	Description
PATH Timeouts	The total number of path timeouts.
RESV Timeouts	The total number of RESV timeouts.

Sample Output

```
*A:SRU4>show>router>rsvp# statistics
===============================================================================
RSVP Global Statistics
===============================================================================
PATH Timeouts      : 1026               RESV Timeouts      : 182
===============================================================================
*A:SRU4>show>router>rsvp#
```

status

Syntax **rsvp status**

Context show>router>rsvp

Description This command displays RSVP status.

Output **RSVP Status —** The following table describes RSVP status output fields.

Label	Description
Admin Status	Down — RSVP is administratively disabled.
	Up — RSVP is administratively enabled.
Oper Status	Down — RSVP is operationally down.
	Up — RSVP is operationally up.
Keep Multiplier	Displays the **keep-multiplier** *number* used by RSVP to declare that a reservation is down or the neighbor is down.
Refresh Time	Displays the **refresh-time** interval, in seconds, between the successive Path and Resv refresh messages.
Message Pacing	Enabled — RSVP messages, specified in the **max-burst** command, are sent in a configured interval, specified in the **period** command.

Label	Description (Continued)
	`Disabled` — Message pacing is disabled. RSVP message transmission is not regulated.
`Pacing Period`	Displays the time interval, in milliseconds, when the router can send the specified number of RSVP messages specified in the **rsvp max-burst** command.
`Max Packet Burst`	Displays the maximum number of RSVP messages that are sent in the specified period under normal operating conditions.
`Soft Preemption Timer`	Displays the time, in seconds, a node holds on to a reservation for which it has triggered the soft preemption procedur.
`Rapid Retransmit`	Displays the value of the rapid retransmission interval.
`Rapid Retry Limit`	Displays the rapid retry limit.
`Graceful Shutdown`	Specifies whether graceful shutdown of the RSVP node is enabled.

Sample Output

```
*A:SRU4>show>router>rsvp# status
===============================================================================
RSVP Status
===============================================================================
Admin Status       : Up                  Oper Status        : Up
Keep Multiplier    : 3                   Refresh Time       : 30 sec
Message Pacing     : Disabled            Pacing Period      : 100 msec
Max Packet Burst   : 650 msgs            Refresh Bypass     : Disabled
Rapid Retransmit   : 100 hmsec           Rapid Retry Limit  : 3
Graceful Shutdown  : Disabled            SoftPreemptionTimer: 300 sec
Implicit Null Label: Disabled
DiffServTE AdmModel: Basic
Percent Link Bw CT0: 100                 Percent Link Bw CT4: 0
Percent Link Bw CT1: 0                   Percent Link Bw CT5: 0
Percent Link Bw CT2: 0                   Percent Link Bw CT6: 0
Percent Link Bw CT3: 0                   Percent Link Bw CT7: 0
TE0 -> Class Type  : 0                   Priority           : 0
TE1 -> Class Type  : 0                   Priority           : 1
TE2 -> Class Type  : 0                   Priority           : 2
TE3 -> Class Type  : 0                   Priority           : 3
TE4 -> Class Type  : 0                   Priority           : 4
TE5 -> Class Type  : 0                   Priority           : 5
TE6 -> Class Type  : 0                   Priority           : 6
TE7 -> Class Type  : 0                   Priority           : 7
IgpThresholdUpdate : Disabled
Up Thresholds(%)   : 0 15 30 45 60 75 80 85 90 95 96 97 98 99 100
Down Thresholds(%) : 100 99 98 97 96 95 90 85 80 75 60 45 30 15 0
Update Timer       : N/A
Update on CAC Fail : Disabled
===============================================================================
*A:SRU4>show>router>rsvp#
```

Tools Commands

cspf

Syntax **cspf to** *ip-addr* [**from** *ip-addr*] [**bandwidth** *bandwidth*] [**include-bitmap** *bitmap*] [**exclude-bitmap** *bitmap*] [**hop-limit** *limit*] [**exclude-address** *excl-addr* [*excl-addr*...(up to 8 max)]] [**use-te-metric**] [**strict-srlg**] [**srlg-group** *grp-id...*(up to 8 max)] [**exclude-node** *excl-node-id* [*excl-node-id*..(up to 8 max)]] [**skip-interface** *interface-name*] [**ds-class-type** *class-type*] [**cspf-reqtype** *req-type*] [**least-fill-min-thd** *thd*] [**setup-priority** *val*] [**hold-priority** *val*]

Context tools>perform>router>mpls

Description This command computes a CSPF path with specified user constraints.

Default none

Parameters **to** *ip-addr* — Specify the destination IP address.

from *ip-addr* — Specify the originating IP address.

bandwidth *bandwidth* — Specifies the amount of bandwidth in mega-bits per second (Mbps) to be reserved.

include-bitmap *bitmap* — Specifies to include a bit-map that specifies a list of admin groups that should be included during setup.

exclude-bitmap *bitmap* — Specifies to exclude a bit-map that specifies a list of admin groups that should be included during setup.

hop-limit *limit* — Specifies the total number of hops a detour LSP can take before merging back onto the main LSP path.

exclude-address *ip-addr* — Specifies IP addresses, up to 8, that should be included during setup.

use-te-metric — Specifies the use of the traffic engineering metric used on the interface.

strict-srlg — Specifies whether to associate the LSP with a bypass or signal a detour if a bypass or detour satisfies all other constraints except the SRLG constraints.

srlg-group *grp-id* — Specifies up to 8 Shared Risk Loss Groups (SRLGs). An SRLG group represents a set of interfaces which could be subject to the same failures or defects and thus share the same risk of failing.

Values 0 — 4294967295

exclude-node *excl-node-id* — specifies a list of address that should be excluded when this LSP is setup.

skip-interface *interface-name* — Specifies an interface name that should be skipped during setup.

ds-class-type *class-type* — Specifies the class type (CT) associated with this LSP.

Values 0 — 7

cspf-reqtype *req-type* — Specifies the req. type.

Values all, random, least-fill

least-fill-min-thd *thd* **—** Specifies whether the use of the least-fill path selection method for the computation of the path of this LSP is enabled.

Values 1 — 100

setup-priority *val* **—** Specifies the setup priority to use when insufficient bandwidth is available to setup an LSP.

Values 0 — 7

hold-priority *val* **—** Specifies the hold priority value to use when insufficient bandwidth is available to setup an LSP.

Values 0 — 7

resignal

Syntax **resignal** {**lsp** *lsp-name* **path** *path-name* **| delay** *minutes*}
resignal {**p2mp-lsp** *p2mp-lsp-name* **p2mp-instance** *p2mp-instance-name* **| p2mp-delay** *p2mp-minutes*}

Context tools>perform>router>mpls

Description This command resignals a specific LSP path. The *minutes* parameter configures the global timer or all LSPs for resignal. If only lsp-name and path-name are provided, the LSP will be resignaled immediately.

Parameters *lsp-name* — Specifies an existing LSP name to resignal.

path-name — Specifies an existing path name to resignal.

delay *minutes* **—** Configures the global timer or all LSPs to resignal.

p2mp-lsp *p2mp-lsp-name* **—** Specifies an existing point-to-multipoint LSP name.

p2mp-instance *p2mp-instance-name* **—** Specifies a name that identifies the P2MP LSP instance

p2mp-delay *p2mp-minutes* **—** Specifies the delay time, in minutes.

Values 0 — 60

te-lspinfo

Syntax **te-lspinfo** [**endpoint** *ip-address*] [**sender** *ip-address*] [**lspid** *lsp-id*] [**detail**] [**p2p |** ***p2p-tid*** *tunnel-id*]
te-lspinfo [**endpoint** *ip-address*] [**sender** *ip-address*] [**lspid** *lsp-id*] [**detail**] [**p2p | p2p-tid** *tunnel-id*]{ [**phops**] [**nhops**] [**s2l** *ip-address*] } }

Context tools>dump>router>mpls

Description This command displays TE LSP information for MPLS.

Default none

Sample Output

```
B:Dut-R# tools dump router mpls te-lspinfo
Key P2P: Session(10.10.3.2, 201, 3.3.3.3) Sender(3.3.3.3, 2) PHOP(10.10.3.1), Flags
0x0

Key P2P: Session(10.10.3.1, 1035, 4.4.4.4) Sender(4.4.4.4, 22) PHOP(10.10.11.2),
Flags 0x0

Key P2MP: Session(0.0.0.0, 1, 4.4.4.4) Sender(4.4.4.4, 52226) PHOP(0.0.0.0) Flags
0x10
  S2L [1] Key: endPoint to 2.2.2.2 subGroupId - 1 subGroupOrigId - 4.4.4.4
  S2L [2] Key: endPoint to 10.10.2.2 subGroupId - 3 subGroupOrigId - 4.4.4.4
  S2L [3] Key: endPoint to 10.10.13.2 subGroupId - 4 subGroupOrigId - 4.4.4.4

Key P2MP: Session(0.0.0.0, 2, 4.4.4.4) Sender(4.4.4.4, 51714) PHOP(0.0.0.0) Flags
0x10
  S2L [1] Key: endPoint to 2.2.2.2 subGroupId - 1 subGroupOrigId - 4.4.4.4
  S2L [2] Key: endPoint to 10.10.2.2 subGroupId - 3 subGroupOrigId - 4.4.4.4
  S2L [3] Key: endPoint to 10.10.13.2 subGroupId - 4 subGroupOrigId - 4.4.4.4

Key P2MP: Session(0.0.0.0, 3, 4.4.4.4) Sender(4.4.4.4, 53250) PHOP(0.0.0.0) Flags
0x10

*A:Dut-T# tools dump router mpls te-lspinfo p2mp-tid 102 nhops

  Key P2MP: Session(0.0.0.0, 102, 4.4.4.4) Sender(4.4.4.4, 3074) PHOP(0.0.0.0) Flags
0x10
  --------------------------------------------------------------------------
        List of NEXT HOPS
  --------------------------------------------------------------------------

  NextHop [1] =>
  Key: Nhop - isFrr 0, outIf 0, NextHop 0.0.0.0 label - 128843  global Instance 0 is
Leaf node
        ----------------------------------------------------------------------
        Primary NHLFE => outLabel - 0 and NextHop - 0.0.0.0, outIf 0 (0)
                Port(NONE) NhIdx 0, ProtNhIdx 0, NumS2L 1
                ProtectInstance - 0, ProtectGroup 0
        POP
        No Backup NHLFEs for this Ltn entry
  Mid List :    3428 numS2Ls - 1 (Primary MID),

  NextHop [2] =>
  Key: Nhop - isFrr 0, outIf 3, NextHop 10.10.13.2 label - 128806  global Instance -
48747
        ----------------------------------------------------------------------
        Primary NHLFE => outLabel - 128806 and NextHop - 10.10.13.2, outIf 3 (126)
                Port(9/1/1) NhIdx 4322, ProtNhIdx 2275, NumS2L 1
                ProtectInstance - 1, ProtectGroup 126
        SWAP
        Backup NHLFE => outLabel - 130223 and NextHop - 10.10.3.2, outIf 5 (124)
                Port(9/2/3) outPushLabel 128806, NhIdx 5469, ProtNhIdx 0, NumS2L 1
  Mid List :    3428 numS2Ls - 1 (Primary MID),

  NextHop [3] =>
  Key: Nhop - isFrr 0, outIf 4, NextHop 10.10.2.2 label - 128836  global Instance -
48974
        ----------------------------------------------------------------------
        Primary NHLFE => outLabel - 128836 and NextHop - 10.10.2.2, outIf 4 (125)
                Port(lag-1) NhIdx 4292, ProtNhIdx 2245, NumS2L 2
```

```
                ProtectInstance - 1, ProtectGroup 125
        SWAP
        Backup NHLFE => outLabel - 130223 and NextHop - 10.10.3.2, outIf 5 (124)
                Port(9/2/3) outPushLabel 128836, NhIdx 5659, ProtNhIdx 0, NumS2L 2
  Mid List :    3428 numS2Ls - 1 (Primary MID),   3471 numS2Ls - 1 (Backup MID),

  S2L [1] Key: endPoint to 2.2.2.2 subGroupId - 1 subGroupOrigId - 4.4.4.4
  S2L [2] Key: endPoint to 3.3.3.3 subGroupId - 2 subGroupOrigId - 4.4.4.4
  S2L [3] Key: endPoint to 10.10.2.2 subGroupId - 3 subGroupOrigId - 4.4.4.4
  S2L [4] Key: endPoint to 10.10.13.2 subGroupId - 4 subGroupOrigId - 4.4.4.4

  Total TeLspInfo Count    : 1
```

trap-suppress

Syntax **trap-suppress** *number-of-traps time-interval*

Context tools>perform>router>mpls

Description This command modifies thresholds for trap suppression. The *time-interval* parameter is used to suppress traps after a certain number of traps have been raised within a period. By executing this command, there will be no more than *number-of-traps* within *time-interval*.

Parameters *number-of-traps* — Specifies to suppress the number of traps raised within a period.

Values 100 — 1000, in multiples of 100

time-interval — Specifies to suppress a certain number of traps raised within a period.

Values 1 — 300

tunnel-interface

Syntax [**no**] **tunnel-interface rsvp-p2mp** *lsp-name* [**sender** *sender-address*]

Context config>router
config>router>igmp

Description This command creates a tunnel interface associated with an RSVP P2MP LSP. IPv4 multicast packets are forwarded over the P2MP LSP at the ingress LER based on a static join configuration of the multicast group against the tunnel interface associated with the originating P2MP LSP. At the egress LER, packets of a multicast group are received from the P2MP LSP via a static assignment of the specific <S,G> to the tunnel interface associated with a terminating LSP.

At ingress LER, the tunnel interface identifier consists of a string of characters representing the LSP name for the RSVP P2MP LSP. The user can create one or more tunnel interfaces and associate each to a different RSVP P2MP LSP.

At egress LER, the tunnel interface identifier consists of a couple of string of characters representing the LSP name for the RSVP P2MP LSP followed by the system address of the ingress LER. The LSP name must correspond to a P2MP LSP name configured by the user at the ingress LER. The LSP name string must not contain "::" (two :s) nor contain a ":" (single ":") at the end of the LSP name. However, a ":" (single ":") can appear anywhere in the string except at the end of the name.

Default none

Parameters **rsvp-p2mp** *lsp-name* — Specifies the LSP. The LSP name can be up to 32 characters long and must be unique.

sender *sender-address* — Specifies system address of the ingress LER for the P2MP RSVP LSP.

update-path

Syntax **update-path** {**lsp** *lsp-name* **path** *current-path-name* **new-path** *new-path-name*}

Context tools>perform>router>mpls

Description This command enables you to instruct MPLS to replace the path of a primary or secondary LSP. The primary or secondary LSP path is indirectly identified via the *current-path-name* value. The same path name cannot be used more than once in a given LSP name.

This command applies to both CSPF LSP and to a non-CSPF LSP. This command will only work when the specified *current-path-name* has the adaptive option enabled. The adaptive option can be enabled at the LSP level or the path level.

The new path must have been configured in the CLI or provided via SNMP. The CLI command for entering the path is

configure router mpls path *path-name*

The command fails if any of the following conditions exist:

- The specified *current-path-name* of this LSP does not have the adaptive option enabled.
- The specified *new-path-name* value does not correspond to a previously defined path.
- The specified *new-path-name* value exists but is being used by any path of the same LSP, including this one.

When you execute this command, MPLS performs the following procedures:

- MPLS performs a single MBB attempt to move the LSP path to the new path.
- If the MBB is successful, MPLS updates the new path
  - MPLS writes the corresponding NHLFE in the data path if this path is the current backup path for the primary.
  - If the current path is the active LSP path, it will update the path, write the new NHLFE in the data path that will cause traffic to switch to the new path.
- If the MBB is not successful, the path retains it current value.
- The update-path MBB has the same priority as the manual re-signal MBB.

Clear Commands

interface

Syntax **interface** *ip-int-name* [**statistics**]

Context clear>router>mpls

Description This command resets or clears statistics for MPLS interfaces.

Parameters *ip-int-name* — The name of an existing IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

statistics — This parameter clears only statistics.

lsp

Syntax **lsp** *lsp-name*

Context clear>router>mpls

Description This command resets and restarts an LSP.

Parameters *lsp-name* — The name of the LSP to clear up to 64 characters in length.

ingress-stats

Syntax **ingress-statistics**

Context clear>router>mpls

Description This command provides the context for the user to enter the LSP names for the purpose of enabling ingress data path statistics at the terminating node of the LSP (for example, egress LER).

Default none

lsp-egress-stats

Syntax **lsp-egress-stats**
lsp-egress-stats *lsp-name*

Context clear>router>mpls

Description This command clears MPLS LSP egress statistics information.

lsp-ingress-stats

Syntax **lsp-ingress-stats**
lsp-ingress-stats *ip-address* **lsp** *lsp-name*

Context clear>router>mpls

Description This command clears MPLS LSP ingress statistics information.

interface

Syntax **interface** *ip-int-name* **statistics**

Context clear>router>rsvp

Description This command resets or clears statistics for an RSVP interface.

Parameters *ip-int-name* — The name of the IP interface to clear. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

statistics — This parameter clears only statistics.

statistics

Syntax **statistics**

Context clear>router>rsvp

Description This command clears global statistics for the RSVP instance, for example, clears **path** and **resv time-out** counters.

Debug Commands

mpls

Syntax **mpls** [**lsp** *lsp-name*] [**sender** *source-address*] [**endpoint** *endpoint-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**interface** *ip-int-name*]
no mpls

Context debug>router

Description This command enables and configures debugging for MPLS.

Parameters **lsp** *lsp-name* — Name that identifies the LSP. The LSP name can be up to 32 characters long and must be unique.

sender *source-address* — The system IP address of the sender.

endpoint *endpoint-address* — The far-end system IP address.

tunnel-id *tunnel-id* — The MPLS SDP ID.

Values 0 — 4294967295

lsp-id *lsp-id* — The LSP ID.

Values 1 — 65535

interface *ip-int-name* — Name that identifies the interface. The interface name can be up to 32 characters long and must be unique. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

event

Syntax [**no**] **event**

Context debug>router>mpls
debug>router>rsvp

Description This command enables debugging for specific events.

The **no** form of the command disables the debugging.

all

Syntax **all** [**detail**]
no all

Context debug>router>mpls>event
debug>router>rsvp>event

Description This command debugs all events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about all events.

frr

Syntax **frr** [**detail**]
no frr

Context debug>router>mpls>event

Description This command debugs fast re-route events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about re-route events.

iom

Syntax **iom** [**detail**]
no iom

Context debug>router>mpls>event

Description This command debugs MPLS IOM events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about MPLS IOM events.

lsp-setup

Syntax **lsp-setup** [**detail**]
no lsp-setup

Context debug>router>mpls>event

Description This command debugs LSP setup events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about LSP setup events.

mbb

Syntax **mbb** [**detail**]
no mbb

Context debug>router>mpls>event

Description This command debugs the state of the most recent invocation of the make-before-break (MBB) functionality.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about MBB events.

misc

Syntax **misc** [**detail**]
no misc

Context debug>router>mpls>event
debug>router>rsvp>event

Description This command debugs miscellaneous events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about miscellaneous events.

p2mp-lsp-ping

Syntax **p2mp-lsp-ping** *lsp-name* [**p2mp-instance** *instance-name* [**s2l-dest-addr** *ip-address*…[*ip-address*...up-to-5]]] [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *octets*] [**ttl** *label-ttl*] [**timeout** *timeout*] [**detail**]

Context oam

Description This command performs an in-band connectivity test for an RSVP P2MP LSP.

The echo request message is sent on the active P2MP instance and is replicated in the data path over all branches of the P2MP LSP instance. By default, all egress LER nodes that are leaves of the P2MP LSP instance will reply to the echo request message.

You can reduce the scope of the echo reply messages by explicitly entering a list of addresses for the egress LER nodes that are required to reply. You can specify a maximum of five addresses in a single run of the p2mp-lsp-ping command. An LER node is able to parse the list of Egress LER addresses and if its address is included, it will reply with an echo reply message.

The output of the command without the detail option provides a high-level summary of error codes and/or success codes received. The output of the command with the detail option shows a line for each replying node as in the output of the LSP ping for a P2P LSP.

The display will be delayed until all responses are received or the timer configured in the timeout parameter has expired. No other CLI commands can be entered while waiting for the display. A **^C** will abort the ping operation.

Parameters *lsp-name* — A name that identifies a P2MP LSP to ping. The LSP name can be up to 32 characters long.

p2mp-instance *instance-name* **—** Configures the name of the specific instance of the P2MP LSP to send the echo request.

Values The instance name can be up to 32 characters long.

s2l-dest-addr *instance-name…*[*ip-address*...up-to-5] **—** Specifies the list of egress LER system addresses that are required to reply to the LSP ping echo request message.

Values ipv4-address: a.b.c.d

fc *fc-name* **—** The fc parameter is used to indicate the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

The LSP-EXP mappings on the receive network interface controls the mapping back to the internal forwarding class used by the far-end 7750 SR that receives the message request. The egress mappings of the egress network interface on the far-end 7750 SR controls the forwarding class markings on the return reply message.

The LSP-EXP mappings on the receive network interface controls the mapping of the message reply back at the originating 7750 SR.

Default be

Values be, l2, af, l1, h2, ef, h1, nc

profile {**in | out**} **—** The profile of the LSP ping echo request message.

Default out

size *octets* — The MPLS echo request packet size in octets, expressed as a decimal integer. The request payload is padded with zeroes to the specified size.

Default 128 octets. The system sends the minimum packet size for an RSVP P2MP LSP.

Values 128-65535

ttl *label-ttl* — The TTL value for the MPLS label expressed as a decimal integer.

Default 255

Values 1-255

timeout *timeout* — The timeout parameter in seconds, expressed as a decimal integer. This value is used to override the default timeout value and is the amount of time that the router will wait for an echo reply message from all leaves of the P2MP LSP after sending the message request message. Upon the expiration of message timeout, the requesting router assumes that the missing replies will not be received. Any echo reply message received after the request times out will be silently discarded.

Default 10 seconds

Values 1-120

p2mp-lsp-trace

Syntax **p2mp-lsp-trace** *lsp-name* **p2mp-instance** *instance-name* **s2l-dest-addr** *ip-address* [**fc** *fc-name* [**profile** {**in** | **out**}]] [**size** *octets*] [**max-fail** *no-response-count*] [**probe-count** *probes-per-hop*] [**min-ttl** *min-label-ttl*]] [**max-ttl** *max-label-ttl*] [**timeout** *timeout*] [**interval** *interval*] [**detail**]

Context oam

Description This command discovers and displays the hop-by-hop path for a Source-to-Leaf (S2L) sub-LSP of an RSVP P2MP LSP.

The LSP trace capability allows the user to trace the path of a single S2L path of a P2MP LSP. Its operation is similar to that of the p2mp-lsp-ping but the sender of the echo reply request message includes the Downstream Mapping TLV to request the downstream branch information from a branch LSR or BUD LSR. The branch LSR or BUD LSR will then also include the Downstream Mapping TLV to report the information about the downstream braches of the P2MP LSP. An egress LER must not include this TLV in the echo response message.

The parameter probe-count operates in the same way as in LSP Trace on a P2P LSP. It represents the maximum number of probes sent per TTL value before giving up on receiving the echo reply message. If a response is received from the traced node before reaching the maximum number of probes, then no more probes are sent for the same TTL. The sender of the echo request then increments the TTL and uses the information it received in the Downstream Mapping TLV to start sending probes to the node downstream of the last node that replied. This continues until the egress LER for the traced S2L path replied.

Similar to the case of p2mp-lsp-ping, an LSP trace probe results on all egress LER nodes eventually receiving the echo request message but only the traced egress LER node will reply to the last probe.

Also any branch LSR node or BUD LSR node in the P2MP LSP tree may receive a copy of the echo request message with the TTL in the outer label expiring at this node. However, only a branch LSR or BUD LSR that has a downstream branch over which the traced egress LER is reachable will respond.

When a branch LSR or BUD LSR responds, it sets the B-flag in the downstream mapping TLV to indicate to the sender of the echo request message it has other branches for this LSP. A BUD LSR will also set the E-flag in the downstream mapping TLV to indicate to the sender of the echo request message that it is also an egress LER for the P2MP LSP when the traced Egress is reachable via a downstream branch. In this case, the return code must correspond to the LSR role and must code #8: “Label switched at stack-depth <RSC>”.

Parameters *lsp-name* — A name that identifies a P2MP LSP to ping. The LSP name can be up to 32 characters long.

p2mp-instance *instance-name* **—** Configures the name of the specific instance of the P2MP LSP to send the echo request.

Values The instance name can be up to 32 characters long.

s2l-dest-addr *instance-name…*[*ip-address*...up-to-5] **—** Specifies the egress LER system address of the S2L sub-LSP path which is being traced.

Values ipv4-address: a.b.c.d

fc *fc-name* **—** The fc parameter is used to indicate the forwarding class of the MPLS echo request packets. The actual forwarding class encoding is controlled by the network egress LSP-EXP mappings.

The LSP-EXP mappings on the receive network interface controls the mapping back to the internal forwarding class used by the far-end 7750 SR that receives the message request. The egress mappings of the egress network interface on the far-end 7750 SR controls the forwarding class markings on the return reply message.

The LSP-EXP mappings on the receive network interface controls the mapping of the message reply back at the originating 7750 SR.

Default be

Values be, l2, af, l1, h2, ef, h1, nc

profile {**in** | **out**} **—** The profile of the LSP trace echo request message.

Default out

size *octets* — The MPLS echo request packet size in octets, expressed as a decimal integer. The request payload is padded with zeroes to the specified size.

Default 128 octets. The system sends the minimum packet size for an RSVP P2MP LSP.

Values 128-65535

max-fail *no-response-count* — The maximum number of consecutive MPLS echo requests, expressed as a decimal integer that do not receive a reply before the trace operation fails for a given TTL.

Default 5

Values 1-255

min-ttl *min-label-ttl* — The minimum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer.

Default 1

Values 1-255

max-ttl *max-label-ttl* — The maximum TTL value in the MPLS label for the LSP trace test, expressed as a decimal integer.

Default 30

Values 1-255

probe-count *probes-per-hop* — The number of LSP trace echo request messages to send per TTL value.

Default 1

Values 1-10

timeout *timeout* — The timeout parameter in seconds expressed as a decimal integer. This value is used to override the default timeout value and is the amount of time that the router will wait for an echo reply message from all leaves of the P2MP LSP after sending the message request message. Upon the expiration of the message timeout, the requesting router assumes that the missing replies will not be received. Any echo reply message received after the request times out will be silently discarded.

Default 3

Values 1-60

interval *interval* — The interval parameter in seconds, expressed as a decimal integer. This parameter is used to override the default echo request message send interval and defines the minimum amount of time that must expire before the next echo request message is sent.

If the interval is set to 1 second, and the timeout value is set to 10 seconds, then the maximum time between message requests is 10 seconds and the minimum is 1 second. This depends upon the receipt of an echo reply message corresponding to the outstanding message request.

Default 1

Values 1-10

xc

Syntax **xc** [**detail**]
no xc

Context debug>router>mpls>event

Description This command debugs cross connect events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about cross connect events.

rsvp

Syntax [**lsp** *lsp-name*] [**sender** *source-address*] [**endpoint** *endpoint-address*] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*] [**interface** *ip-int-name*]
no rsvp

Context debug>router

Description This command enables and configures debugging for RSVP.

Parameters **lsp** *lsp-name* — Name that identifies the LSP. The LSP name can be up to 32 characters long and must be unique.

sender *source-address* — The system IP address of the sender.

endpoint *endpoint-address* — The far-end system IP address.

tunnel-id *tunnel-id* — The RSVP tunnel ID.

Values 0 — 4294967295

lsp-id *lsp-id* — The LSP ID.

Values 1 — 65535

interface *ip-int-name* — The interface name. The interface name can be up to 32 characters long and must be unique. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

nbr

Syntax **nbr** [**detail**]
no nbr

Context debug>router>rsvp>event

Description This command debugs neighbor events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about neighbor events.

path

Syntax **path** [**detail**]
no path

Context debug>router>rsvp>event

Description This command debugs path-related events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about path-related events.

resv

Syntax **resv** [**detail**]
no resv

Context debug>router>rsvp>event

Description This command debugs RSVP reservation events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about RSVP reservation events.

te-threshold-update

Syntax **te-threshold-update**
no te-threshold-update

Context debug>router>rsvp>event
debug>router>rsvp>ip-int-name>event

Description This command debugs the te-threshold-update events.

The **no** form of this command disables the debugging

packet

Syntax [**no**] **packet**

Context debug>router>rsvp>

Description This command enters the syntax to debug packets.

all

Syntax **all** [**detail**]
no all

Context debug>router>rsvp>packet

Description This command debugs all packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about all RSVP packets.

hello

Syntax **hello** [**detail**]
no hello

Context debug>router>rsvp>packet

Description This command debugs hello packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about hello packets.

path

Syntax **path** [**detail**]
no path

Context debug>router>rsvp>packet

Description This command enables debugging for RSVP path packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about path-related events.

patherr

Syntax **patherr** [**detail**]
no patherr

Context debug>router>rsvp>packet

Description This command debugs path error packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about path error packets.

pathtear

Syntax **pathtear** [**detail**]
no pathtear

Context debug>router>rsvp>packet

Description This command debugs path tear packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about path tear packets.

resv

Syntax **resv** [**detail**]
no resv

Context debug>router>rsvp>packet

Description This command enables debugging for RSVP resv packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about RSVP Resv events.

resverr

Syntax **resverr** [**detail**]
no resverr

Context debug>router>rsvp>packet

Description This command debugs ResvErr packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about ResvErr packets.

resvtear

Syntax **resvtear** [**detail**]
no resvtear

Context debug>router>rsvp>packet

Description This command debugs ResvTear packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about ResvTear packets.

Label Distribution Protocol

In This Chapter

This chapter provides information to enable Label Distribution Protocol (LDP).

Topics in this chapter include:

Label Distribution Protocol

Label Distribution Protocol (LDP) is a protocol used to distribute labels in non-traffic-engineered applications. LDP allows routers to establish label switched paths (LSPs) through a network by mapping network-layer routing information directly to data link layer-switched paths.

An LSP is defined by the set of labels from the ingress Label Switching Router (LSR) to the egress LSR. LDP associates a Forwarding Equivalence Class (FEC) with each LSP it creates. A FEC is a collection of common actions associated with a class of packets. When an LSR assigns a label to a FEC, it must let other LSRs in the path know about the label. LDP helps to establish the LSP by providing a set of procedures that LSRs can use to distribute labels.

The FEC associated with an LSP specifies which packets are mapped to that LSP. LSPs are extended through a network as each LSR splices incoming labels for a FEC to the outgoing label assigned to the next hop for the given FEC.

LDP allows an LSR to request a label from a downstream LSR so it can bind the label to a specific FEC. The downstream LSR responds to the request from the upstream LSR by sending the requested label.

LSRs can distribute a FEC label binding in response to an explicit request from another LSR. This is known as Downstream On Demand (DOD) label distribution. LSRs can also distribute label bindings to LSRs that have not explicitly requested them. This is called Downstream Unsolicited (DUS).

LDP and MPLS

LDP performs the label distribution only in MPLS environments. The LDP operation begins with a hello discovery process to find LDP peers in the network. LDP peers are two LSRs that use LDP to exchange label/FEC mapping information. An LDP session is created between LDP peers. A single LDP session allows each peer to learn the other's label mappings (LDP is bi-directional) and to exchange label binding information.

LDP signaling works with the MPLS label manager to manage the relationships between labels and the corresponding FEC. For service-based FECs, LDP works in tandem with the Service Manager to identify the virtual leased lines (VLLs) and Virtual Private LAN Services (VPLSs) to signal.

An MPLS label identifies a set of actions that the forwarding plane performs on an incoming packet before discarding it. The FEC is identified through the signaling protocol (in this case, LDP) and allocated a label. The mapping between the label and the FEC is communicated to the forwarding plane. In order for this processing on the packet to occur at high speeds, optimized tables are maintained in the forwarding plane that enable fast access and packet identification.

When an unlabeled packet ingresses the 7750 SR router, classification policies associate it with a FEC. The appropriate label is imposed on the packet, and the packet is forwarded. Other actions that can take place before a packet is forwarded are imposing additional labels, other encapsulations, learning actions, etc. When all actions associated with the packet are completed, the packet is forwarded.

When a labeled packet ingresses the router, the label or stack of labels indicates the set of actions associated with the FEC for that label or label stack. The actions are preformed on the packet and then the packet is forwarded.

The 7750 SR LDP implementation provides DOD, DUS, ordered control, liberal label retention mode support.

LDP Architecture

LDP comprises a few processes that handle the protocol PDU transmission, timer-related issues, and protocol state machine. The number of processes is kept to a minimum to simplify the architecture and to allow for scalability. Scheduling within each process prevents starvation of any particular LDP session, while buffering alleviates TCP-related congestion issues.

The LDP subsystems and their relationships to other subsystems are illustrated in Figure 16. This illustration shows the interaction of the LDP subsystem with other subsystems, including memory management, label management, service management, SNMP, interface management, and RTM. In addition, debugging capabilities are provided through the logger.

Communication within LDP tasks is typically done by inter-process communication through the event queue, as well as through updates to the various data structures. The primary data structures that LDP maintains are:

- FEC/label database — This database contains all the FEC to label mappings that include, both sent and received. It also contains both address FECs (prefixes and host addresses) as well as service FECs (L2 VLLs and VPLS).
- Timer database — This database contains all the timers for maintaining sessions and adjacencies.
- Session database — This database contains all the session and adjacency records, and serves as a repository for the LDP MIB objects.

Subsystem Interrelationships

The sections below describe how LDP and the other subsystems work to provide services.

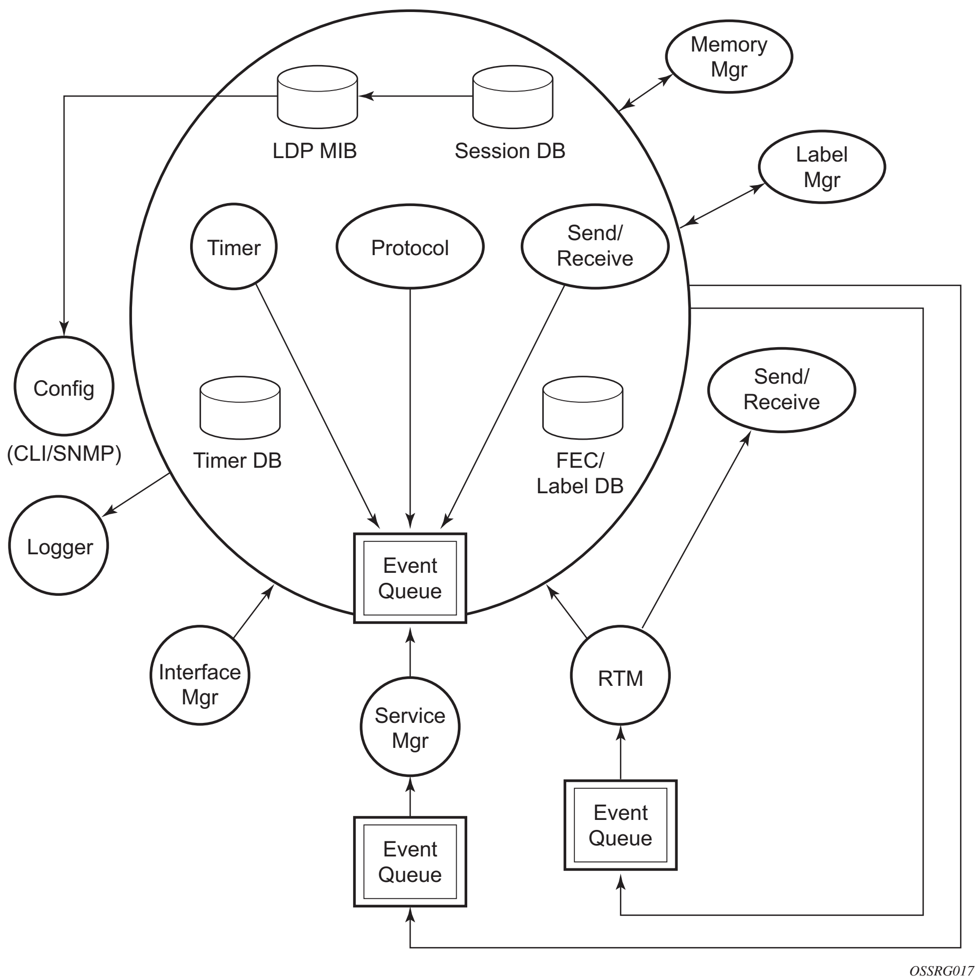

Figure 16: Subsystem Interrelationships

Memory Manager and LDP

LDP does not use any memory until it is instantiated. It pre-allocates some amount of fixed memory so that initial startup actions can be performed. Memory allocation for LDP comes out of a pool reserved for LDP that can grow dynamically as needed. Fragmentation is minimized by allocating memory in larger chunks and managing the memory internally to LDP. When LDP is shut down, it releases all memory allocated to it.

Label Manager

LDP assumes that the label manager is up and running. LDP will abort initialization if the label manager is not running. The label manager is initialized at system boot-up; hence, anything that causes it to fail will likely imply that the system is not functional. The 7750 SR uses a label range from 28672 (28K) to 131071 (128K-1) to allocate all dynamic labels, including RSVP allocated labels and VC labels.

LDP Configuration

The 7750 SR uses a single consistent interface to configure all protocols and services. CLI commands are translated to SNMP requests and are handled through an agent-LDP interface. LDP can be instantiated or deleted through SNMP. Also, LDP targeted sessions can be set up to specific endpoints. Targeted-session parameters are configurable.

Logger

LDP uses the logger interface to generate debug information relating to session setup and teardown, LDP events, label exchanges, and packet dumps. Per-session tracing can be performed.

Service Manager

All interaction occurs between LDP and the service manager, since LDP is used primarily to exchange labels for Layer 2 services. In this context, the service manager informs LDP when an LDP session is to be set up or torn down, and when labels are to be exchanged or withdrawn. In turn, LDP informs service manager of relevant LDP events, such as connection setups and failures, timeouts, labels signaled/withdrawn.

Execution Flow

LDP activity in 7750 SR OS is limited to service-related signaling. Therefore, the configurable parameters are restricted to system-wide parameters, such as hello and keepalive timeouts.

Initialization

MPLS must be enabled when LDP is initialized. LDP makes sure that the various prerequisites, such as ensuring the system IP interface is operational, the label manager is operational, and there is memory available, are met. It then allocates itself a pool of memory and initializes its databases.

Session Lifetime

In order for a targeted LDP (T-LDP) session to be established, an adjacency must be created. The LDP extended discovery mechanism requires hello messages to be exchanged between two peers for session establishment. After the adjacency establishment, session setup is attempted.

Adjacency Establishment

In the 7750 SR, the adjacency management is done through the establishment of a Service Distribution Path (SDP) object, which is a service entity in the Alcatel-Lucent service model.

The Alcatel-Lucent service model uses logical entities that interact to provide a service. The service model requires the service provider to create configurations for four main entities:

- Customers
- Services
- Service Access Paths (SAPs) on local 7750 SR routers
- Service Distribution Points (SDPs) that connect to one or more remote 7750 SR routers.

An SDP is the network-side termination point for a tunnel to a remote 7750 SR router. An SDP defines a local entity that includes the system IP address of the remote routers and a path type. Each SDP comprises:

- The SDP ID
- The transport encapsulation type, either MPLS or GRE
- The far-end system IP address

If the SDP is identified as using LDP signaling, then an LDP extended hello adjacency is attempted.

If another SDP is created to the same remote destination, and if LDP signaling is enabled, no further action is taken, since only one adjacency and one LDP session exists between the pair of nodes.

An SDP is a uni-directional object, so a pair of SDPs pointing at each other must be configured in order for an LDP adjacency to be established. Once an adjacency is established, it is maintained through periodic hello messages.

Session Establishment

When the LDP adjacency is established, the session setup follows as per the LDP specification. Initialization and keepalive messages complete the session setup, followed by address messages to exchange all interface IP addresses. Periodic keepalives or other session messages maintain the session liveliness.

Since TCP is back-pressured by the receiver, it is necessary to be able to push that back-pressure all the way into the protocol. Packets that cannot be sent are buffered on the session object and re-attempted as the back-pressure eases.

Label Exchange

Label exchange is initiated by the service manager. When an SDP is attached to a service (for example, the service gets a transport tunnel), a message is sent from the service manager to LDP. This causes a label mapping message to be sent. Additionally, when the SDP binding is removed from the service, the VC label is withdrawn. The peer must send a label release to confirm that the label is not in use.

Other Reasons for Label Actions

Other reasons for label actions include:

- MTU changes: LDP withdraws the previously assigned label, and re-signals the FEC with the new MTU in the interface parameter.
- Clear labels: When a service manager command is issued to clear the labels, the labels are withdrawn, and new label mappings are issued.
- SDP down: When an SDP goes administratively down, the VC label associated with that SDP for each service is withdrawn.
- Memory allocation failure: If there is no memory to store a received label, it is released.
- VC type unsupported: When an unsupported VC type is received, the received label is released.

Cleanup

LDP closes all sockets, frees all memory, and shuts down all its tasks when it is deleted, so its memory usage is 0 when it is not running.

LDP Filters

Both inbound and outbound LDP label binding filtering is supported.

Inbound filtering (import policy) allows configuration of a policy to control the label bindings an

LSR accepts from its peers. Label bindings can be filtered based on:

- Neighbor: Match on bindings received from the specified peer.
- Prefix-list: Match on bindings with the specified prefix/prefixes.

Note: The default import behavior is to accept all FECs received from peers. The LDP export policy can be used to explicitly add FECs (or non-LDP routes) for label propagation and does not filter out or stop propagation of any FEC received from neighbors.

Export policy enables configuration of a policy to advertise label bindings based on:

- Direct: All local subnets.
- Prefix-list: Match on bindings with the specified prefix or prefixes.

Note: The LDP export policy will not filter out FECs. It is only used to explicitly add FECs (or non-LDP routes) for label propagation.

The default export behavior originates label bindings for system address and propagate all FECs received.

Configuring Implicit Null

The implicit null label option allows a 7x50 egress LER to receive MPLS packets from the previous hop without the outer LSP label. The operation of the previous hop is referred to as penultimate hop popping (PHP). This option is signaled by the egress LER to the previous hop during the FEC signaling by the LDP control protocol.

The user can configure to signal the implicit null option for all LDP FECs for which this node is the egress LER using the following command:

config>router>ldp>implicit-null-label

When the user changes the implicit null configuration option, LDP withdraws all the FECs and readvertises them using the new label value.

LDP Filters

LDP provides both global and per-peer FEC, or label binding, import and export filter policies.

Inbound filtering (import policy) allows the user to configure a policy to control the label bindings an LSR accepts from its peers. Label bindings can be filtered based on:

- Prefix-list — Match on bindings with the specified prefix/prefixes.

The default import behavior is to accept all FECs received from peers.

Outbound filtering (export policy) allows the user to configure a policy to control the set of LDP label bindings advertised by the LSR. Label bindings can be advertised based on:

- Direct — All local subnets.
- Prefix-list — Match on bindings with the specified prefix/prefixes.

The default export behavior is to originate label bindings for system address and propagate all FECs received.

Per LDP Peer FEC Import and Export Policies

The FEC prefix export policy provides a way to control which FEC prefixes received from a peer should be re-distributed to all other LDP and T-LDP peers.

The user configures the FEC prefix export policy using the following command:

config>router>ldp>peer-parameters>peer>export-prefixes policy-name

The FEC prefix import policy provides a mean of controlling which FEC prefixes received from other LDP and T-LDP peers should be re-distributed to this LDP peer.

By default, all FEC prefixes from this peer are exported.

The user configures the FEC prefix export policy using the following command:

config>router>ldp>peer-parameters>peer>import-prefixes policy-name

By default, all FEC prefixes are re-distributed to this peer.

Configuring Multiple LDP LSR ID

The multiple LDP LSR-ID feature provides the ability to configure and initiate multiple T-LDP sessions on the same system using different LDP LSR-IDs. In the current implementation, all T-LDP sessions must have the LSR-ID match the system interface address. This feature continues to allow the use of the system interface but also any other loopback interface or local interface address on a per T-LDP session basis. Note that LDP control plane will not allow more than a single T-LDP session with the same local LSR ID to two different LSR-IDS on the same remote node.

An SDP of type LDP will use the source address configured as the local LSR-ID for the TLDP session to the peer matching a specific SDP far-end address. If no targeted session has been explicitly pre-provisioned to the far-end node under LDP, then the SDP will autoestablish one using the system interface address as the LSR-ID.

An SDP of type RSVP must have the local LSR-ID as the destination of the RSVP LSP from the peer. The local LSR-ID must be a local interface which is not a loopback if CSPF is enabled on the RSVP LSP.

An SDP of type GRE can only use a T-LDP session with a local LSR-ID set to the system interface.

The multiple LDP LSR-ID also provides the ability to use the LDP local interface address instead of the system address as the LSR-ID for the LDP adjacency to the peer over the local interface. In this case, the transport interface will automatically be set to use the same local interface address.

This feature can be configured for any I-LDP session. When used as such, the I-LDP transport-address parameter is ignored and the session is forced to use the interface as transport-address.

Tracking a T-LDP Peer with BFD

BFD tracking of an LDP session associated with a T-LDP adjacency allows for faster detection of the liveliness of the session by registering the transport address of a LDP session with a BFD session.

By enabling BFD for a selected targeted session, the state of that session is tied to the state of the underneath BFD session between the two nodes. The parameters used for the BFD are set with the BFD command under the IP interface.

LDP LSP Statistics

RSVP-TE LSP statistics is extended to LDP to provide the following counters:

- Per-forwarding-class forwarded in-profile packet count
- Per-forwarding-class forwarded in-profile byte count
- Per-forwarding-class forwarded out-of-profile packet count
- Per-forwarding-class forwarded out-of-profile byte count

The counters are available for the egress data path of an LDP FEC at ingress LER and at LSR. Because an ingress LER is also potentially an LSR for an LDP FEC, combined egress data path statistics will be provided whenever applicable.

This feature is supported on IOM2-20g, IMM and IOM3-XP and requires chassis mode C or higher.

TTL Security for BGP and LDP

The BGP TTL Security Hack (BTSH) was originally designed to protect the BGP infrastructure from CPU utilization-based attacks. It is derived from the fact that the vast majority of ISP eBGP peerings are established between adjacent routers. Since TTL spoofing is considered nearly impossible, a mechanism based on an expected TTL value can provide a simple and reasonably robust defense from infrastructure attacks based on forged BGP packets.

While TTL Security Hack (TSH) is most effective in protecting directly connected peers, it can also provide a lower level of protection to multi-hop sessions. When a multi-hop BGP session is required, the expected TTL value can be set to 255 minus the configured range-of-hops. This approach can provide a qualitatively lower degree of security for BGP (such as a DoS attack could, theoretically, be launched by compromising a box in the path). However, BTSH will catch a vast majority of observed distributed DoS (DDoS) attacks against eBGP.

TSH can be used to protect LDP peering sessions as well. For details, see draft-chen-ldp-ttl-xx.txt, *TTL-Based Security Option for LDP Hello Message*.

The TSH implementation supports the ability to configure TTL security per BGP/LDP peer and evaluate (in hardware) the incoming TTL value against the configured TTL value. If the incoming TTL value is less than the configured TTL value, the packets are discarded and a log is generated.

ECMP Support for LDP

ECMP support for LDP performs load balancing for LDP based LSPs by having multiple outgoing next-hops for a given IP prefix on ingress and transit LSRs.

An LSR that has multiple equal cost paths to a given IP prefix can receive an LDP label mapping for this prefix from each of the downstream next-hop peers. As the LDP implementation uses the liberal label retention mode, it retains all the labels for an IP prefix received from multiple next-hop peers.

Without ECMP support for LDP, only one of these next-hop peers will be selected and installed in the forwarding plane. The algorithm used to determine the next-hop peer to be selected involves looking up the route information obtained from the RTM for this prefix and finding the first valid LDP next-hop peer (for example, the first neighbor in the RTM entry from which a label mapping was received). If, for some reason, the outgoing label to the installed next-hop is no longer valid, say the session to the peer is lost or the peer withdraws the label, a new valid LDP next-hop peer will be selected out of the existing next-hop peers and LDP will reprogram the forwarding plane to use the label sent by this peer.

With ECMP support, all the valid LDP next-hop peers, those that sent a label mapping for a given IP prefix, will be installed in the forwarding plane. In both cases, ingress LER and transit LSR, an ingress label will be mapped to the nexthops that are in the RTM and from which a valid mapping label has been received. The forwarding plane will then use an internal hashing algorithm to determine how the traffic will be distributed amongst these multiple next-hops, assigning each “flow” to a particular next-hop.

The hash algorithm at LER and transit LSR are described in the LAG and ECMP Hashing section of the 7750 SR OS Interface Guide.

Label Operations

If an LSR is the ingress for a given IP prefix, LDP programs a push operation for the prefix in the IOM. This creates an LSP ID to the Next Hop Label Forwarding Entry (NHLFE) (LTN) mapping and an LDP tunnel entry in the forwarding plane. LDP will also inform the Tunnel Table Manager (TTM) of this tunnel. Both the LTN entry and the tunnel entry will have a NHLFE for the label mapping that the LSR received from each of its next-hop peers.

If the LSR is to behave as a transit for a given IP prefix, LDP will program a swap operation for the prefix in the IOM. This involves creating an Incoming Label Map (ILM) entry in the forwarding plane. The ILM entry will have to map an incoming label to possibly multiple NHLFEs. If an LSR is an egress for a given IP prefix, LDP will program a POP entry in the IOM. This too will result in an ILM entry being created in the forwarding plane but with no NHLFEs.

When unlabeled packets arrive at the ingress LER, the forwarding plane will consult the LTN entry and will use a hashing algorithm to map the packet to one of the NHLFEs (push label) and forward the packet to the corresponding next-hop peer. For labeled packets arriving at a transit or egress LSR, the forwarding plane will consult the ILM entry and either use a hashing algorithm to map it to one of the NHLFEs if they exist (swap label) or simply route the packet if there are no NHLFEs (pop label).

Static FEC swap will not be activated unless there is a matching route in system route table that also matches the user configured static FEC next-hop.

LDP over RSVP Tunnels

LDP over RSVP-TE provides end-to-end tunnels that have two important properties, fast reroute and traffic engineering which are not available in LDP. LDP over RSVP-TE is focused at large networks (over 100 nodes in the network). Simply using end-to-end RSVP-TE tunnels will not scale. While an LER may not have that many tunnels, any transit node will potentially have thousands of LSPs, and if each transit node also has to deal with detours or bypass tunnels, this number can make the LSR overly burdened.

LDP over RSVP-TE allows tunneling of user packets using an LDP LSP inside an RSVP LSP.The main application of this feature is for deployment of MPLS based services, for example, VPRN, VLL, and VPLS services, in large scale networks across multiple IGP areas without requiring full mesh of RSVP LSPs between PE routers.

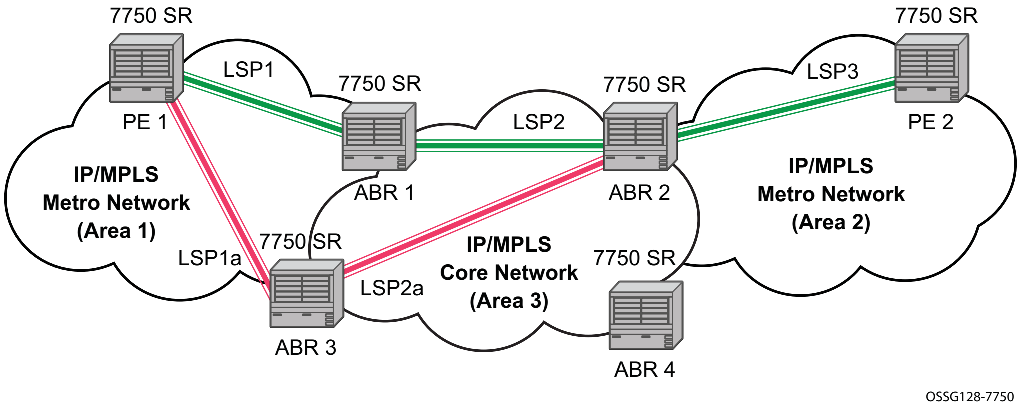

Figure 17: LDP over RSVP Application

The network displayed in Figure 17 consists of two metro areas, Area 1 and 2 respectively, and a core area, Area 3. Each area makes use of TE LSPs to provide connectivity between the edge routers. In order to enable services between PE1 and PE2 across the three areas, LSP1, LSP2, and LSP3 are set up using RSVP-TE. There are in fact 6 LSPs required for bidirectional operation but we will refer to each bi-directional LSP with a single name, for example, LSP1. A targeted LDP (T-LDP) session is associated with each of these bidirectional LSP tunnels. That is, a T-LDP adjacency is created between PE1 and ABR1 and is associated with LSP1 at each end. The same is done for the LSP tunnel between ABR1 and ABR2, and finally between ABR2 and PE2. The loopback address of each of these routers is advertised using T-LDP. Similarly, backup bidirectional LDP over RSVP tunnels, LSP1a and LSP2a, are configured via ABR3.

This setup effectively creates an end-to-end LDP connectivity which can be used by all PEs to provision services. The RSVP LSPs are used as a transport vehicle to carry the LDP packets from one area to another. Note that only the user packets are tunneled over the RSVP LSPs. The T-LDP control messages are still sent unlabeled using the IGP shortest path.

Note that in this application, the bi-directional RSVP LSP tunnels are not treated as IP interfaces and are not advertised back into the IGP. A PE must always rely on the IGP to look up the next hop for a service packet. LDP-over-RSVP introduces a new tunnel type, tunnel-in-tunnel, in addition to the existing LDP tunnel and RSVP tunnel types. If multiple tunnels types match the destination PE FEC lookup, LDP will prefer an LDP tunnel over an LDP-over-RSVP tunnel by default.

The design in Figure 17 allows a service provider to build and expand each area independently without requiring a full mesh of RSVP LSPs between PEs across the three areas.

In order to participate in a VPRN service, PE1 and PE2 perform the autobind to LDP. The LDP label which represents the target PE loopback address is used below the RSVP LSP label. Therefore a 3 label stack is required.

In order to provide a VLL service, PE1 and PE2 are still required to set up a targeted LDP session directly between them. Again a 3 label stack is required, the RSVP LSP label, followed by the LDP label for the loopback address of the destination PE, and finally the pseudowire label (VC label).

This implementation supports a variation of the application in Figure 17, in which area 1 is an LDP area. In that case, PE1 will push a two label stack while ABR1 will swap the LDP label and push the RSVP label as illustrated in Figure 18. LDP-over-RSVP tunnels can also be used as IGP shortcuts.

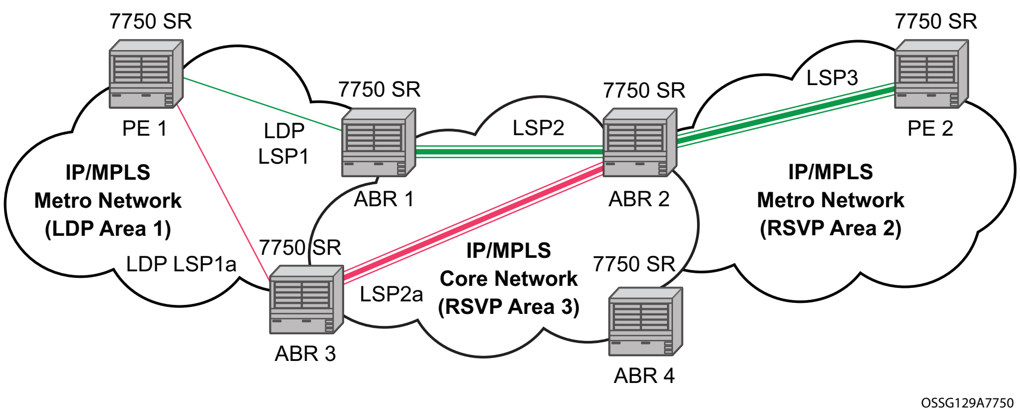

Figure 18: LDP over RSVP Application Variant

Signaling and Operation

- LDP Label Distribution and FEC Resolution on page 291
- Default FEC Resolution Procedure on page 292

LDP Label Distribution and FEC Resolution

The user creates a targeted LDP (T-LDP) session to an ABR or the destination PE. This results in LDP hellos being sent between the two routers. These messages are sent unlabeled over the IGP path. Next, the user enables LDP tunneling on this T-LDP session and optionally specifies a list of LSP names to associate with this T-LDP session. By default, all RSVP LSPs which terminate on the T-LDP peer are candidates for LDP-over-RSVP tunnels. At this point in time, the LDP FECs resolving to RSVP LSPs are added into the Tunnel Table Manager as tunnel-in-tunnel type.

Note that if LDP is running on regular interfaces also, then the prefixes LDP learns are going to be distributed over both the T-LDP session as well as regular IGP interfaces. The policy controls which prefixes go over the T-LDP session, for example, only /32 prefixes, or a particular prefix range.

LDP-over-RSVP works with both OSPF and ISIS. These protocols include the advertising router when adding an entry to the RTM. LDP-over-RSVP tunnels can be used as shortcuts for BFP next-hop resolution.

Default FEC Resolution Procedure

When LDP tries to resolve a prefix received over a T-LDP session, it performs a lookup in the Routing Table Manager (RTM). This lookup returns the next hop to the destination PE and the advertising router (ABR or destination PE itself). If the next-hop router advertised the same FEC over link-level LDP, LDP will prefer the LDP tunnel by default unless the user explicitly changed the default preference using the system wide prefer-tunnel-in-tunnel command. If the LDP tunnel becomes unavailable, LDP will select an LDP-over-RSVP tunnel if available.

When searching for an LDP-over-RSVP tunnel, LDP selects the advertising router(s) with best route. If the advertising router matches the T-LDP peer, LDP then performs a second lookup for the advertising router in the Tunnel Table Manager (TTM) which returns the user configured RSVP LSP with the best metric. If there are more than one configured LSP with the best metric, LDP selects the first available LSP.

If all user configured RSVP LSPs are down, no more action is taken. If the user did not configure any LSPs under the T-LDP session, the lookup in TTM will return the first available RSVP LSP which terminates on the advertising router with the lowest metric.

FEC Resolution Procedure When prefer-tunnel-in-tunnel is Enabled

When LDP tries to resolve a prefix received over a T-LDP session, it performs a lookup in the Routing Table Manager (RTM). This lookup returns the next hop to the destination PE and the advertising router (ABR or destination PE itself).

When searching for an LDP-over-RSVP tunnel, LDP selects the advertising router(s) with best route. If the advertising router matches the targeted LDP peer, LDP then performs a second lookup for the advertising router in the Tunnel Table Manager (TTM) which returns the user configured RSVP LSP with the best metric. If there are more than one configured LSP with the best metric, LDP selects the first available LSP.

If all user configured RSVP LSPs are down, then an LDP tunnel will be selected if available.

If the user did not configure any LSPs under the T-LDP session, a lookup in TTM will return the first available RSVP LSP which terminates on the advertising router. If none are available, then an LDP tunnel will be selected if available.

Rerouting Around Failures

Every failure in the network can be protected against, except for the ingress and egress PEs. All other constructs have protection available. These constructs are LDP-over-RSVP tunnel and ABR.

- LDP-over-RSVP Tunnel Protection on page 293
- ABR Protection on page 293

LDP-over-RSVP Tunnel Protection

An RSVP LSP can deal with a failure in two ways.

- If the LSP is a loosely routed LSP, then RSVP will find a new IGP path around the failure, and traffic will follow this new path. This may involve some churn in the network if the LSP comes down and then gets re-routed. The tunnel damping feature was implemented on the LSP so that all the dependent protocols and applications do not flap unnecessarily.
- If the LSP is a CSPF-computed LSP with the fast reroute option enabled, then RSVP will switch to the detour path very quickly. From that point, a new LSP will be attempted from the head-end (global revertive). When the new LSP is in place, the traffic switches over to the new LSP with make-before-break.

ABR Protection

If an ABR fails, then routing around the ABR requires that a new next-hop LDP-over-RSVP tunnel be found to a backup ABR. If an ABR fails, then the T-LDP adjacency fails. Eventually, the backup ABR becomes the new next hop (after SPF converges), and LDP learns of the new next-hop and can reprogram the new path.

LDP over RSVP Without Area Boundary

The LDP over RSVP capability set includes the ability to stitch LDP-over-RSVP tunnels at internal (non-ABR) OSPF and IS-IS routers.

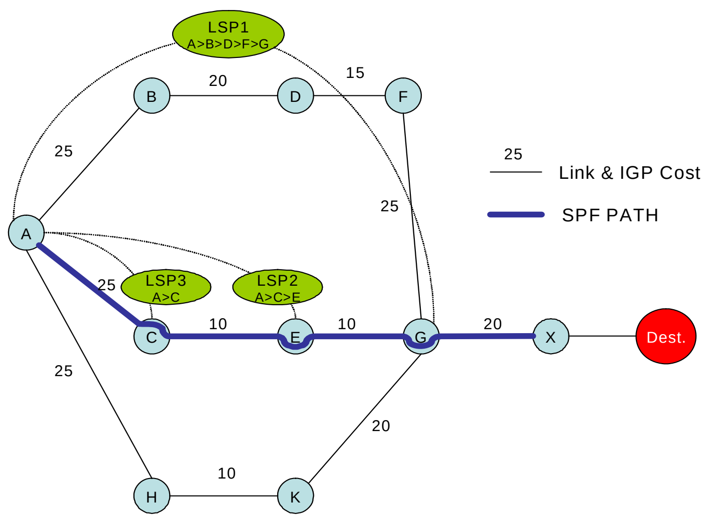

Figure 19: LDP over RSVP Without ABR Stitching Point

In Figure 19, assume that the user wants to use LDP over RSVP between router A and destination "Dest". The first thing that happens is that either OSPF or IS-IS will perform an SPF calculation resulting in an SPF tree. This tree specifies the lowest possible cost to the destination. In the example shown, the destination "Dest" is reachable at the lowest cost through router X. The SPF tree will have the following path: A>C>E>G>X.

Using this SPF tree, router A will search for the endpoint that is closest (farthest/highest cost from the origin) to "Dest" that is eligible. Assuming that all LSPs in the above diagram are eligible, LSP endpoint G will be selected as it terminates on router G while other LSPs only reach routers C and E, respectively.

IGP and LSP metrics associated with the various LSP are ignores; only tunnel endpoint matters to IGP. The endpoint that terminates closest to "Dest" (highest IGP path cost) will be selected for further selection of the LDP over RSVP tunnels to that endpoint. Note that the explicit path the tunnel takes may not match the IGP path the SPF computes.

If router A and G have an additional LSP terminating on router G, there would now be two tunnels both terminating on the same router closest to the final destination. For IGP, it does not make any difference on the numbers of LDPs to G, only that there is at least one LSP to G. In this case, the LSP metric will be considered by LDP when deciding which LSP to stitch for the LDP over RSVP connection.

The IGP only passes endpoint information to LDP. LDP looks up the tunnel table for all tunnels to that endpoint and picks up the one with the least tunnel metric. There may be many tunnels with the same least cost.

LDP over RSVP and ECMP

ECMP for LDP over RSVP is supported (also see ECMP Support for LDP on page 286). If ECMP applies, all LSP endpoints found over the ECMP IGP path will be installed in the routing table by the IGP for consideration by LDP. It is important to note that IGP costs to each endpoint may differ because IGP selects the farthest endpoint per ECMP path.

LDP will choose the endpoint that is highest cost in the route entry and will do further tunnel selection over those endpoints. If there are multiple endpoints with equal highest cost, then LDP will consider all of them.

LDP FEC to BGP Label Route Stitching

The stitching of an LDP FEC to a BGP labeled route allows LDP capable PE devices to offer servicers to PE routers in other areas or domains without the need to support BGP labeled routes.

This feature is used in a large network to provide services across multiple areas or autonomous systems. Figure 20 shows a network with a core area and regional areas.

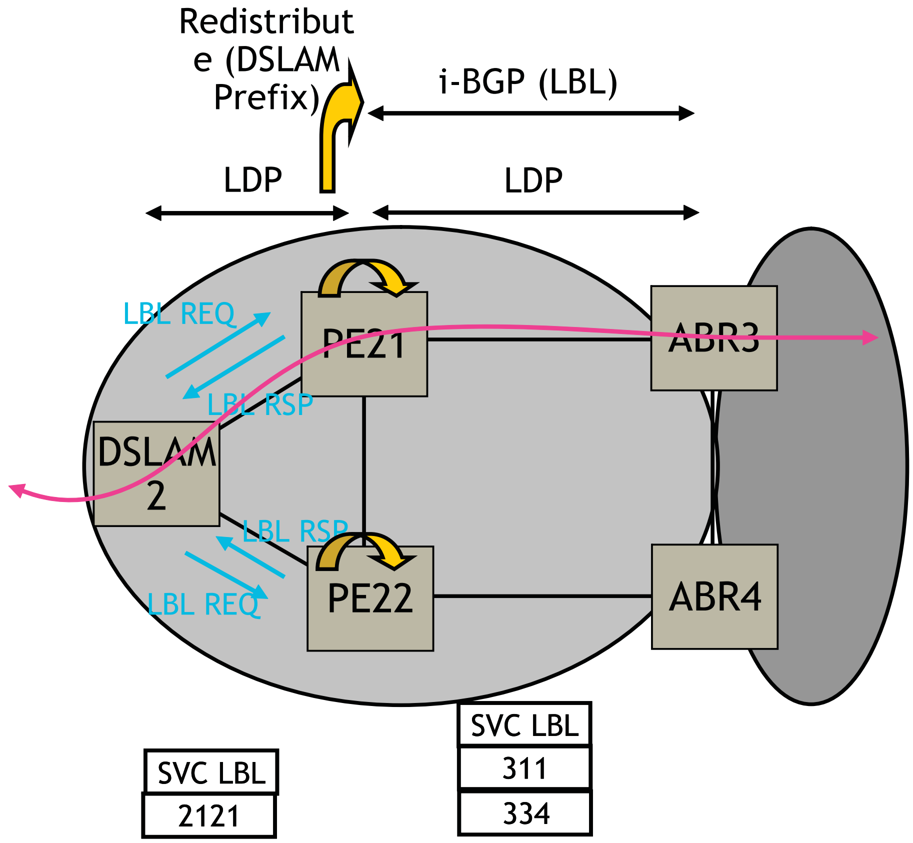

Figure 20: Application of LDP to BGP FEC Stitching

Specific /32 routes in a regional area are not redistributed into the core area. Therefore, only nodes within a regional area and the ABR nodes in the same area exchange LDP FECs. A PE router, for example, PE21, in a regional area learns the reachability of PE routers in other regional areas via RFC 3107 BGP labeled routes redistributed by the remote ABR nodes via the core area. The remote ABR then sets the next-hop self on the labeled routes before re-distributing them into the core area. The local ABR for PE2, for example, ABR3 may or may not set next-hop self when it re-distributes these labeled BGP routes from the core area to the local regional area.

When forwarding a service packet to the remote PE, PE21 inserts a VC label, the BGP route label to reach the remote PE, and an LDP label to reach either ABR3, if ABR3 sets next-hop self, or ABR1.

In the same network, an MPLS capable DSLAM also act as PE router for VLL services and will need to establish a PW to a PE in a different regional area via router PE21, acting now as an LSR. To achieve that, PE21 is required to perform the following operations:

- Translate the LDP FEC it learned from the DSLAM into a BGP labeled route and re-distribute it via iBGP within its area. This is in addition to redistributing the FEC to its LDP neighbors in the same area.
- Translate the BGP labeled routes it learns via iBGP into an LDP FEC and re-distribute it to its LDP neighbors in the same area. In the application in Figure 20, the DSLAM requests the LDP FEC of the remote PE router using LDP Downstream on Demand (DoD).
- When a packet is received from the DSLAM, PE21 swaps the LDP label into a BGP label and pushes the LDP label to reach ABR3 or ABR1. When a packet is received from ABR3, the top label is removed and the BGP label is swapped for the LDP label corresponding to the DSLAM FEC.

Configuration

The user enables the stitching of routes between LDP and BGP by configuring separately tunnel table route export policies in both protocols and enabling the advertising of RFC 3107 formatted labeled routes for prefixes learned from LDP FECs.

The route export policy in BGP instructs BGP to listen to LDP route entries in the CPM tunnel table. If a /32 LDP FEC prefix matches an entry in the export policy, BGP originates a BGP labeled route, stitches it to the LDP FEC, and re-distributes the BGP labeled route to its iBGP neighbors.

The user adds LDP FEC prefixes with the statement ‘from protocol ldp’ in the configuration of the existing BGP export policy at the global level, the peer-group level, or at the peer level using the commands:

- **configure>router>bgp>export** *policy-name*
- **configure>router>bgp>group>export** *policy-name*
- **configure>router>bgp>group>neighbour>export** *policy-name*

To indicate to BGP to evaluate the entries with the ‘from protocol ldp’ statement in the export policy when applied to a specific BGP neighbor, a new argument is added to the existing advertise-label command:

configure>router>bgp>group>neighbour>advertise-label ipv4 include-ldp-prefix

Without the new **include-ldp-prefix** argument, only core IPv4 routes learned from RTM are advertised as BGP labeled routes to this neighbor. And the stitching of LDP FEC to the BGP labeled route is not performed for this neighbor even if the same prefix was learned from LDP.

The tunnel table route export policy in LDP instructs LDP to listen to BGP route entries in the CPM Tunnel Table. If a /32 BGP labeled route matches a prefix entry in the export policy, LDP originates an LDP FEC for the prefix, stitches it to the BGP labeled route, and re-distributes the LDP FEC its iBGP neighbors.

The user adds BGP labeled route prefixes with the statement ‘from protocol bgp’ in the configuration of a new LDP tunnel table export policy using the command:

configure>router>ldp>export-tunnel-table *policy-name*.

Note that the ‘from protocol’ statement has an effect only when the protocol value is ldp. Policy entries with protocol values of rsvp, bgp, or any value other than ldp are ignored at the time the policy is applied to LDP.

Detailed LDP FEC Resolution

When a 7x50 LSR receives a FEC-label binding from an LDP neighbor for a given specific FEC1 element, the following procedures are performed.

1. LDP installs the FEC if:
   - → It was able to perform a successful exact match or a longest match, if aggregate-prefix-match option is enabled in LDP, of the FEC /32 prefix with a prefix entry in the routing table.
   - → The advertising LDP neighbor is the next-hop to reach the FEC prefix.
2. When such a FEC-label binding has been installed in the LDP FIB, LDP will perform the following:
   - → Program a push and a swap NHLFE entries in the egress data path to forward packets to FEC1.
   - → Program the CPM tunnel table with a tunnel entry for the NHLFE.
   - → Advertise a new FEC-label binding for FEC1 to all its LDP neighbors according to the global and per-peer LDP prefix export policies.
   - → Install the ILM entry pointing to the swap NHLFE.

3. When BGP learns the LDP FEC via the CPM tunnel table and the FEC prefix exists in the BGP route export policy, it will perform the following:
   → Originate a labeled BGP route for the same prefix with this node as the next-hop and advertise it via iBGP to its BGP neighbours, for example, the local ABR/ASBR nodes, which have the advertise-label for LDP FEC prefixes is enabled.
   → Install the ILM entry pointing to the swap NHLFE programmed by LDP.

Detailed BGP Labeled Route Resolution

When a 7x50 LSR receives a BGP labeled route via iBGP for a given specific /32 prefix, the following procedures are performed.

1. BGP resolves and installs the route in BGP if:
   → There exists an LDP LSP to the BGP neighbor, for example, the ABR or ASBR, which advertised it and which is the next-hop of the BGP labeled route.
2. Once the BGP route is installed, BGP programs the following:
   → Push NHLFE in the egress data path to forward packets to this BGP labeled route.
   → The CPM tunnel table with a tunnel entry for the NHLFE.
3. When LDP learns the BGP labeled route via the CPM tunnel table and the prefix exists in the new LDP tunnel table route export policy, it performs the following:
   → Advertise a new LDP FEC-label binding for the same prefix to its LDP neighbors according the global and per-peer LDP export prefix policies. If LDP already advertised a FEC for the same /32 prefix after receiving it from an LDP neighbor then no action is required. For LDP neighbors that negotiated LDP Downstream on Demand (DoD) [ldp-dod-prd], the FEC is advertised only when this node receives a Label Request message for this FEC from its neighbor.
   → Install the ILM entry pointing the BGP NHLFE if a new LDP FEC-label binding is advertised. If an ILM entry exists and points to an LDP NHLFE for the same prefix then no update to ILM entry is performed. The LDP route has always preference over the BGP labeled route.

Data Plane Forwarding

When a packet is received from an LDP neighbor, the 7x50 LSR swaps the LDP label into a BGP label and pushes the LDP label to reach the BGP neighbor, for example, ABR/ASBR, which advertised the BGP labeled route with itself as the next-hop.

When a packet is received from a BGP neighbor such as an ABR/ASBR, the top label is removed and the BGP label is swapped for the LDP label to reach the next-hop for the prefix.

Multicast P2MP LDP for GRT

P2MP LDP LSP setup is initiated by each leaf node of multicast tree. A leaf PE node learns to initiate a multicast tree setup from client application and sends a label map upstream towards the root node of the multicast tree. On propagation of label map, intermediate nodes that are common on path for multiple leaf nodes become branch nodes of the tree.

Figure 21 illustrates wholesale video distribution over P2MP LDP LSP. Static IGMP entries on edge are bound to P2MP LDP LSP tunnel-interface for multicast video traffic distribution.

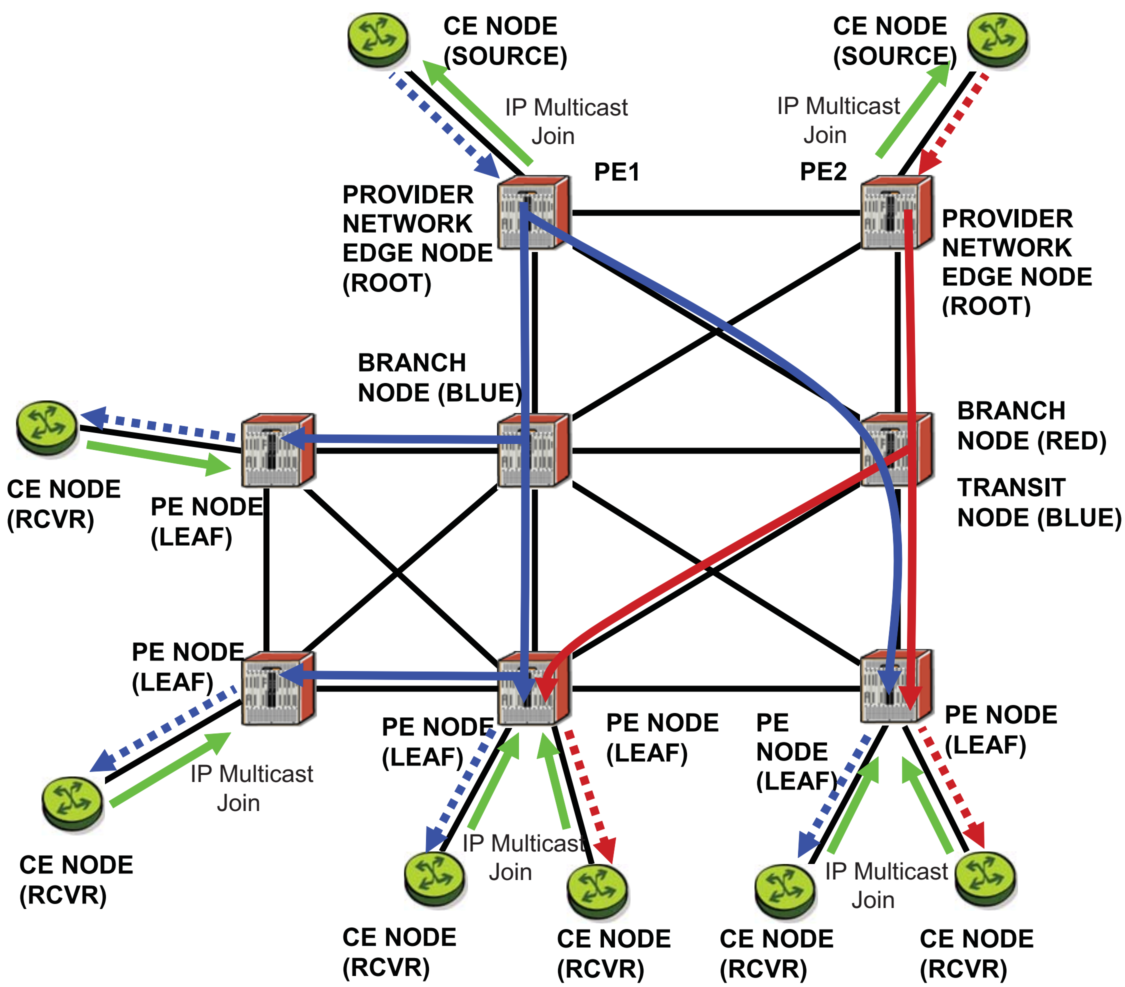

Figure 21: Video Distribution using P2MP LDP

LDP P2MP Support

LDP P2MP Configuration

A node running LDP also supports P2MP LSP setup using LDP. By default, it would advertise the capability to a peer node using P2MP capability TLV in LDP initialization message.

This configuration option per interface is provided to restrict/allow the use of interface in LDP multicast traffic forwarding towards a downstream node. Interface configuration option does not restrict/allow exchange of P2MP FEC via established session to the peer on an interface, but it would only restrict/allow use of next-hops over the interface.

LDP P2MP Protocol

Only a single generic identifier range is defined for signaling multipoint tree for all client applications. Implementation on 7x50 SR reserves the range (1..8292) of generic LSP P2MP-ID on root node for static P2MP LSP.

Make Before Break (MBB)

When a transit or leaf node detects that the upstream node towards the root node of multicast tree has changed, it follows graceful procedure that allows make-before-break transition to the new upstream node. Make-before-break support is optional. If the new upstream node doe not support MBB procedures then the downstream node waits for the configured timer before switching over to the new upstream node.

ECMP Support

If multiple ECMP paths exist between two adjacent nodes then the upstream node of the multicast receiver programs all entries in forwarding plane. Only one entry is active based on ECMP hashing algorithm.

Multi-Area and Multi-Instance Extensions to LDP

In order to extend LDP across multiple areas of an IGP instance or across multiple IGP instances, the current standard LDP implementation based on RFC 3036 requires that all /32 prefixes of PEs be leaked between the areas or instances. This is because an exact match of the prefix in the routing table is required to install the prefix binding in the LDP Forwarding Information Base (FIB). Although a 7750 SR7450 ESS7710 SR will do this by default when configured as Area Border Router (ABR), this increases the convergence of IGP on routers when the number of PE nodes scales to thousands of nodes.

Multi-area and multi-instance extensions to LDP provide an optional behavior by which LDP installs a prefix binding in the LDP FIB by simply performing a longest prefix match with an aggregate prefix in the routing table (RIB). That way, the ABR will be configured to summarize the /32 prefixes of PE routers. This method is compliant to RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*.

LDP Shortcut for BGP Next-Hop Resolution

LDP shortcut for BGP next-hop resolution shortcuts allow for the deployment of a 'route-less core' infrastructure. Many service providers either have or intend to remove the IBGP mesh from their network core, retaining only the mesh between routers connected to areas of the network that require routing to external routes.

Shortcuts are implemented by utilizing Layer 2 tunnels (i.e., MPLS LSPs) as next hops for prefixes that are associated with the far end termination of the tunnel. By tunneling through the network core, the core routers forwarding the tunnel have no need to obtain external routing information and are immune to attack from external sources.

The tunnel table contains all available tunnels indexed by remote destination IP address. LSPs derived from received LDP /32 route FECs will automatically be installed in the table associated with the advertising router-ID when IGP shortcuts are enabled.

Evaluating tunnel preference is based on the following order in descending priority:

1. LDP /32 route FEC shortcut
2. Actual IGP next-hop

If a higher priority shortcut is not available or is not configured, a lower priority shortcut is evaluated. When no shortcuts are configured or available, the IGP next-hop is always used. Shortcut and next-hop determination is event driven based on dynamic changes in the tunneling mechanisms and routing states.

Refer to the 7750 SR OS Routing Protocols Guide for details on the use of LDP FEC and RSVP LSP for BGP Next-Hop Resolution.

LDP Shortcut for IGP Routes

The LDP shortcut for IGP route resolution feature allows forwarding of packets to IGP learned routes using an LDP LSP. When LDP shortcut is enabled globally, IP packets forwarded over a network IP interface will be labeled with the label received from the next-hop for the route and corresponding to the FEC-prefix matching the destination address of the IP packet. In such a case, the routing table will have the shortcut next-hop as the best route. If such a LDP FEC does not exist, then the routing table will have the regular IP next-hop and regular IP forwarding will be performed on the packet.

An egress LER advertises and maintains a FEC, label binding for each IGP learned route. This is performed by the existing LDP fec-originate capability.

A typical application of the LDP shortcut is in providing Broadband Network Gateway (BNG) capability for subscriber/host routes on a 7750 SR as shown in Figure 22.

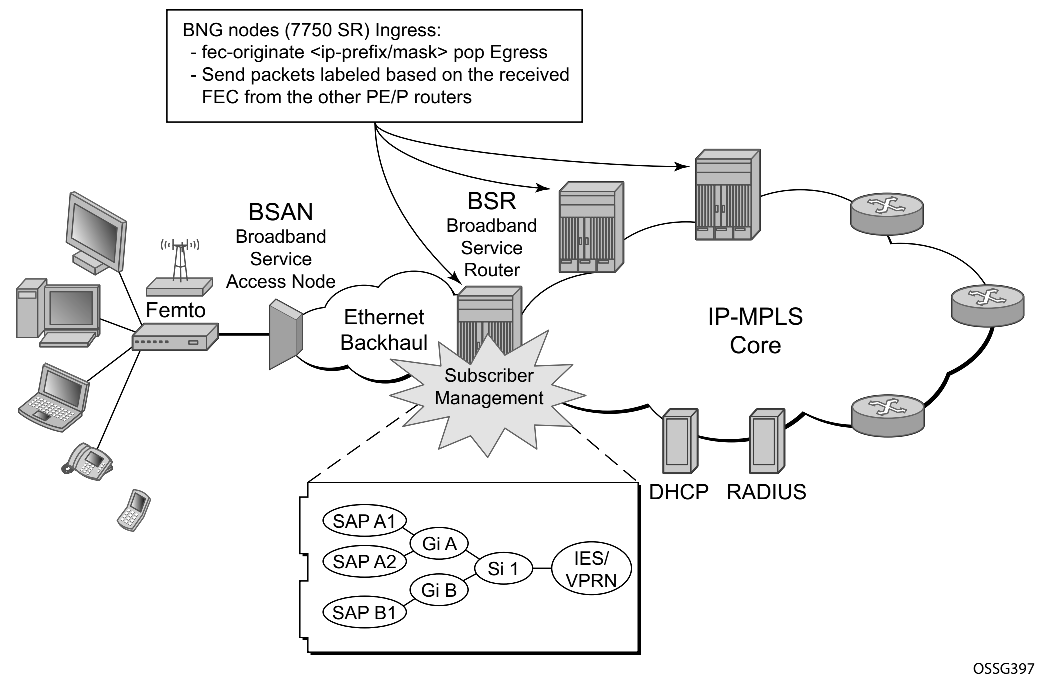

Figure 22: 1 Application of LDP Shortcut

Subscriber routes are statically configured or dynamically learned by DHCP over a subscriber IES interface. The user advertises the routes from the 7750 SR BNG to the rest of the network using IS-IS routing. The user also advertises label bindings for the FEC prefix corresponding to these routes using the 7750 static prefix FEC capability. The 7750 BNG learns IS-IS routes and LDP FECs from other PE and P routers in the network.

When an IP packet is received on a subscriber interface on the 7750 BNG, it is forwarded using the LDP shortcut if there exists an LDP LSP with a FEC prefix matching the IS-IS route of the packet.

When a packet is received from the LDP LSP, the packet is looked up and is forwarded over a subscriber interface if the route is resolved to the subscriber/host static or dynamic route.

LDP Shortcut Configuration

The user enables the use of LDP shortcut for resolving IGP routes by entering the global command **config>router>ldp-shortcut.**

This command enables forwarding of user IP packets and specified control IP packets using LDP shortcuts over all network interfaces in the system which participate in the IS-IS and OSPF routing protocols. The default is to disable the LDP shortcut across all interfaces in the system.

IGP Route Resolution

When LDP shortcut is enabled, LDP populates the RTM with next-hop entries corresponding to all prefixes for which it activated an LDP FEC. For a given prefix, two route entries are populated in RTM. One corresponds to the LDP shortcut next-hop and has an owner of LDP. The other one is the regular IP next-hop. The LDP shortcut next-hop always has preference over the regular IP next-hop for forwarding user packets and specified control packets over a given outgoing interface to the route next-hop.

The prior activation of the FEC by LDP is done by performing an exact match with an IGP route prefix in RTM. It can also be done by performing a longest prefix-match with an IGP route in RTM if the aggregate-prefix-match option is enabled globally in LDP.

This feature is not restricted to /32 FEC prefixes. However only /32 FEC prefixes will be populated in the CPM Tunnel Table for use as a tunnel by services.

All user and specified control packets for which the longest prefix match in RTM yields the FEC prefix will be forwarded over the LDP LSP. The following is an example of the resolution process.

Assume the egress LER advertised a FEC for some /24 prefix using the fec-originate command. At the ingress LER, LDP resolves the FEC by checking in RTM that an exact match exists for this prefix. Once LDP activated the FEC, it programs the NHLFE in the egress data path and the LDP tunnel information in the ingress data path tunnel table.

Next, LDP provides the shortcut route to RTM which will associate it with the same /24 prefix. There will be two entries for this /24 prefix, the LDP shortcut next-hop and the regular IP next-hop. The latter was used by LDP to validate and activate the FEC. RTM then resolves all user prefixes which succeed a longest prefix match against the /24 route entry to use the LDP LSP.

Assume now the aggregate-prefix-match was enabled and that LDP found a /16 prefix in RTM to activate the FEC for the /24 FEC prefix. In this case, RTM adds a new more specific route entry of /24 and has the next-hop as the LDP LSP but it will still not have a specific /24 IP route entry. RTM then resolves all user prefixes which succeed a longest prefix match against the /24 route entry to use the LDP LSP while all other prefixes which succeed a longest prefix-match against the /16 route entry will use the IP next-hop.

LDP Shortcut Forwarding Plane

Once LDP activated a FEC for a given prefix and programmed RTM, it also programs the ingress Tunnel Table in IOM with the LDP tunnel information.

When an IPv4 packet is received on an ingress network interface, a subscriber IES interface, or a regular IES interface, the lookup of the packet by the ingress IOM will result in the packet being sent labeled with the label stack corresponding to the NHLFE of the LDP LSP when the preferred RTM entry corresponds to an LDP shortcut.

If the preferred RTM entry corresponds to an IP next-hop, the IPv4 packet is forwarded unlabeled.

ECMP Considerations

When ECMP is enabled and multiple equal-cost next-hops exit for the IGP route, the ingress IOM sprays the packets for this route based on hashing routine currently supported for IPv4 packets.

When the preferred RTM entry corresponds to an LDP shortcut route, spraying will be performed across the multiple next-hops for the LDP FEC. The FEC next-hops can either be direct link LDP neighbors or T-LDP neighbors reachable over RSVP LSPs in the case of LDP-over-RSVP but not both. This is as per ECMP for LDP in existing implementation.

When the preferred RTM entry corresponds to a regular IP route, spraying will be performed across regular IP next-hops for the prefix.

Disabling TTL Propagation in an LSP Shortcut

This feature provides the option for disabling TTL propagation from a transit or a locally generated IP packet header into the LSP label stack when an LDP LSP is used as a shortcut for BGP next-hop resolution, a static-route next-hop resolution, or for an IGP route resolution.

A transit packet is a packet received from an IP interface and forwarded over the LSP shortcut at ingress LER.

A locally-generated IP packet is any control plane packet generated from the CPM and forwarded over the LSP shortcut at ingress LER.

TTL handling can be configured for all LDP LSP shortcuts originating on an ingress LER using the following global commands:

config>router>ldp>[**no**] **shortcut-transit-ttl-propagate**
config>router>ldp>[**no**] **shortcut-local-ttl-propagate**

These commands apply to all LDP LSPs which are used to resolve static routes, BGP routes, and IGP routes.

When the **no** form of the above command is enabled for local packets, TTL propagation is disabled on all locally generated IP packets, including ICMP Ping, traceroute, and OAM packets that are destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack. This is referred to as pipe mode.

Similarly, when the **no** form is enabled for transit packets, TTL propagation is disabled on all IP packets received on any IES interface and destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack.

LDP Process Overview

Figure 23 displays the process to provision basic LDP parameters.

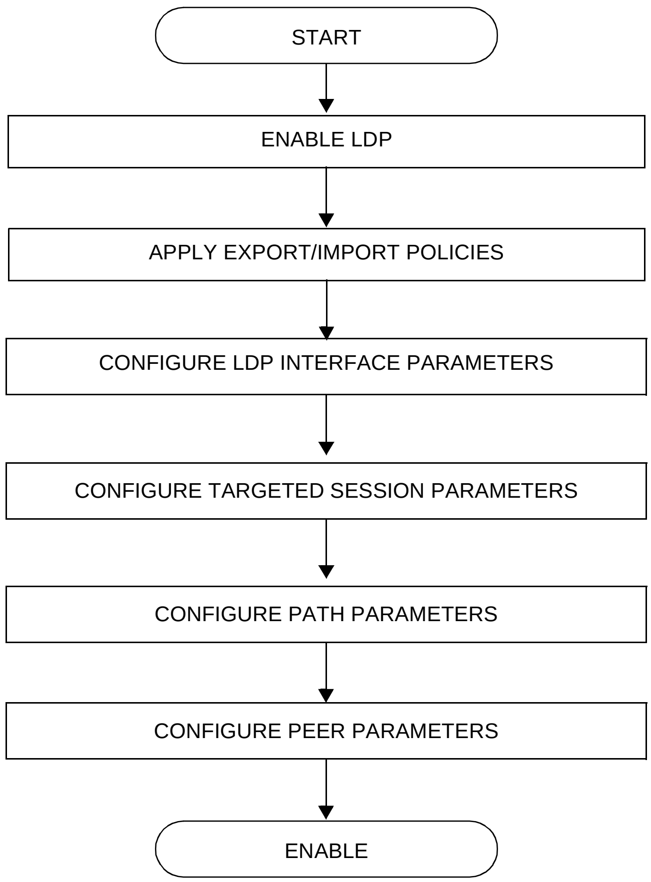

Figure 23: LDP Configuration and Implementation

Configuring LDP with CLI

This section provides information to configure LDP using the command line interface.

Topics in this section include:

LDP Configuration Overview

When the 7750 SR OS implementation of LDP is instantiated, the protocol is in the `no shutdown` state. In addition, targeted sessions are then enabled. The default parameters for LDP are set to the documented values for targeted sessions in *draft-ietf-mpls-ldp-mib-09.txt*.

LDP must be enabled in order for signaling to be used to obtain the ingress and egress labels in frames transmitted and received on the service distribution path (SDP). When signaling is *off*, labels must be manually configured when the SDP is bound to a service.

Basic LDP Configuration

This chapter provides information to configure LDP and remove configuration examples of common configuration tasks.

The LDP protocol instance is created in the `no shutdown` (enabled) state.

The following displays the default LDP configuration.

```
A:ALA-1>config>router>ldp# info
----------------------------------------------
            interface-parameters
            exit
            targeted-session
            exit
----------------------------------------------
A:ALA-1>config>router>ldp#
```

Common Configuration Tasks

This section provides information to configure:

Enabling LDP

LDP must be enabled in order for the protocol to be active. MPLS must also be enabled. MPLS is enabled in the `config>router>mpls` context.

Use the following syntax to enable LDP on a 7750 SR OS router:

CLI Syntax: `ldp`

Example: `config>router# ldp`

The following displays the enabled LDP configuration.

```
A:ALA-1>config>router# info
----------------------------------------------
...
#------------------------------------------
echo "LDP Configuration"
#------------------------------------------
        ldp
            interface-parameters
            exit
            targeted-session
            exit
```

```
        exit
----------------------------------------------
...
A:ALA-1>config>router#
```

Configuring FEC Originate Parameters

A FEC can be added to the LDP IP prefix database with a specific label operation on the node. Permitted operations are pop or swap. For a swap operation, an incoming label can be swapped with a label in the range of 16 to 1048575. If a swap- label is not configured then the default value is 3.

A route table entry is required for a FEC with a pop operation to be advertised. For a FEC with a swap operation, a route-table entry must exist and user configured next-hop for swap operation must match one of the next-hops in route-table entry.

Use the following syntax to configure FEC originate parameters:

CLI Syntax:
```
config>router>ldp
  fec-originate ip-prefix/mask [advertised-label in-label]
     next-hop ip-address [swap-label out-label]
  fec-originate ip-prefix/mask [advertised-label in-label] pop
```

The following displays a FEC originate configuration example.

```
A:ALA-5>config>router# info
----------------------------------------------
            fec-originate 100.1.1.1/32 pop
            fec-originate 100.2.1.1/32 advertised-label 1000 next-hop 10.10.1.2
            fec-originate 100.3.1.1/32 advertised-label 1001 next-hop 10.10.2.3
              swap-label 131071
            interface-parameters
            exit
            targeted-session
            exit
        exit
----------------------------------------------
A:ALA-5>config>router>ldp#
```

Configuring Graceful-Restart Helper Parameters

Graceful-restart helper advertises to its LDP neighbors by carrying the fault tolerant (FT) session TLV in the LDP initialization message, assisting the LDP in preserving its IP forwarding state across the restart. Alcatel-Lucent’s recovery is self-contained and relies on information stored internally to self-heal. This feature is only used to help third-party routers without a self-healing capability to recover.

Maximum recovery time is the time (in seconds) the sender of the TLV would like the receiver to wait, after detecting the failure of LDP communication with the sender.

Neighbor liveness time is the time (in seconds) the LSR is willing to retain its MPLS forwarding state. The time should be long enough to allow the neighboring LSRs to re-sync all the LSPs in a graceful manner, without creating congestion in the LDP control plane.

Use the following syntax to configure graceful-restart parameters:

CLI Syntax:
```
config>router>ldp
     [no] graceful-restart
```

Applying Export and Import Policies

Both inbound and outbound label binding filtering are supported. Inbound filtering allows a route policy to control the label bindings an LSR accepts from its peers. An import policy can accept or reject label bindings received from LDP peers.

Label bindings can be filtered based on:

- Neighbor — Match on bindings received from the specified peer.
- Interface — Match on bindings received from a neighbor or neighbors adjacent over the specified interface.
- Prefix-list — Match on bindings with the specified prefix/prefixes.

Outbound filtering allows a route policy to control the set of LDP label bindings advertised by the LSR. An export policy can control the set of LDP label bindings advertised by the router. By default, label bindings for only the system address are advertised and propagate all FECs that are received. All other local interface FECs can be advertised using policies. Beware that the system IP address AND static FECs cannot be blocked using an export policy.

Matches can be based on:

- Loopback — loopback interfaces.
- All — all local subnets.
- Match — match on bindings with the specified prefix/prefixes.

Use the following syntax to apply import and export policies:

CLI Syntax:
```
config>router>ldp
  export policy-name [policy-name...(upto 32 max)]
  import policy-name [policy-name...(upto 32 max)]
```

The following displays export and import policy configuration examples.

```
A:ALA-1>config>router# info
----------------------------------------------
            export "LDP-export"
            fec-originate 100.1.1.1/32 pop
            fec-originate 100.2.1.1/32 advertised-label 1000 next-hop 10.10.1.2
            import "LDP-import"
            interface-parameters
            exit
            targeted-session
            exit
----------------------------------------------
A:ALA-1>config>router#
```

Targeted Session Parameters

Use the following syntax to specify `targeted-session` parameters:

CLI Syntax:
```
config>router# ldp
 targeted-session
    disable-targeted-session
    export-prefixes policy-name [policy-name...(up to 5 max)]
    hello timeout factor
    import-prefixes policy-name [policy-name...(up to 5 max)]
    keepalive timeout factor
    peer ip-address
       hello timeout factor
       keepalive timeout factor
       no shutdown
       tunneling
          lsp lsp-name
```

The following example displays an LDP configuration example:

```
A:ALA-1>config>router>ldp# info
----------------------------------------------
...
            targeted-session
                hello 5000 255
                keepalive 5000 255
                peer 10.10.10.104
                    hello 2500 104
                    keepalive 15 3
                exit
            exit
----------------------------------------------
A:ALA-1>config>router>ldp#
```

Interface Parameters

Use the following syntax to configure interface parameters:

CLI Syntax:
```
config>router# ldp
 interface-parameters
    hello timeout factor
    keepalive timeout factor
    transport-address {system|interface}
    interface ip-int-name
       hello timeout factor
       keepalive timeout factor
       transport-address {system|interface}
       no shutdown
```

The following example displays an interface parameter configuration example:

```
A:ALA-1>config>router>ldp# info
----------------------------------------------
...
            targeted-session
                no disable-targeted-session
                hello 5000 255
                keepalive 5000 255
                peer 10.10.10.104
                    hello 2500 104
                    keepalive 15 3
                    no shutdown
                exit
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>router>ldp#
```

Peer Parameters

Use the following syntax to specify interface parameters:

CLI Syntax:
```
config>router# ldp
  peer-parameters
    peer ip-address
      auth-keychain name
      authentication-key [authentication-key|hash-key]
      [hash|hash2]
      ttl-security min-ttl-value [log log-id]
```

The following example displays an LDP configuration example:

```
A:ALA-1>config>router>ldp# info
----------------------------------------------
            export "LDP-export"
            import "LDP-import"
            peer-parameters
                peer 10.10.10.104
                    authentication-key "3WErEDozxyQ" hash
                exit
            exit
            interface-parameters
                interface "test"
                exit
                interface "to-104"
                    hello 15 3
                exit
            exit
            targeted-session
                hello 5000 255
                keepalive 5000 255
                peer 10.10.10.104
                    hello 2500 100
                    keepalive 15 3
                exit
            exit
----------------------------------------------
A:ALA-1>config>router>ldp#
```

LDP Signaling and Services

When LDP is enabled, targeted sessions can be established to create remote adjacencies with nodes that are not directly connected. When service distribution paths (SDPs) are configured, extended discovery mechanisms enable LDP to send periodic targeted hello messages to the SDP's far-end point. The exchange of LDP hellos trigger session establishment. The SDP's signaling default enables **tldp**. The service SDP uses the targeted-session parameters configured in the **config>router>ldp>targeted-session** context.

The SDP's LDP and LSP commands are mutually exclusive; either one LSP can be specified or LDP can be enabled. If LDP is already enabled on an MPLS SDP, then an LSP cannot be specified on the SDP. If an LSP is specified on an MPLS SDP, then LDP cannot be enabled on the SDP.

To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the no lsp lsp-name command. For further information about configuring SDPs, refer to the 7750 SR OS Services Guide.

The following example displays the command syntax usage to configure enable LDP on an MPLS SDP:

CLI Syntax:
```
config>service>sdp#
  ldp
  signaling {off|tldp}
```

The following displays an example of an SDP configuration showing the signaling default `tldp` enabled.

```
A:ALA-1>config>service>sdp# info detail
----------------------------------------------
            description "MPLS: to-99"
            far-end 10.10.10.99
            ldp
            signaling tldp
            path-mtu 4462
            keep-alive
                hello-time 10
                hold-down-time 10
                max-drop-count 3
                timeout 5
                no message-length
                no shutdown
            exit
            no shutdown
----------------------------------------------
A:ALA-1>config>service>sdp#
```

The following shows a working configuration of LDP over RSVP-TE (1) where tunnels look like the second example (2):

1.

```
*A:ALA-1>config>router>ldp# info
----------------------------------------------
            prefer-tunnel-in-tunnel
            interface-parameters
                interface "port-1/1/3"
                exit
                interface "port-lag-1"
                exit
            exit
            targeted-session
                peer 10.51.0.1
                    shutdown
                    tunneling
                        lsp "to_P_1"
                    exit
                exit
                peer 10.51.0.17
                    shutdown
                    tunneling
                        lsp "to_P_6"
                    exit
                exit
            exit
----------------------------------------------
*A:ALA-1>config>router>ldp#
```

2.

```
*A:ALA-1>config>router>mpls# info
----------------------------------------------
            resignal-timer 30
            admin-group "lower" 2
            admin-group "upper" 1
            interface "system"
            exit
            interface "port-1/1/3"
            exit
            interface "port-lag-1"
            exit
            path "dyn"
                no shutdown
            exit
            lsp "to_P_1"
                to 10.51.0.1
                cspf
                fast-reroute facility
                exit
                primary "dyn"
                exit
                no shutdown
            exit
            lsp "to_P_6"
                to 10.51.0.17
                cspf
                fast-reroute facility
                exit
                primary "dyn"
```

```
                exit
                no shutdown
            exit
            no shutdown
----------------------------------------------
*A:ALA-1>config>router>mpls#
```

LDP Configuration Management Tasks

This section discusses the following LDP configuration management tasks:

- Disabling LDP on page 323
- Modifying Targeted Session Parameters on page 324
- Modifying Interface Parameters on page 325
- Modifying Interface Parameters on page 325

Disabling LDP

The `no ldp` command disables the LDP protocol on the router. All parameters revert to the default settings. LDP must be shut down before it can be disabled.

Use the following command syntax to disable LDP:

CLI Syntax:
```
no ldp
 shutdown
```

Modifying Targeted Session Parameters

You can modify LDP parameters without shutting down entities. The changes take effect immediately. Individual parameters cannot be deleted. The `no` form of a **targeted-session** parameter command reverts modified values back to the default.

The following example displays the command syntax usage to revert targeted session parameters back to the default values:

Example:

```
config>router# ldp
config>router>ldp# targeted-session
config>router>ldp>targeted# no authentication-key
config>router>ldp>targeted# no disable-targeted-session
config>router>ldp>targeted# no hello
config>router>ldp>targeted# no keepalive
config>router>ldp>targeted# no peer 10.10.10.99
```

The following output displays the default values:

```
A:ALA-1>config>router>ldp>targeted# info detail
----------------------------------------------
                no disable-targeted-session
                hello 45 3
                keepalive 40 4
----------------------------------------------
A:ALA-1>config>router>ldp>targeted#
```

Modifying Interface Parameters

You can modify LDP interface parameters without shutting down entities. The changes take effect immediately. Individual parameters cannot be deleted. The **no** form of a **interface-parameter** command reverts modified values back to the defaults.

The following output displays the default values:

```
A:ALA-1>config>router>ldp>targeted# info detail
----------------------------------------------
                hello 15 3
                keepalive 30 3
                no transport-address
----------------------------------------------
A:ALA-1>config>router>ldp>targeted#
```

LDP Command Reference

Command Hierarchies

LDP Commands

config
— **router**
— [**no**] **ldp**
— [**no**] **aggregate-prefix-match**
— **prefix-exclude** ***policy-name*** [***policy-name***...(up to 5 max)]
— **no prefix-exclude**
— [**no**] **shutdown**
— **egress-statistics**
— [**no**] **fec-prefix** *ip-prefix[/mask]*
— **accounting-policy** *policy-id*
— **no accounting-policy**
— [**no**] **collect-stats**
— [**no**] **shutdown**
— **export** *policy-name* [*policy-name*...(up to 5 max)]
— **no export**
— **[no] export-tunnel-table** *policy-name*
— **fec-originate** *ip-prefix/mask* [**advertised-label in-label**] **next-hop** *ip-address* [**swap-label** *out-label*]
— **fec-originate** *ip-prefix/mask* [**advertised-label in-label**] **pop**
— **no fec-originate** *ip-prefix/mask* **next-hop** *ip-address*
— **no fec-originate** *ip-prefix/mask* **pop**
— [**no**] **graceful-restart**
— **maximum-recovery-time** *interval*
— **no maximum-recovery-time**
— **neighbor-liveness-time** *interval*
— **no neighbor-liveness-time**
— [**no**] **implicit-null-label**
— **import** *policy-name* [*policy-name*...(u pto 5 max)]
— **no import**
— **interface-parameters**
— **hello** *timeout factor*
— **no hello**
— [**no**] **interface** *ip-int-name*
— **hello** *timeout factor*
— **no hello**
— **keepalive** *timeout factor*
— **no keepalive**
— **multicast-traffic** **{enable|disable}**
— **local-lsr-id** {**system** | **interface**}

— **no local-lsr-id**
— [**no**] **shutdown**
— **transport-address** {**system** | **interface**}
— **no transport-address**
— **keepalive** *timeout factor*
— **no keepalive**
— **transport-address** {**system** | **interface**}
— **no transport-address**
— **label-withdrawal-delay** *seconds*
— **peer-parameters**
— **peer** *ip-address*
— **no peer** [*ip-address*]
— **auth-keychain** *name*
— **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
— **no authentication-key**
— [**no**] **dod-label-distribution**
— [**no**] **export-prefixes** ***policy-name***
— [**no**] **fec129-cisco-interop**
— [**no**] **import-prefixes** *policy-name*
— **ttl-security** *min-ttl-value*
— **[no] ttl-security**
— **[no] p2mp-mbb-time**
— [**no**] **prefer-tunnel-in-tunnel**
— [**no**] **shortcut-transit-ttl-propagate**
— [**no**] **shortcut-local-ttl-propagate**
— [**no**] **shutdown**
— **targeted-session**
— [**no**] **disable-targeted-session**
— **export-prefixes** *policy-name* [*policy-name*...(up to 5 max)]
— **no export-prefixes**
— **hello** *timeout factor*
— **no hello**
— **import-prefixes** *policy-name* [*policy-name*...(up to 5 max)]
— **no import-prefixes**
— **keepalive** *timeout factor*
— **no keepalive**
— **local-lsr-id** *interface-name*
— **no local-lsr-id**
— **peer** *ip-address*
— **no peer** *ip-address*
— [**no**] **bfd-enable**
— **hello** *timeout factor*
— **no hello**
— **keepalive** *timeout factor*
— **no keepalive**
— **local-lsr-id** *interface-name*
— **no local-lsr-id**
— [**no**] **shutdown**
— **tunnel-down-damp-time** *seconds*
— **no tunnel-down-damp-time**
— [**no**] **ldp-shortcut**

Show Commands

show
— **router**
— **ldp**
— **auth-keychain** [*keychain*]
— **bindings**[**fec-type** *fec-type* [**detail** | **summary**]] [**session** *ip-addr*[:*label-space*]]
— **bindings** [*label-type*] [*start-label* [*end-label*]
— **bindings** {**prefix** *ip-prefix/mask* [**detail**]}[**session** *ip-addr*[:*label-space*]]
— **bindings** **active** [**prefix** *ip-prefix/mask*] [**summary** | **egress-nh** *ip-prefix/mask* | **egress-if** *port-id* | **egress-lsp** *tunnel-id*]
— **bindings** **service-id** *service-id* [**detail**]
— **bindings** **vc-type** *vc-type* [{**vc-id** *vc-id*| **agi** *agi*} [**session** *ip-addr*[:*lab el-space*]]]
— **discovery** [{**peer** [*ip-address*]} | {**interface** [*ip-int-name*]}] [**state** *state*] [**detail**] [**adjacency-type** *type*]
— **fec-egress-stats** [*ip-prefix/mask*]
— **fec-egress-stats** **active**
— **fec-originate** *ip-prefix/mask* [*operation-type*]
— **interface** [*ip-int-name* | *ip-address*] [**detail**]
— **parameters**
— **peer** [*ip-address*] [**detail**]
— **peer-parameters** *peer-ip-address*
— **session** [*ip-addr*[:*label-space*]] [**detail** | **statistics** [*packet-type*]] [*session-type*]
— **status**

Note: Refer to the OS OAM and Diagnostics Guide for tools command descriptions, syntax, and usage information.

Clear Commands

clear
— **router**
— **ldp**
— **fec-egress-statistics** [*ip-prefix/mask*]
— **instance**
— **interface** [*ip-int-name*]
— **peer** [*ip-address*] [**statistics**]
— **session** [*ip-addr*[:*label-space*]] [**statistics**]
— **statistics**

Debug Commands

[**no**] **debug**
— **router**
— [**no**] **ldp**
— [**no**] **interface** ***interface-name***
— [**no**] **event**
— [**no**] **messages**
— [**no**] **packet** [**detail**]
— **hello** [**detail**]
— **no hello**
— **peer** ***ip-address***
— [**no**] **event**
— [**no**] **bindings**
— [**no**] **messages**
— [**no**] **packet**
— **hello** [**detail**]
— **no hello**
— **init** [**detail**]
— **no init**
— [**no**] **keepalive**
— **label** [**detail**]
— **no label**

Tools Commands

See 7750 SR OS OAM and Diagnostics Guide for CLI description and syntax.

tools
— **dump**
— **ldp-treetrace** {**prefix** *ip-prefix/mask*| **manual-prefix** *ip-prefix/mask*}[**path-destination** *ip-address*] [**trace-tree**]

LDP Configuration Commands

Generic Commands

ldp

Syntax [**no**] **ldp**

Context config>router

Default This command creates the context to configure an LDP parameters. LDP is not enabled by default and must be explicitely enabled (**no shutdown**).

To suspend the LDP protocol, use the **shutdown** command. Configuration parameters are not affected.

The **no** form of the command deletes the LDP protocol instance, removing all associated configuration parameters. The LDP instance must first be disabled with the **shutdown** command before being deleted.

Default none (LDP must be explicitly enabled)

ldp-shortcut

Syntax [**no**] **ldp-shortcut**

Context config>router

Description This command enables the resolution of IGP routes using LDP LSP across all network interfaces participating in the IS-IS and OSPF routing protocol in the system.

When LDP shortcut is enabled, LDP populates the routing table with next-hop entries corresponding to all prefixes for which it activated an LDP FEC. For a given prefix, two route entries are populated in the system routing table. One corresponds to the LDP shortcut next-hop and has an owner of LDP. The other one is the regular IP next-hop. The LDP shortcut next-hop always has preference over the regular IP next-hop for forwarding user packets and specified control packets over a given outgoing interface to the route next-hop.

All user and specified control packets for which the longest prefix match in RTM yields the FEC prefix will be forwarded over the LDP LSP.

When an IPv4 packet is received on an ingress network interface, a subscriber IES interface, or a regular IES interface, the lookup of the packet by the ingress IOM will result in the packet being sent labeled with the label stack corresponding to the NHLFE of the LDP LSP when the preferred RTM entry corresponds to an LDP shortcut.

If the preferred RTM entry corresponds to an IP next-hop, the IPv4 packet is forwarded unlabelled.

When ECMP is enabled and multiple equal-cost next-hops exit for the IGP route, the ingress IOM will spray the packets for this route based on hashing routine currently supported for IPv4 packets.

When the preferred RTM entry corresponds to an LDP shortcut route, spraying will be performed across the multiple next-hops for the LDP FEC. The FEC next-hops can either be direct link LDP neighbors or T-LDP neighbors reachable over RSVP LSPs in the case of LDP-over-RSVP but not both.

When the preferred RTM entry corresponds to a regular IP route, spraying will be performed across regular IP next-hops for the prefix..

The **no** form of this command disables the resolution of IGP routes using LDP shortcuts.

Default no ldp-shortcut

shutdown

Syntax [**no**] **shutdown**

Context config>router>ldp
config>router>ldp>if-params>if
config>router>ldp>targ-session>peer
config>router>ldp>egr-stats>fec-prefix
config>router>ldp>aggregate-prefix-match

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The **no** form of this command administratively enables an entity.

Unlike other commands and parameters where the default state is not indicated in the configuration file, the **shutdown** and **no shutdown** states are always indicated in system generated configuration files.

The **no** form of the command places an entity in an administratively enabled state.

Default **no shutdown**

aggregate-prefix-match

Syntax [**no**] **aggregate-prefix-match**

Context config>router>ldp

Description The command enables the use by LDP of the aggregate prefix match procedures.

When this option is enabled, LDP performs the following procedures for all prefixes. When an LSR receives a FEC-label binding from an LDP neighbor for a given specific FEC1 element, it will install the binding in the LDP FIB if:

- It is able to perform a successful longest IP match of the FEC prefix with an entry in the routing table, and
- The advertising LDP neighbor is the next-hop to reach the FEC prefix.

When such a FEC-label binding has been installed in the LDP FIB, then LDP programs an NHLFE entry in the egress data path to forward packets to FEC1. It also advertises a new FEC-label binding for FEC1 to all its LDP neighbors.

When a new prefix appears in the routing table, LDP inspects the LDP FIB to determine if this prefix is a better match (a more specific match) for any of the installed FEC elements. For any FEC for which this is true, LDP may have to update the NHLFE entry for this FEC.

When a prefix is removed from the routing table, LDP inspects the LDP FIB for all FEC elements which matched this prefix to determine if another match exists in the routing table. If so, it updates the NHLFE entry accordingly. If not, it sends a label withdraw message to its LDP neighbors to remove the binding.

When the next hop for a routing prefix changes, LDP updates the LDP FIB entry for the FEC elements which matched this prefix. It also updates the NHLFE entry for these FEC elements accordingly.

The **no** form of this command disables the use by LDP of the aggregate prefix procedures and deletes the configuration. LDP resumes performing exact prefix match for FEC elements.

Default no aggregate-prefix-match

prefix-exclude

Syntax **prefix-exclude** *policy-name* [*policy-name*...(up to 5 max)]
no prefix-exclude

Context config>router>ldp>aggregate-prefix-match

Description This command specifies the policy name containing the prefixes to be excluded from the aggregate prefix match procedures. In this case, LDP will perform an exact match of a specific FEC element prefix as opposed to a longest match of one or more LDP FEC element prefixes, against this prefix when it receives a FEC-label binding or when a change to this prefix occurs in the routing table.

The **no** form of this command removes all policies from the configuration.

Default no prefix-exclude.

egress-statistics

Syntax **egress-statistics**

Context config>router>ldp

Description This command provides the context for the user to enter the LDP FEC prefix for the purpose of enabling egress data path statistics at the ingress LER for this FEC.

Default none

fec-prefix

Syntax [**no**] **fec-prefix** *ip-prefix[/mask]*

Context config>router>ldp>egr-stats

Description This command configures statistics in the egress data path at the ingress LER or LSR for an LDP FEC. The user must execute the **no shutdown** command for this command to effectively enable statistics.

The egress data path counters will be updated for both originating and transit packets. Originating packets may be service packets or IP user and control packets forwarded over the LDP LSP when used as an IGP shortcut. Transit packets of the FEC which are label switched on this node.

When ECMP is enabled and multiple paths exist for a FEC, the same set of counters are updated for each packet forwarded over any of the NHLFEs associated with this FEC and for as long as this FEC is active.

The statistics can be enabled on prefix FECs imported from both LDP neighbors and T-LDP neighbors (LDP over RSVP).Only /32 FEC prefixes are accepted. Service FECs, i.e., FEC 128 and FEC 129 are not valid.

The **no** form of this command disables the statistics in the egress data path and removes the accounting policy association from the LDP FEC.

Default none

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context config>router>ldp>egr-stats

Description This command associates an accounting policy to the MPLS instance.

An accounting policy must be defined before it can be associated else an error message is generated.

The **no** form of this command removes the accounting policy association.

Default none

Parameters *acct-policy-id* — Enter the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 — 99

collect-stats

Syntax [**no**] **collect-stats**

Context config>router>ldp>egr-stats

Description This command enables accounting and statistical data collection. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the IOMCFM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default collect-stats

export

Syntax **export** *policy-name* [*policy-name …*upto 5 max]
no export

Context config>router>ldp

Description This command specifies the export route policies used to determine which routes are exported to LDP. Policies are configured in the **config>router>policy-options** context.

If no export policy is specified, non-LDP routes will not be exported from the routing table manager to LDP. LDP-learned routes will be exported to LDP neighbors. Present implementation of export policy (outbound filtering) can be used “only” to add FECs for label propagation. The export policy does not stop propagation of FECs that an LSR receives from its neighbors.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of the command removes all policies from the configuration.

Default **no export** — No export route policies specified.

Parameters *policy-name* — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

export-tunnel-table

Syntax **[no] export-tunnel-table** *policy-name*

Context config>router>ldp

Description This command applies a tunnel table export policy to LDP for the purpose of learning BGP labeled routes from the CPM tunnel table and stitching them to LDP FEC for the same prefix.

The user enables the stitching of routes between LDP and BGP by configuring separately tunnel table route export policies in both protocols and enabling the advertising of RFC 3107 formatted labeled routes for prefixes learned from LDP FECs.

The route export policy in BGP instructs BGP to listen to LDP route entries in the CPM Tunnel Table. If a /32 LDP FEC prefix matches an entry in the export policy, BGP originates a BGP labeled route, stitches it to the LDP FEC, and re-distributes the BGP labeled route to its iBGP neighbors.

The user adds LDP FEC prefixes with the statement '**from protocol ldp**' in the configuration of the existing BGP export policy at the global level, the peer-group level, or at the peer level using the commands:

- **configure>router>bgp>export policy-name**
- **configure>router>bgp>group>export policy-name**
- **configure>router>bgp>group>neighbour>export policy-name**

To indicate to BGP to evaluate the entries with the '**from protocol ldp**' statement in the export policy when applied to a specific BGP neighbor, a new argument is added to the existing advertise-label command:

configure>router>bgp>group>neighbour>advertise-label ipv4 include-ldp-prefix

Without the new **include-ldp-prefix** argument, only core IPv4 routes learned from RTM are advertised as BGP labeled routes to the neighbor. No stitching of LDP FEC to the BGP labeled route will be performed for this neighbor even if the same prefix was learned from LDP.

The tunnel table route export policy in LDP instructs LDP to listen to BGP route entries in the CPM Tunnel Table. If a /32 BGP labeled route matches a prefix entry in the export policy, LDP originates an LDP FEC for the prefix, stitches it to the BGP labeled route, and re-distributes the LDP FEC to its iBGP neighbors.

The user can add BGP labeled route prefixes with the statement '**from protocol bgp**' in the configuration of the LDP tunnel table export policy. Note that the '**from protocol**' statement has an effect only when the protocol value is ldp. Policy entries with protocol values of rsvp, bgp, or any value other than ldp are ignored at the time the policy is applied to LDP.

The **no** form of the command removes the policy from the configuration.

Default **no export-tunnel-table** — no tunnel table export route policy is specified.

Parameters *policy-name* — The export-tunnel-table route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string. The specified name(s) must already be defined.

fec-originate

Syntax **fec-originate** *ip-prefix/mask* [**advertised-label** *in-label*] **next-hop** *ip-address* [**swap-label** *out-label*]
fec-originate *ip-prefix/mask* [**advertised-label** *in-label*] **pop**
no fec-originate *ip-prefix/mask* **next-hop** *ip-address*
no fec-originate *ip-prefix/mask* **pop**

Context config>router>ldp

Description This command defines a way to originate a FEC (with a swap action) for which the LSR is not egress, or to orginate a FEC (with a pop action) for which the LSR is egress.

Parameters *ip-prefix/mask* — Specify information for the specified IP prefix and mask length.

next-hop — Specify the IP address of the next hop of the prefix.

advertised-label — Specify the label advertised to the upstream peer. If not configured, then the label advertised should be from the label pool. If the configured static label is not available then the IP prefix is not advertised.

out-label — Specify the LSR to swap the label. If configured, then the LSR should swap the label with the configured swap-label. If not configured, then the default action is pop if the next-hop parameter is not defined.

NOTE: The next-hop, advertised-label, swap-label parameters are all optional. If next-hop is configured but no swap label specified, then it will be a swap with label 3, such as, pop and forward to the next-hop. If the next-hop and swap-label are configured, then it is a regular swap. If no parameters are specified, then a pop and route is performed.

Values 16 — 1048575

in-label — Specifies the number of labels to send to the peer associated with this FEC.

Values 32 — 1023

pop — Specifies to pop the label and transmit without the label.

graceful-restart

Syntax [**no**] **graceful-restart**

Context config>router>ldp

Description This command enables graceful restart helper.

The **no** form of the command disables graceful restart.

Default **no graceful-restart** (**disabled**) — Graceful-restart must be explicitely enabled.

implicit-null-label

Syntax [**no**] **implicit-null-label**

Context config>router>ldp

Description This command enables the use of the implicit null label. Use this command to signal the IMPLICIT NULL option for all LDP FECs for which this node is the egress LER.

The **no** form of this command disables the signaling of the implicit null label.

Default **no implicit-null-label**

maximum-recovery-time

Syntax **maximum-recovery-time** *interval*
no maximum-recovery-time

Context config>router>ldp

Description This command configures the local maximum recovery time.

The **no** form of the command returns the default value.

Default 120

Parameters *interval* — Specifies the length of time in seconds.

Values 15 — 1800

neighbor-liveness-time

Syntax **neighbor-liveness-time** *interval*
no neighbor-liveness-time

Context config>router>ldp

Description This command configures the neighbor liveness time.

The **no** form of the command returns the default value.

Default 120

Parameters *interval* — Specifies the length of time in seconds.

Values 5 — 300

import

Syntax **import** *policy-name* [*policy-name …*upto 5 max]
no import

Context config>router>ldp

Description This command configures import route policies to determine which routes are accepted from LDP neighbors. Policies are configured in the **config>router>policy-options** context.

If no import policy is specified, LDP accepts all routes from configured LDP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of the command removes all policies from the configuration.

Default **no import** — No import route policies specified.

Parameters *policy-name* — The import route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

label-withdrawal-delay

Syntax **label-withdrawal-delay** *seconds*

Context config>router>ldp

Description This command specifies configures the time interval, in seconds, LDP will delay for the withdrawal of FEC-label binding it distributed to its neighbors when FEC is de-activated. When the timer expires, LDP then sends a label withdrawal for the FEC to all its neighbous. This is applicable only to LDP transport tunnels (IPv4 prefix FECs) and is not applicable to pseudowires (service FECs).

Default no label-withdrawal-delay

Parameters *seconds* — Specifies the time that LDP delays the withdrawal of FEC-label binding it distributed to its neighbors when FEC is de-activated.

Values 3 — 120

tunnel-down-damp-time

Syntax **tunnel-down-damp-time** *seconds*
no tunnel-down-damp-time

Context config>router>ldp

Description This command specifies the time interval, in seconds, that LDP waits before posting a tunnel down event to the Route Table Manager. If a tunnel up, an event is generated before the damping interval has elapsed. A tunnel modify event will be posted to the Route Table Manager (RTM).

The **no** form of this command then tunnel down events are not damped.

Parameters *seconds* — The time interval, in seconds, that LDP waits before posting a tunnel down event to the Route Table Manager.

keepalive

Syntax **keepalive** *timeout factor*
no keepalive

Context config>router>ldp>if-params
config>router>ldp>if-params>if
config>router>ldp>targ-session
config>router>ldp>targ-session>peer

Description This command configures the time interval, in seconds, that LDP waits before tearing down the session. The **factor** parameter derives the keepalive interval.

If no LDP messages are exchanged for the configured time interval, the LDP session is torn down. Keepalive timeout is usually three times the keepalive interval. To maintain the session permanently, regardless of the activity, set the value to zero.

When LDP session is being set up, the keepalive timeout is negotiated to the lower of the two peers. Once a operational value is agreed upon, the keepalive factor is used to derive the value of the keepalive interval.

The **no** form of the command at the interface-parameters and targeted-session levels sets the **keepalive timeout** and the **keepalive factor** to the default value.

The **no** form of the command, at the interface level, sets the **keepalive timeout** and the **keepalive factor** to the value defined under the **interface-parameters** level.

The **no** form of the command, at the peer level, will set the **keepalive timeout** and the **keepalive factor** to the value defined under the **targeted-session** level.

Default

Context	timeout	factor
config>router>ldp>if-params	30	3
config>router>ldp>targ-session	40	4
config>router>ldp>if-params>if	Inherits values from interface-parameters context.	
config>router>ldp>targ-session>peer	Inherits values from targeted-session context.	

Parameters *timeout* — Configures the time interval, expressed in seconds, that LDP waits before tearing down the session.

Values 1 — 65535

factor — Specifies the number of keepalive messages, expressed as a decimal integer, that should be sent on an idle LDP session in the keepalive timeout interval.

Values 1 — 255

local-lsr-id

Syntax **local-lsr-id** {**system | interface**}
no local-lsr-id

Context config>router>ldp>interface-parameters>interface

Description This command enables the use of the address of the local LDP interface as the LSR-ID to establish a link LDP adjacency and session with a directly connected LDP peer.

By default, the LDP session uses the system interface address as the LSR-ID unless explicitly configured using the above command. Note however that the system interface must always be configured on the router or the LDP protocol will not come up on the node. There is no requirement to include it in any routing protocol though.

At initial configuration, the LDP session to the peer will remain down while the interface is down.

If the user changes the LSR-ID on the fly between system and interface values while the LDP session is up, LDP will immediately tear down the session and will attempt to re-establish it using the new LSR-ID.

If the interface used as LSR-ID goes down, then the LDP session goes down.

Note that when the interface option is selected, the transport connection (TCP) for the link LDP session will also use the address of the local LDP interface as the transport address. If system is the value configured in the **configure>router>ldp>interface-parameters>interface>transport-address** context it will be overridden.

The **no** form of the command returns to the default behavior in which case the system interface address is used as the LSR-ID.

Default system.

local-lsr-id

Syntax **local-lsr-id** *interface-name*
no local-lsr-id

Context config>router>ldp>targeted-session>peer

Description This command enables the use the use of the address of a specific interface as the LSR-ID for the hello adjacency of a T-LDP session. The interface can be a regular interface or a loopback interface, including the system interface.

By default, a T-LDP session uses the system interface address as the LSR-ID. Note however that the system interface must always be configured on the router or the LDP protocol will not come up on the node. There is no requirement to include it in any routing protocol though.

At initial configuration, the T-LDP session will remain down while the specified interface is down. LDP will not try to bring it up using the system interface.

If the user changes the LSR-ID on the fly while the T-LDP session is up, LDP will immediately tear down the session and will attempt to establish one using the new LSR-ID regardless of operational state of new specified interface.

If the interface used as LSR-ID goes down, then the T-LDP session will go down.

The user configured LSR-ID is used exclusively for extended peer discovery to establish the T-LDP hello adjacency. It is also used as the transport address for the TCP session of the LDP session when it is bootstrapped by the T-LDP hello adjacency. The user configured LSR-ID is however not used in basic peer discovery to establish a link-level LDP hello adjacency.

The **no** form of this command returns to the default behavior in which case the system interface address is used as the LSR-ID.

Default no local-lsr-id.

Parameters *interface-name* — Specifies the name, up to 32 characters in length, of the network IP interface. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

tunneling

Syntax [**no**] **tunneling**

Context config>router>ldp>targ-session>peer

Description This command enables LDP over tunnels.

The **no** form of the command disables tunneling.

Default **no tunneling**

lsp

Syntax [**no**] **lsp** *lsp-name*

Context config>router>ldp>targ-session>tunneling

Description This command configures a specific LSP destined to this peer and to be used for tunneling of LDP FEC over RSVP. A maximum of 4 RSVP LSPs can be explicitly used for tunneling LDP FECs to the T-LDP peer.

It is not necessary to specify any RSVP LSP in this context unless there is a need to restrict the tunneling to selected LSPs. All RSVP LSPs with a to address matching that of the T-LDP peer are eligible by default. The user can also exclude specific LSP names by using the ldp-over-rsvp exclude command in the **configure->router->mpls->lsp** *lsp-name* context.

Interface Parameters Commands

interface-parameters

Syntax **interface-parameters**

Context config>router>ldp

Description This command enables the context to configure LDP interfaces and parameters applied to LDP interfaces.

hello

Syntax **hello** *timeout factor*
no hello

Context config>router>ldp>if-params
config>router>ldp>if-params>if
config>router>ldp>targ-session
config>router>ldp>targ-session>peer

Description This command configures the time interval to wait before declaring a neighbor down. The **factor** parameter derives the hello interval.

Hold time is local to the system and sent in the hello messages to the neighbor. Hold time cannot be less than three times the hello interval. The hold time can be configured globally (applies to all LDP interfaces) or per interface. The most specific value is used.

When LDP session is being set up, the holddown time is negotiated to the lower of the two peers. Once a operational value is agreed upon, the hello factor is used to derive the value of the hello interval.

The **no** form of the command at the interface-parameters and targeted-session level sets the **hello timeout** and the **hello factor** to the default values.

The **no** form of the command, at the interface level, will set the **hello timeout** and the **hello factor** to the value defined under the interface-parameters level.

The **no** form of the command, at the peer level, will set the **hello timeout** and the **hello factor** to the value defined under the targeted-session level.

Default

Context	Timeout	Factor
config>router>ldp>if-params	15	3
config>router>ldp>targ-session	45	3
config>router>ldp>if-params>if	Inherits values from interface-parameters context.	
config>router>ldp>targ-session>peer	Inherits values from targeted-session context.	

Parameters *timeout* — Configures the time interval, in seconds, that LDP waits before a neighbor down.

Values 1 — 65535

factor — Specifies the number of keepalive messages that should be sent on an idle LDP session in the hello timeout interval.

Values 1 — 255

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>router>ldp>if-params

Description This command enables LDP on the specified IP interface.

The **no** form of the command deletes the LDP interface and all configuration information associated with the LDP interface.

The LDP interface must be disabled using the **shutdown** command before it can be deleted.

Parameters *ip-int-name* — The name of an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

transport-address

Syntax **transport-address** {**interface** | **system**}
no transport-address

Context config>router>ldp>if-params
config>router>ldp>if-params>if

Description This command configures the transport address to be used when setting up the LDP TCP sessions. The transport address can be configured as **interface** or **system**. The transport address can be configured globally (applies to all LDP interfaces) or per interface. The most specific value is used.

With the transport-address command, you can set up the LDP interface to the connection which can be set to the interface address or the system address. However, there can be an issue of which address to use when there are parallel adjacencies. This situation can not only happen with parallel links, it could be a link and a targeted adjacency since targeted adjacencies request the session to be set up only to the system IP address.

Note that the **transport-address** value should not be **interface** if multiple interfaces exist between two LDP neighbors. Depending on the first adjacency to be formed, the TCP endpoint is chosen. In other words, if one LDP interface is set up as **transport-address interface** and another for **transport-address system**, then, depending on which adjacency was set up first, the TCP endpoint addresses are determined. After that, because the hello contains the LSR ID, the LDP session can be checked to verify that it is set up and then match the adjacency to the session.

Note that for any given ILDP interface, as the **local-lsr-id** parameters is changed to **interface**, the **transport-address** configuration loses effectiveness. Since it will be ignored and the ILDP session will *always* use the relevant interface IP address as transport-address even though system is chosen.

The **no** form of the command, at the global level, sets the transport address to the default value. The **no** form of the command, at the interface level, sets the transport address to the value defined under the global level.

Default **system** — The system IP address is used.

Parameters **interface —** The IP interface address is used to set up the LDP session between neighbors. The transport address interface cannot be used if multiple interfaces exist between two neighbors, since only one LDP session is set up between two neighbors.

system — The system IP address is used to set up the LDP session between neighbors.

multicast-traffic

Syntax **multicast-traffic**

Context config>router>ldp>interface-parameters>interface

Description This command enables P2MP multicast traffic forwarding on the interface.

The **no** form of command disables P2MP LDP multicast traffic on the interface. P2MP tree branching out on the interface would not withdraw label map from the peer session on interface shutdown or multicast traffic is disabled. Session may exist on multiple parallel interfaces. Only forwarding entry is changed when interface is shutdown or multicast traffic support is disabled.

Default multicast-traffic enable

p2mp-mbb-time

Syntax **[no] mp-mbb-time**

Context config>router>ldp>

Description This command configures the maximum time a P2MP transit/bud node must wait before switching over to the new path if the new node does not send MBB TLV to inform of the availability of data plane.

The **no** form of command should configure the default timer of 3 seconds.

Default 3 seconds

Parameters *interval* — seconds.

Values 1-10 seconds

Peer Parameters Commands

peer-parameters

Syntax **peer-parameters**

Context config>router>ldp

Description This command enables the context to configure peer specific parameters.

peer

Syntax [**no**] **peer** *ip-address*

Context config>router>ldp>peer-parameters

Description This command configures parameters for an LDP peer.

Default **none**

Parameters *ip-addr* — The IP address of the LDP peer in dotted decimal notation.

auth-keychain

Syntax **auth-keychain** *name*

Context config>router>ldp>peer-parameters>peer

Description This command configures TCP authentication keychain to use for the session.

Parameters *name* — Specifies the name of the keychain to use for the specified TCP session or sessions. This keychain allows the rollover of authentication keys during the lifetime of a session up to 32 characters in length.

authentication-key

Syntax **authentication-key** [*authentication-key* **|** *hash-key*] [**hash | hash2**]
no authentication-key

Context config>router>ldp>peer-parameters>peer

Description This command specifies the authentication key to be used between LDP peers before establishing sessions. Authentication uses the MD-5 message-based digest.

The **no** form of this command disables authentication.

Default **none**

Parameters *authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 16 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of up 33 alphanumeric characters. If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** keyword is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

dod-label-distribution

Syntax [**no**] **dod-label-distribution**

Context config>router>ldp>peer-parameters>peer

Description This command enables the use of the LDP Downstream-on-Demand (DoD) label distribution procedures.

When this option is enabled, LDP will set the A-bit in the Label Initialization message when the LDP session to the peer is established. When both peers set the A-bit, they will both use the DoD label distribution method over the LDP session [rfc5036].

This feature can only be enabled on a link-level LDP session and therefore will apply to prefix labels only, not service labels.

As soon as the link LDP session comes up, the 7x50 will send a label request to its DoD peer for the FEC prefix corresponding to the peer’s LSR-id. The DoD peer LSR-id is found in the basic Hello discovery messages the peer used to establish the Hello adjacency with the 7x50.

Similarly if the 7x50 and the directly attached DoD peer entered into extended discovery and established a targeted LDP session, the 7x50 will immediately send a label request for the FEC prefix corresponding to the peer’s LSR-id found in the extended discovery messages.

However, the 7x50 node will not advertise any <FEC, label> bindings, including the FEC of its own LSR-id, unless the DoD peer requested it using a Label Request Message.

When the DoD peer sends a label request for any FEC prefix, the 7x50 will reply with a <FEC, label> binding for that prefix if the FEC was already activated on the 7x50. If not, the 7x50 replies with a notification message containing the status code of “no route.” The 7x50 will not attempt in the latter case to send a label request to the next-hop for the FEC prefix when the LDP session to this next-hop uses the DoD label distribution mode. Hence the reference to single-hop LDP DoD procedures.

As soon as the link LDP session comes up, the 7x50 will send a label request to its DoD peer for the FEC prefix corresponding to the peer’s LSR-id. The DoD peer LSR-id is found in the basic Hello discovery messages the peer used to establish the Hello adjacency with the 7x50.

Similarly if the 7x50 and the directly attached DoD peer entered into extended discovery and established a targeted LDP session, the 7x50 will immediately send a label request for the FEC prefix corresponding to the peer's LSR-id found in the extended discovery messages.

The no form of this command disables the DoD label distribution with an LDP neighbor.

Default no dod-label-distribution

export-prefixes

Syntax [**no**] **export-prefixes** *policy-name*

Context config>router>ldp>peer-parameters>peer

Description This command specifies the export route policy used to determine which FEC prefixes received from this peer over the LDP session to this peer are exported to other LDP and T-LDP peers. A prefix that is filtered out (deny) will not be exported. A prefix that is filtered in (accept) will be exported.

If no export policy is specified, all FEC prefixes learned from the LDP peer will be exported. This policy is applied in addition to the global LDP policy.

Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified.

The **no** form of the command removes the policy from the configuration.

Default no export-prefixes - no export route policy is specified

Parameters *policy-name* — The export-prefix route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string. The specified name(s) must already be defined.

fec129-cisco-interop

Syntax [**no**] **fec129-cisco-interop**

Context config>router>ldp>peer-parameters>peer

Description This command specifies whether LDP will provide translation between non-compliant FEC 129 formats of Cisco. Peer LDP sessions must be manually configured towards the non-compliant Cisco PEs.

When enabled, Cisco non-compliant format will be used to send and interpret received label release messages i.e. the FEC129 SAII and TAII fields will be reversed.

When the disabled, Cisco non-compliant format will not be used or supported.

The **no** form of the command returns the default .

Default no fec129-cisco-interop

import-prefixes

Syntax [**no**] **import-prefixes** *policy-name*

Context config>router>ldp>peer-parameters>peer

Description This command configures the import FEC prefix policy to determine which prefixes received from other LDP and T-LDP peers are re-distributed to this LDP peer via the LDP session to this peer. A FEC prefix that is filtered out (deny) will not be imported. A FEC prefix that is filtered in (accept) will be imported.

If no import policy is specified, the node will re-distribute to the LDP peer all prefixes it learned from all configured LDP and targeted LDP peers. This policy is applied in addition to the global LDP policy.

Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified.

The **no** form of the command removes the policy from the configuration.

Default no import-prefixes - no import route policy is specified

Parameters *policy-name* — The import-prefix route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains spaces, use double quotes to delimit the start and end of the string. The specified name(s) must already be defined

ttl-security

Syntax **ttl-security** *min-ttl-value*
no ttl-security

Context config>router>ldp>peer-parameters>peer

Description This command configures TTL security parameters for incoming packets. When the feature is enabled, BGP/LDP will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer.

The **no** form of the command disables TTL security.

Default **no ttl-security**

Parameters *min-ttl-value* — Specify the minimum TTL value for an incoming packet.

Values 1 — 255

prefer-tunnel-in-tunnel

Syntax [**no**] **prefer-tunnel-in-tunnel**

Context config>router>ldp

Description This command specifies to use tunnel-in-tunnel over a simple LDP tunnel. Specifically, the user packets for LDP FECs learned over this targeted LDP session can be sent inside an RSVP LSP which terminates on the same egress router as the destination of the targeted LDP session. The user can specify an explicit list of RSVP LSP tunnels under the Targeted LDP session or LDP will perform a lookup in the Tunnel Table Manager (TTM) for the best RSVP LSP. In the former case, only the specified LSPs will be considered to tunnel LDP user packets. In the latter case, all LSPs available to the TTM and which terminate on the same egress 7750 SR router as this target ed LDP session will be considered. In both cases, the metric specified under the LSP configuration is used to control this selection.

Note that the lookup in the TTM will prefer a LDP tunnel over an LDP-over-RSVP tunnel if both are available. Also note that the tunneling operates on the dataplane only. Control packets of this targeted LDP session are sent over the IGP path.

shortcut-transit-ttl-propagate

Syntax [**no**] **shortcut-transit-ttl-propagate**

Context config>router>ldp
config>router>mpls

Description This command configures the TTL handling of transit packets for all LSP shortcuts originating on this ingress LER. It applies to all LDP or RSVP LSPs that are used to resolve static routes, BGP routes, and IGP routes.

The user can enable or disable the propagation of the TTL from the header of an IP packet into the header of the resulting MPLS packet independently for local and transit packets forwarded over an LSP shortcut.

By default, the feature propagates the TTL from the header of transit IP packets into the label stack of the resulting MPLS packets forwarded over the LSP shortcut. This is referred to as Uniform mode.

When the **no** form of the command is enabled, TTL propagation is disabled on all transit IP packets received on any IES interface and destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack. This is referred to as Pipe mode.

Default shortcut-transit-ttl-propagate

shortcut-local-ttl-propagate

Syntax **[no] shortcut-local-ttl-propagate**

Context config>router>ldp
config>router>mpls

Description This command configures the TTL handling of locally generated packets for all LSP shortcuts originating on this ingress LER. It applies to all LDP or RSVP LSPs that are used to resolve static routes, BGP routes, and IGP routes.

The user can enable or disable the propagation of the TTL from the header of an IP packet into the header of the resulting MPLS packet independently for local and transit packets forwarded over an LSP shortcut.

Local IP packets include ICMP Ping, traceroute, and OAM packets, that are destined to a route that is resolved to the LSP shortcut. Transit IP packets are all IP packets received on any IES interface and destined to a route that is resolved to the LSP shortcut

By default, the feature propagates the TTL from the header of locally generated IP packets into the label stack of the resulting MPLS packets forwarded over the LSP shortcut. This is referred to as Uniform mode.

When the **no** form of the above command is enabled, TTL propagation is disabled on all locally generated IP packets, including ICMP Ping, traceroute, and OAM packets, that are destined to a route that is resolved to the LSP shortcut. In this case, a TTL of 255 is programmed onto the pushed label stack. This is referred to as Pipe mode.

Default shortcut-local-ttl-propagate

Targeted Session Commands

targeted-session

Syntax **targeted-session**

Context config>router>ldp

Description This command configures targeted LDP sessions. Targeted sessions are LDP sessions between non-directly connected peers. Hello messages are sent directly to the peer platform instead of to all the routers on this subnet multicast address.

The discovery messages for an indirect LDP session are addressed to the specified peer and not to the multicast address.

Default **none**

bfd-enable

Syntax [**no**] **bfd-enable**

Context config>router>ldp>targ-session>peer

Description This command enables the bidirectional forwarding detection (BFD) session for the selected TLDP session. By enabling BFD for a selected targeted session, the state of that session is tied to the state of the underneath BFD session between the two nodes.

The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes the TLDP session operational state binding to the central BFD session one.

Default no bfd-enable

disable-targeted-session

Syntax [**no**] **disable-targeted-session**

Context config>router>ldp>targ-session

Description This command disables support for SDP triggered automatic generated targeted sessions. Targeted sessions are LDP sessions between non-directly connected peers. The discovery messages for an indirect LDP session are addressed to the specified peer and not to the multicast address.

The **no** form of the command enables the set up of any targeted sessions.

Default **no disable-targeted-session**

peer

Syntax [**no**] **peer** *ip-address*

Context config>router>ldp>targeted-session

Description This command configures parameters for an LDP peer.

Default **none**

Parameters *ip-address* — The IP address of the LDP peer in dotted decimal notation.

export-prefixes

Syntax **export-prefixes** *policy-name* [*policy-name*...(up to 5 max)]
no export-prefixes

Context config>router>ldp>targeted-session

Description This command configures an export route policy used to determine which routes are exported to this targeted LDP session.

Parameters *policy-name* — The export policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

import-prefixes

Syntax **import-prefixes** *policy-name* [*policy-name*...(up to 5 max)]
no import-prefixes

Context config>router>ldp>targeted-session

Description This command configures an import route policy used to determine which routes are imported to this targeted LDP session.

Parameters *policy-name* — The import policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Show LDP Commands

auth-keychain

Syntax **auth-keychain** [*keychain*]

Context show>router>ldp

Description This command displays LDP sessions using a particular authentication key-chain.

Parameters *keychain* — Specifies an existing keychain name.

Sample Output

```
*A:ALA-48>config>router>ldp# show router ldp auth-keychain
===============================================================================
LDP Peers
===============================================================================
Peer             TTL Security Min-TTL-Value Authentication Auth key chain
-------------------------------------------------------------------------------
10.20.1.3        Disabled     n/a           Disabled       eta_keychain1
-------------------------------------------------------------------------------
No. of Peers: 1
===============================================================================
*A:ALA-48>config>router>ldp#
```

bindings

Syntax **bindings** [**fec-type** *fec-type* [**detail | summary**]] [**session** *ip-addr*[:*label-space*]]
bindings [*label-type*] [*start-label* [*end-label*]
bindings {**prefix** *ip-prefix/mask* [**detail**]} [**session** *ip-addr*[:*label-space*]]
bindings active [**prefix** *ip-prefix/mask*] [**summary | egress-nh** *ip-prefix/mask* **| egress-if** *port-id* **| egress-lsp** *tunnel-id*]
bindings service-id *service-id* [**detail**]
bindings vc-type *vc-type* [{**vc-id** *vc-id* **| agi** *agi*} [**session** *ip-addr*[:*lab el-space*]]]

Context show>router>ldp

Description This command displays the contents of the label information base.

Parameters **fec-type** *fec-type* **—** Specify the kind of FEC that the label mapping, withdraw, release and request messages are referring to.

detail — Displays detailed information.

summary — Displays information in a summarized format.

session *ip-addr* **—** displays configuration information about LDP sessions.

ip-prefix — Specify information for the specified IP prefix and mask length. Host bits must be 0.

mask — Specifies the 32-bit address mask used to indicate the bits of an IP address that are being used for the subnet address.

Values 0 — 32

label-space — Specifies the label space identifier that the router is advertising on the interface.

Values 0 — 65535

start-label — Specifies a label value to begin the display.

Values 16 — 1048575

end-label — Specifies a label value to end the display.

Values 17 — 1048575

vc-type — Specifies the VC type to display.

Values **ethernet** , **vlan** , **mirror**

vc-id — Specifies the VC ID to display.

Values 1 — 4294967295

service-id — Specifies the service ID number to display.

Values 1 — 2147483647

egress-lsp *tunnel-id* —

Values 0 — 4294967295

egress-if *port-id* — Specifies the egress interface port ID.

Values slot[/mda[/port]] or slot/mda/port[.channel]

aps-id	aps-group-id[.channel]
aps	keyword
group-id	1— 64
ccag-id	slot/mda/path-id[cc-type]
path-id	a, b
cc-type	.sap-net, .net-sap

Output **LDP Bindings Output —** The following table describes the LDP bindings fields.

Label	Description	
`Legend`	U: Label In Use N: Label Not In Use W: Label Withdrawn S: Status Signaled Up D: Status Signaled Down E: Epipe service V: VPLS service	M: Mirror service A: Apipe service F: Fpipe service I: IES service R: VPRN service P: Ipipe service
`Type`	The service type exchanging labels in the SDP. The possible types displayed are VPLS, Epipe, Spoke, and Unknown.	
`VCId`	The value used by each end of an SDP tunnel to identify the VC.	

Label	Description
SvcID	The unique service identification number identifying the service in the service domain.
SDPId	The SDP number identifying the SDP in the service domain.
Peer	The IP address of the peer.
EgrIntf/LspId	Displays the LSP Tunnel ID (not the LSP path ID).
IngLbl	The ingress LDP label.
	U — Label in use.
	R — Label released.
EgrLbl	The egress LDP label.
LMTU	The local MTU value.
RMTU	The remote MTU value.
No. of Service Bindings	The total number of LDP bindings on the router.

Sample Output

```
*A:SRU4>config>router>ldp# show router ldp bindings detail
===============================================================================
LDP LSR ID: 110.20.1.4
===============================================================================
Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn
        S - Status Signaled Up,  D - Status Signaled Down
        E - Epipe Service, V - VPLS Service, M - Mirror Service
        A - Apipe Service, F - Fpipe Service, I - IES Service, R - VPRN service
        P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service
        TLV - (Type, Length: Value)
===============================================================================
LDP Prefix Bindings
===============================================================================
-------------------------------------------------------------------------------
Prefix             : 1.1.1.0/24
-------------------------------------------------------------------------------
Ing Lbl            :   --                   Peer              : 10.20.1.22
Egr Lbl            : 1301
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None                   Ing. Flags        : None
-------------------------------------------------------------------------------
Prefix             : 1.1.1.0/24
-------------------------------------------------------------------------------
Ing Lbl            :   --                   Peer              : 110.20.1.5
Egr Lbl            : 131071
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None                   Ing. Flags        : None
-------------------------------------------------------------------------------
```

```
Prefix              : 1.2.10.0/24
-------------------------------------------------------------------------------
Ing Lbl             :   --                    Peer              : 10.20.1.22
Egr Lbl             : 618
Egr Int/LspId       :   --
EgrNextHop          :   --
Egr. Flags          : None                    Ing. Flags        : None
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Prefix              : 222.0.0.0/10
-------------------------------------------------------------------------------
Ing Lbl             :   --                    Peer              : 110.20.1.5
Egr Lbl             : 128882
Egr Int/LspId       :   --
EgrNextHop          :   --
Egr. Flags          : None                    Ing. Flags        : None
-------------------------------------------------------------------------------
Prefix              : 222.9.69.0/24
-------------------------------------------------------------------------------
Ing Lbl             :   --                    Peer              : 10.20.1.22
Egr Lbl             : 1402
Egr Int/LspId       :   --
EgrNextHop          :   --
Egr. Flags          : None                    Ing. Flags        : None
-------------------------------------------------------------------------------
Prefix              : 222.9.69.0/24
-------------------------------------------------------------------------------
Ing Lbl             :   --                    Peer              : 110.20.1.5
Egr Lbl             : 128778
Egr Int/LspId       :   --
EgrNextHop          :   --
Egr. Flags          : None                    Ing. Flags        : None
===============================================================================
No. of Prefix Bindings: 3165
===============================================================================
LDP Service FEC 128 Bindings
===============================================================================
===============================================================================
No Matching Entries Found
===============================================================================
LDP Service FEC 129 Bindings
===============================================================================
===============================================================================
No Matching Entries Found
===============================================================================
===============================================================================
*A:SRU4>config>router>ldp#


*A:SRU4>config>router>ldp# show router ldp bindings fec-type prefixes
===============================================================================
LDP LSR ID: 110.20.1.4
===============================================================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
    WP - Label Withdraw Pending
===============================================================================
LDP Prefix Bindings
===============================================================================
Prefix              Peer            IngLbl    EgrLbl EgrIntf/    EgrNextHop
                                                     LspId
```

```
-------------------------------------------------------------------------------
1.1.1.0/24         10.20.1.22        --      1301     --          --
1.2.10.0/24        10.20.1.22        --      618      --          --
1.2.11.0/24        10.20.1.22        --      617      --          --
1.2.12.0/24        10.20.1.22        --      619      --          --
1.2.101.0/24       10.20.1.22        --      656      --          --
1.2.111.0/24       10.20.1.22        --      341      --          --
1.2.121.0/24       10.20.1.22        --      346      --          --
1.38.38.0/24       10.20.1.22        --      624      --          --
1.38.39.0/24       10.20.1.22        --      625      --          --
1.38.138.0/24      10.20.1.22        --      368      --          --
1.38.139.0/24      10.20.1.22        --      626      --          --
...
222.0.0.0/10       10.20.1.22        --      298      --          --
222.0.0.0/10       110.20.1.5        --      128741   --          --
222.9.69.0/24      10.20.1.22        --      1402     --          --
222.9.69.0/24      110.20.1.5        --      128778   --          --
-------------------------------------------------------------------------------
No. of Prefix Bindings: 2939
===============================================================================
*A:SRU4>config>router>ldp#

A:both2# show router ldp bindings fec-type services
===============================================================================
LDP LSR ID: 1.1.1.57
===============================================================================
Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn
        S - Status Signaled Up,  D - Status Signaled Down
        E - Epipe Service, V - VPLS Service, M - Mirror Service
        A - Apipe Service, F - Fpipe Service, I - IES Service, R - VPRN service
        P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service
        TLV - (Type, Length: Value)
===============================================================================
LDP Service Bindings
===============================================================================
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
-------------------------------------------------------------------------------
E-Eth  100        1          1      1.1.1.30        131067U 131068S 1500  1500
E-Eth  500        5          1      1.1.1.30        131066W 131066  3960  3960
-------------------------------------------------------------------------------
No. of VC Labels: 2
===============================================================================
A:both2#


*A:SRU4#  show router ldp bindings session 10.8.100.15
===============================================================================
LDP LSR ID: 110.20.1.4
===============================================================================
Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn
        S - Status Signaled Up,  D - Status Signaled Down
        E - Epipe Service, V - VPLS Service, M - Mirror Service
        A - Apipe Service, F - Fpipe Service, I - IES Service, R - VPRN service
        P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service
        TLV - (Type, Length: Value)
===============================================================================
LDP Prefix Bindings
===============================================================================
Prefix             Peer            IngLbl    EgrLbl EgrIntf     EgrNextHop
-------------------------------------------------------------------------------
No Matching Entries Found
```

```
===============================================================================
LDP Service FEC 128 Bindings
===============================================================================
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
-------------------------------------------------------------------------------
No Matching Entries Found

===============================================================================
LDP Service FEC 129 Bindings
===============================================================================
AGI                                 SAII                    TAII
Type              SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
*A:SRU4#


A:ALA-12# show router ldp bindings ingress-label 2048 131071
===============================================================================
LDP LSR ID: 10.20.1.10
===============================================================================
Legend:  U - Label In Use,  R - Label Released
===============================================================================
LDP Prefix Bindings
===============================================================================
Prefix             Peer            IngLbl  EgrLbl EgrIntf       EgrNextHop
-------------------------------------------------------------------------------
10.20.1.10/32      10.20.1.3       131069U   --     --             --
-------------------------------------------------------------------------------
No. of Prefix Bindings: 1
===============================================================================
LDP Service Bindings
===============================================================================
Type   VCId       SvcId      SDPId  Peer            IngLbl  EgrLbl  LMTU  RMTU
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
A:ALA-12#

*A:SRU4>config>router>ldp#  show router ldp bindings active
===============================================================================
Legend:  (S) - Static
===============================================================================
LDP Prefix Bindings (Active)
===============================================================================
Prefix                 Op   IngLbl    EgrLbl    EgrIntf/LspId  EgrNextHop
-------------------------------------------------------------------------------
10.20.1.20/32          Push   --      0         3/2/1          10.100.30.20
10.20.1.20/32          Swap 131041    0         3/2/1          10.100.30.20
10.20.1.22/32          Push   --      0         3/2/7          160.60.60.2
10.20.1.22/32          Swap 131039    0         3/2/7          160.60.60.2
10.161.201.0/24        Push   --      0         3/2/7          160.60.60.2
10.161.201.0/24        Swap 131038    0         3/2/7          160.60.60.2
110.20.1.1/32          Push   --      441790    3/2/1          10.100.30.20
110.20.1.1/32          Swap 131045    441790    3/2/1          10.100.30.20
110.20.1.4/32          Pop  3           --        --             --
160.60.70.0/24         Push   --      0         3/2/7          160.60.60.2
160.60.70.0/24         Swap 131036    0         3/2/7          160.60.60.2
160.60.80.0/24         Push   --      0         3/2/7          160.60.60.2
```

```
160.60.80.0/24         Swap 129982    0         3/2/7          160.60.60.2
-------------------------------------------------------------------------------
No. of Prefix Bindings: 13
*A:SRU4>config>router>ldp#

A:Dut-B# show router ldp bindings  prefix 10.20.1.3/32 detail
===============================================================================
LDP LSR ID: 10.20.1.2
===============================================================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
    WP - Label Withdraw Pending
===============================================================================
LDP Prefix Binding
===============================================================================
-------------------------------------------------------------------------------
Prefix             : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl            : 130996U                Peer             : 1.1.2.2
Egr Lbl            : 131017
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None                   Ing. Flags       : None
-------------------------------------------------------------------------------
Prefix             : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl            :   --                   Peer             : 3.3.2.2
Egr Lbl            : 3
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None                   Ing. Flags       : None
-------------------------------------------------------------------------------
Prefix             : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl            : 130996U                Peer             : 4.4.2.2
Egr Lbl            : 130969
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None                   Ing. Flags       : None
-------------------------------------------------------------------------------
Prefix             : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl            : 130996U                Peer             : 5.5.2.2
Egr Lbl            : 131005
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None                   Ing. Flags       : None
-------------------------------------------------------------------------------
Prefix             : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl            : 130996U                Peer             : 6.6.2.2
Egr Lbl            : 130993
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None                   Ing. Flags       : None
-------------------------------------------------------------------------------
Prefix             : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl            : 130996U                Peer             : 10.10.1.1
Egr Lbl            : 131017
Egr Int/LspId      :   --
EgrNextHop         :   --
```

```
Egr. Flags          : None                    Ing. Flags         : None
-------------------------------------------------------------------------------
Prefix              : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl             :   --                    Peer               : 10.10.3.3
Egr Lbl             : 3
Egr Int/LspId       :   --
EgrNextHop          :   --
Egr. Flags          : None                    Ing. Flags         : None
-------------------------------------------------------------------------------
Prefix              : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl             : 130996U                 Peer               : 10.10.4.4
Egr Lbl             : 130969
Egr Int/LspId       :   --
EgrNextHop          :   --
Egr. Flags          : None                    Ing. Flags         : None
-------------------------------------------------------------------------------
Prefix              : 10.20.1.3/32
-------------------------------------------------------------------------------
Ing Lbl             :   --                    Peer               : 10.10.12.3
Egr Lbl             : 3
Egr Int/LspId       : lag-1
EgrNextHop          : 10.10.12.3
Egr. Flags          : None                    Ing. Flags         : None
Metric              : 333                     Mtu                : 1500
===============================================================================
No. of Prefix Bindings: 9
===============================================================================
*A:Dut-B#
```

discovery

Syntax **discovery** [{**peer** [*ip-address*]} | {**interface** [*ip-int-name*]}] [**state** *state*] [**detail**] [**adjacency-type** *type*]

Context show>router>ldp

Description This command displays the status of the interfaces participating in LDP discovery.

Parameters **peer** *ip-address* — Specifies to display the IP address of the peer.

interface *ip-int-name* — The name of an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

state *state* — Specifies to display the current operational state of the adjacency.

Values established, trying, down

detail — Specifies to display detailed information.

adjacency-type *type* **—** Specifies to display the adjacency type.

Values link, targeted

Output **LDP Discovery Output —** The following table describes LDP discovery output fields.

Label	Description
Interface Name	The name of the interface.
Local Addr	The IP address of the originating (local) router.
Peer Addr	The IP address of the peer.
Adj Type	The adjacency type between the LDP peer and LDP session is targeted.
State	Established — The adjacency is established.
	Trying — The adjacency is not yet established.
No. of Hello Adjacencies	The total number of hello adjacencies discovered.
Up Time	The amount of time the adjacency has been enabled.
Hold-Time Remaining	The time left before a neighbor is declared to be down.
Hello Mesg Recv	The number of hello messages received for this adjacency.
Hello Mesg Sent	The number of hello messages that have been sent for this adjacency.
Remote Cfg Seq No	The configuration sequence number that was in the hello received when this adjacency started up. This configuration sequence number changes when there is a change of configuration.
Remote IP Address	The IP address used on the remote end for the LDP session.
Local Cfg Seq No	The configuration sequence number that was used in the hello sent when this adjacency started up. This configuration sequence number changes when there is a change of configuration.
Local IP Address	The IP address used locally for the LDP session.

Sample Output

```
*A:SRU4>config>router>ldp# show router ldp discovery
===============================================================================
LDP Hello Adjacencies
===============================================================================
Interface Name                   Local Addr      Peer Addr       AdjType State
-------------------------------------------------------------------------------
N/A                              110.20.1.4      10.8.100.15     Targ    Estab
N/A                              110.20.1.4      10.20.1.20      Targ    Estab
N/A                              110.20.1.4      10.20.1.22      Targ    Estab
N/A                              110.20.1.4      10.100.1.1      Targ    Trying
N/A                              110.20.1.4      110.20.1.1      Targ    Estab
N/A                              110.20.1.4      110.20.1.2      Targ    Trying
N/A                              110.20.1.4      110.20.1.3      Targ    Estab
N/A                              110.20.1.4      110.20.1.5      Targ    Estab
N/A                              110.20.1.4      110.20.1.6      Targ    Trying
N/A                              110.20.1.4      110.20.1.51     Targ    Trying
N/A                              110.20.1.4      110.20.1.52     Targ    Trying
```

```
N/A                               110.20.1.4      110.20.1.53     Targ    Trying
N/A                               110.20.1.4      110.20.1.55     Targ    Trying
N/A                               110.20.1.4      110.20.1.56     Targ    Trying
N/A                               110.20.1.4      110.20.1.110    Targ    Trying
N/A                               110.20.1.4      110.20.1.150    Targ    Trying
N/A                               110.20.1.4      220.220.1.6     Targ    Trying
aps-1                             110.20.1.4      110.20.1.3      Link    Estab
aps-2                             110.20.1.4      110.20.1.3      Link    Estab
aps-3                             110.20.1.4      110.20.1.3      Link    Estab
sr4-1                             110.20.1.4      110.20.1.3      Link    Estab
ess-7-1                           110.20.1.4      110.20.1.5      Link    Estab
ess-7-2                           110.20.1.4      110.20.1.5      Link    Estab
ess-7-3                           110.20.1.4      110.20.1.5      Link    Estab
ess-7-4                           110.20.1.4      110.20.1.5      Link    Estab
ess-7-5                           110.20.1.4      110.20.1.5      Link    Estab
hubA                              110.20.1.4      110.20.1.3      Link    Estab
hubA                              110.20.1.4      110.20.1.5      Link    Estab
hubA                              110.20.1.4      200.0.0.1       Link    Estab
germ-1                            110.20.1.4      110.20.1.110    Link    Estab
src-1.1                           170.70.51.4     224.0.0.2       Link    Trying
src-1.2                           170.70.52.4     224.0.0.2       Link    Trying
src-1.3                           170.70.53.4     224.0.0.2       Link    Trying
src-1.4                           170.70.54.4     224.0.0.2       Link    Trying
src-1.5                           170.70.55.4     224.0.0.2       Link    Trying
src-1.6                           170.70.56.4     224.0.0.2       Link    Trying
src-1.7                           170.70.57.4     224.0.0.2       Link    Trying
src-1.8                           170.70.58.4     224.0.0.2       Link    Trying
src-1.9                           170.70.59.4     224.0.0.2       Link    Trying
src-1.10                          170.70.60.4     224.0.0.2       Link    Trying
srl-1                             110.20.1.4      33.66.32.1      Link    Estab
srl-3                             110.20.1.4      33.66.33.1      Link    Estab
aps-8                             110.20.1.4      33.66.34.1      Link    Estab
aps-9                             110.20.1.4      33.66.35.1      Link    Estab
srr-1                             110.20.1.4      11.22.10.2      Link    Estab
srr-2                             110.20.1.4      11.22.11.2      Link    Estab
srr-3                             110.20.1.4      1.1.1.1         Link    Estab
aps-11                            110.20.1.4      11.22.13.2      Link    Estab
gsr1                              110.20.1.4      10.8.100.15     Link    Estab
gsr2                              110.20.1.4      10.20.1.22      Link    Estab
g7600                             180.50.80.4     224.0.0.2       Link    Trying
m160                              110.20.1.4      10.20.1.20      Link    Estab
-------------------------------------------------------------------------------
No. of Hello Adjacencies: 52
===============================================================================
*A:SRU4>config>router>ldp#


*A:SRU4>config>router>ldp# show router ldp discovery peer 10.8.100.15
===============================================================================
LDP Hello Adjacencies
===============================================================================
Interface Name                    Local Addr      Peer Addr       AdjType State
-------------------------------------------------------------------------------
N/A                               110.20.1.4      10.8.100.15     Targ    Estab
-------------------------------------------------------------------------------
No. of Hello Adjacencies: 1
===============================================================================
*A:SRU4>config>router>ldp#


*A:SRU4>config>router>ldp# show router ldp discovery detail
```

```
===============================================================================
LDP Hello Adjacencies (Detail)
===============================================================================
-------------------------------------------------------------------------------
Peer 10.8.100.15
-------------------------------------------------------------------------------
Local Address      : 110.20.1.4         Peer Address        : 10.8.100.15
Adjacency Type     : Targeted           State               : Established
Up Time            : 0d 12:39:38        Hold Time Remaining : 43
Hello Mesg Recv    : 10403              Hello Mesg Sent     : 3243
Local IP Address   : 110.20.1.4         Remote IP Address   : 10.8.100.15
Local Hello Timeout: 45                 Remote Hello Timeout: 90
Local Cfg Seq No   : 1828354504         Remote Cfg Seq No   : 0
-------------------------------------------------------------------------------
Peer 10.20.1.20
-------------------------------------------------------------------------------
Local Address      : 110.20.1.4         Peer Address        : 10.20.1.20
Adjacency Type     : Targeted           State               : Established
Up Time            : 0d 12:39:57        Hold Time Remaining : 40
Hello Mesg Recv    : 7495               Hello Mesg Sent     : 3244
Local IP Address   : 110.20.1.4         Remote IP Address   : 10.20.1.20
Local Hello Timeout: 45                 Remote Hello Timeout: 45
Local Cfg Seq No   : 572902976          Remote Cfg Seq No   : 1
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Interface "gsr2"
-------------------------------------------------------------------------------
Local Address      : 110.20.1.4         Peer Address        : 10.20.1.22
Adjacency Type     : Link               State               : Established
Up Time            : 0d 12:40:41        Hold Time Remaining : 11
Hello Mesg Recv    : 10414              Hello Mesg Sent     : 11260
Local IP Address   : 160.60.60.4        Remote IP Address   : 160.60.60.2
Local Hello Timeout: 15                 Remote Hello Timeout: 15
Local Cfg Seq No   : 1911286684         Remote Cfg Seq No   : 0
-------------------------------------------------------------------------------
Interface "g7600"
-------------------------------------------------------------------------------
Local Address      : 180.50.80.4        Peer Address        : 224.0.0.2
Adjacency Type     : Link               State               : Trying
-------------------------------------------------------------------------------
Interface "m160"
-------------------------------------------------------------------------------
Local Address      : 110.20.1.4         Peer Address        : 10.20.1.20
Adjacency Type     : Link               State               : Established
Up Time            : 0d 12:40:47        Hold Time Remaining : 14
Hello Mesg Recv    : 10450              Hello Mesg Sent     : 11262
Local IP Address   : 10.100.30.4        Remote IP Address   : 10.100.30.20
Local Hello Timeout: 15                 Remote Hello Timeout: 15
Local Cfg Seq No   : 2523051834         Remote Cfg Seq No   : 1
===============================================================================
*A:SRU4>config>router>ldp#
```

interface

Syntax **interface** [*ip-int-name* **|** *ip-address*] [**detail**]

Context show>router>ldp

Description This command displays configuration information about LDP interfaces.

Parameters *ip-int-name* — The name of an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-address — The IP address of the LDP neighbor.

detail — Displays detailed information.

Output **LDP Interface Output —** The following table describes the LDP interface output fields.

Label	Description
`Interface`	Specifies the interface associated with the LDP instance.
`Adm`	`Up` — The LDP is administratively enabled. `Down` — The LDP is administratively disabled.
`Opr`	`Up` — The LDP is operationally enabled. `Down` — The LDP is operationally disabled.
`Hello Factor`	The value by which the hello timeout should be divided to give the hello time, for example, the time interval, in seconds, between LDP hello messages. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.
`Hold Time`	The hello time, also known as hold time. It is the time interval, in seconds, that LDP waits before declaring a neighbor to be down. Hello timeout is local to the system and is sent in the hello messages to a neighbor.
`KA Factor`	The value by which the keepalive timeout should be divided to give the keepalive time, for example, the time interval, in seconds, between LDP keepalive messages. LDP keepalive messages are sent to keep the LDP session from timing out when no other LDP traffic is being sent between the neighbors.
`KA Timeout`	The time interval, in seconds, that LDP waits before tearing down a session. If no LDP messages are exchanged during this time interval, the LDP session is torn down. Generally the value is configured to be 3 times the keepalive time (the time interval between successive LDP keepalive messages).
`Auth`	`Enabled` — Authentication using MD5 message based digest protocol is enabled. `Disabled` — No authentication is used.
`No. of Interface`	The total number of LDP interfaces.

Sample Output

```
*A:SRU4>config>router>ldp# show router ldp interface "hubA"
===============================================================================
LDP Interfaces
===============================================================================
Interface                        Adm Opr  Hello  Hold  KA     KA      Transport
                                          Factor Time  Factor Timeout Address
-------------------------------------------------------------------------------
hubA                             Up  Up   3      15    3      30      System
-------------------------------------------------------------------------------
No. of Interfaces: 1
===============================================================================
*A:SRU4>config>router>ldp#


*A:SRU4>config>router>ldp# show router ldp interface "hubA" detail
===============================================================================
LDP Interfaces (Detail)
===============================================================================
-------------------------------------------------------------------------------
Interface "hubA"
-------------------------------------------------------------------------------
Admin State        : Up                  Oper State       : Up
Hold Time          : 15                  Hello Factor     : 3
Keepalive Timeout  : 30                  Keepalive Factor : 3
Transport Addr     : System              Last Modified    : 03/03/2010 19:47:34
Active Adjacencies : 3
Tunneling          : Disabled
Lsp Name           : None
Local LSR          : System
BFD Status         : Disabled
===============================================================================
*A:SRU4>config>router>ldp#
```

fec-egress-stats

Syntax **fec-egress-stats** [*ip-prefix/mask*]
fec-egress-stats active

Context show>router>ldp

Description This command displays LDP prefix FECs egress statistics.

Parameters *ip-prefix* — Specify information for the specified IP prefix and mask length. Host bits must be 0.

mask — Specifies the 32-bit address mask used to indicate the bits of an IP address that are being used for the subnet address.

Values 0 — 32

fec-originate

Syntax **fec-originate** [*ip-prefix/mask*] [*operation-type*]

Context show>router>ldp

Description This command displays LDP static prefix FECs.

Parameters *ip-prefix* — Specify information for the specified IP prefix and mask length. Host bits must be 0.

mask — Specifies the 32-bit address mask used to indicate the bits of an IP address that are being used for the subnet address.

Values 0 — 32

operation-type — Specify the operation type to display.

Values pop, swap

Output **FEC Originate Output —** The following table describes the FEC originate parameters output fields.

Label	Description
`Prefix`	Specifies the static prefix FEC.
`NH Type`	Specifies the type of next-hop represented by this row entry. `unknown` — The next-hop type has not been set. `IP Addr` — The next-hop is an IP address. `pop` — There is no next-hop (pop the label and route).
`NextHop`	The IP address of the next-hop.
`IngLabel`	Specifies the label that is advertised to the upstream peer. If this variable is set to the default value of 4294967295, the ingress label will be dynamically assigned by the label manager.
`EgrLabel`	Specifies the egress label associated with this next-hop entry. The LSR will swap the incoming label with the configured egress label. If this egress label has a value of 4294967295, the LSR will pop the incoming label.
`OperIngLabel`	Specifies the actual or operational value of the label that was advertised to the upstream peer.

```
*A:SRU4>config>router>ldp#  show router ldp fec-originate
===============================================================================
LDP Static Prefix FECs
===============================================================================
Prefix              NHType  NextHop         IngLabel    EgrLabel    OperIngLabel
-------------------------------------------------------------------------------
24.1.0.0/16         Pop     n/a               --          --        0
24.1.0.1/32         Pop     n/a               --          --        0
24.1.0.2/32         Pop     n/a               --          --        0
24.1.0.3/32         Pop     n/a               --          --        0
24.1.0.4/32         Pop     n/a               --          --        0
```

```
24.1.0.5/32         Pop     n/a             --          --       0
24.1.0.6/32         Pop     n/a             --          --       0
24.1.0.7/32         Pop     n/a             --          --       0
24.1.0.8/32         Pop     n/a             --          --       0
24.1.0.9/32         Pop     n/a             --          --       0
...
24.251.0.0/16       Pop     n/a             --          --       0
24.252.0.0/16       Pop     n/a             --          --       0
24.253.0.0/16       Pop     n/a             --          --       0
24.254.0.0/16       Pop     n/a             --          --       0
-------------------------------------------------------------------------------
No. of FECs: 508
===============================================================================
*A:SRU4>config>router>ldp#
```

parameters

Syntax **parameters**

Context show>router>ldp

Description This command displays configuration information about LDP parameters.

Output **LDP Parameters Output —** The following table describes the LDP parameters output fields.

Label	Description
`Keepalive Timeout`	The time interval, in seconds, that LDP waits before tearing down a session. If no LDP messages are exchanged during this time interval, the LDP session is torn down. Generally the value is configured to be 3 times the keepalive time (the time interval between successive LDP keepalive messages).
`Timeout Factor`	The value by which the keepalive timeout should be divided to give the keepalive time, for example, the time interval, in seconds, between LDP keepalive messages. LDP keepalive messages are sent to keep the LDP session from timing out when no other LDP traffic is being sent between the neighbors.
`Hold Time`	The hello time, also known as hold time. It is the time interval, in seconds, that LDP waits before declaring a neighbor to be down. Hello timeout is local to the system and is sent in the hello messages to a neighbor.
`Hello Factor`	The value by which the hello timeout should be divided to give the hello time, for example, the time interval, in seconds, between LDP hello messages. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.
`Auth`	`Enabled` — Authentication using MD5 message based digest protocol is enabled. `Disabled` — No authentication is used.

Label	Description (Continued)
Admin Status	inService — The LDP is administratively enabled. outService — The LDP is administratively disabled.
Deaggregated FECs	False — LDP aggregates multiple prefixes into a single Forwarding Equivalence Class (FEC) and advertises a single label for the FEC. This value is only applicable to LDP interfaces and not for targeted sessions. True — LDP de-aggregates prefixes into multiple FECs.
Propagate Policy	The Propagate Policy value specifies whether the LSR should generate FECs and which FECs it should generate. system — LDP will distribute label bindings only for the router's system IP address. interface — LDP will distribute label bindings for all LDP interfaces. all — LDP will distribute label bindings for all prefixes in the routing table. none — LDP will not distribute any label bindings.
Transport Address	interface — The interface's IP address is used to set up the LDP session between neighbors. If multiple interfaces exist between two neighbors, the 'interface' mode cannot be used since only one LDP session is actually set up between the two neighbors. system — The system's IP address is used to set up the LDP session between neighbors.
Label-Retention	liberal — All advertised label mappings are retained whether they are from a valid next hop or not. When the label distribution value is downstream unsolicited, a router may receive label bindings for the same destination for all its neighbors. Labels for the non-next hops for the FECs are retained in the software but not used. When a network topology change occurs where a non-nexthop becomes a true next hop, the label received earlier is then used. conservative — Advertised label mappings are retained only if they will be used to forward packets; for example if the label came from a valid next hop. Label bindings received from non-next hops for each FEC are discarded.
Control Mode	ordered — Label bindings are not distributed in response to a label request until a label binding has been received from the next hop for the destination. independent — Label bindings are distributed immediately in response to a label request even if a label binding has not yet been received from the next hop for the destination.

Label	Description (Continued)
Route Preference	The route preference assigned to LDP routes. When multiple routes are available to a destination, the route with the lowest preference will be used. This value is only applicable to LDP interfaces and not for targeted sessions.
Loop Detection	`enabled` — Loop detection is enabled. `disabled` — Loop detection is disabled. `none` — Loop detection is not supported on this router. `other` — Loop detection is supported but by a method other than `hopCount`, `pathVector`, or `hopCountAndPathVector`. `hopCount` — Loop detection is supported by hop count only. `pathVector` — Loop detection is supported by path vector only. `hopCountAndPathVector` — Loop detection is supported by both path vector and hop count.
Keepalive Timeout	The factor used to derive the Keepalive interval.
Keepalive Factor	The time interval, in seconds, that LDP waits before tearing down the session.
Hold-Time	The time left before a neighbor is declared to be down.
Hello Factor	The value by which the hello timeout should be divided to give the hello time, for example, the time interval, in seconds, between LDP hello messages. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.
Auth	`Enabled` — Authentication using MD5 message based digest protocol is enabled. `Disabled` — No authentication is used.
Passive-Mode	`true` — LDP responds only when it gets a connect request from a peer and will not attempt to actively connect to its neighbors. `false` — LDP actively tries to connect to its peers.
Targeted-Sessions	`true` — Targeted sessions are enabled. `false` — Targeted sessions are disabled.

Sample Output

```
*A:SRU4>config>router>ldp#  show router ldp parameters
===============================================================================
LDP Parameters (LSR ID 110.20.1.4)
===============================================================================
-------------------------------------------------------------------------------
Graceful Restart Parameters
-------------------------------------------------------------------------------
```

```
Nbor Liveness Time : 5 sec                Max Recovery Time : 30
-------------------------------------------------------------------------------
Interface Parameters
-------------------------------------------------------------------------------
Keepalive Timeout  : 30 sec               Keepalive Factor  : 3
Hold Time          : 15 sec               Hello Factor      : 3
Propagate Policy   : system               Transport Address : system
Deaggregate FECs   : False                Route Preference  : 9
Label Distribution : downstreamUnsolicited Label Retention   : liberal
Control Mode       : ordered              Loop Detection    : none
-------------------------------------------------------------------------------
Targeted Session Parameters
-------------------------------------------------------------------------------
Keepalive Timeout  : 40 sec               Keepalive Factor  : 4
Hold Time          : 45 sec               Hello Factor      : 3
Passive Mode       : False                Targeted Sessions : Enabled
===============================================================================
*A:SRU4>config>router>ldp#
```

peer

Syntax **peer** [*ip-address*] [**detail**]

Context show>router>ldp

Description This command displays configuration information about LDP peers.

Parameters *ip-address* — The IP address of the LDP peer.

detail — Displays detailed information.

Output **LDP Peer Output —** The following table describes LDP peer output.

Label	Description
Peer	The IP address of the peer.
Adm	Up — The LDP is administratively enabled. Down — The LDP is administratively disabled.
Opr	Up — The LDP is operationally enabled. Down — The LDP is operationally disabled.
Hello Factor	The value by which the hello timeout should be divided to give the hello time, for example, the time interval, in seconds, between LDP hello messages. LDP uses hello messages to discover neighbors and to detect loss of connectivity with its neighbors.
Hold Time	The hello time or hold time. The time interval, in seconds, that LDP waits before declaring a neighbor to be down. Hello timeout is local to the system and is sent in the hello messages to a neighbor.

Label	Description (Continued)
KA Factor	The value by which the keepalive timeout should be divided to give the keepalive time, for example, the time interval, in seconds, between LDP keepalive messages. LDP keepalive messages are sent to keep the LDP session from timing out when no other LDP traffic is being sent between the neighbors.
KA Timeout	The time interval, in seconds, that LDP waits before tearing down a session. If no LDP messages are exchanged during this time interval, the LDP session is torn down. Generally the value is configured to be 3 times the keepalive time (the time interval between successive LDP keepalive messages).
Auth	Enabled — Authentication using MD5 message based digest protocol is enabled. Disabled — No authentication is used.
Passive Mode	The mode used to set up LDP sessions. This value is only applicable to targeted sessions and not to LDP interfaces. True — LDP responds only when it gets a connect request from a peer and will not attempt to actively connect to its neighbors. False — LDP actively tries to connect to its peers.
Auto Create	Specifies if a targeted peer was automatically created through service manager. For an LDP interface, this value is always false.
No. of Peers	The total number of LDP peers.
Tunneling	Enabled — Tunneling is enabled. Disabled — No tunneling is used.
LSP	The LSP name.

Sample Output

```
*A:SRU4>config>router>ldp#  show router ldp peer
===============================================================================
LDP Peers
===============================================================================
Peer              Adm  Opr  Hello   Hold    KA      KA       Passive   Auto
                            Factor  Time    Factor  Timeout  Mode      Created
-------------------------------------------------------------------------------
10.8.100.15       Up   Up   3       45      4       40       Disabled  No
10.20.1.20        Up   Up   3       45      4       40       Disabled  No
10.20.1.22        Up   Up   3       45      4       40       Disabled  No
10.100.1.1        Up   Up   3       45      4       40       Disabled  No
110.20.1.1        Up   Up   3       45      4       40       Disabled  No
110.20.1.2        Up   Up   3       45      4       40       Disabled  No
110.20.1.3        Up   Up   3       45      4       40       Disabled  No
110.20.1.5        Up   Up   3       45      4       40       Disabled  No
110.20.1.6        Up   Up   3       45      4       40       Disabled  No
```

```
110.20.1.51       Up   Up   3       45      4       40       Disabled  No
110.20.1.52       Up   Up   3       45      4       40       Disabled  No
110.20.1.53       Up   Up   3       45      4       40       Disabled  No
110.20.1.55       Up   Up   3       45      4       40       Disabled  No
110.20.1.56       Up   Up   3       45      4       40       Disabled  No
110.20.1.110      Up   Up   3       45      4       40       Disabled  No
110.20.1.150      Up   Up   3       45      4       40       Disabled  No
220.220.1.6       Up   Up   3       45      4       40       Disabled  No
-------------------------------------------------------------------------------
No. of Peers: 17
===============================================================================
*A:SRU4>config>router>ldp#


*A:SRU4>config>router>ldp#  show router ldp peer detail
===============================================================================
LDP Peers (Detail)
===============================================================================
-------------------------------------------------------------------------------
Peer 10.8.100.15
-------------------------------------------------------------------------------
Admin State        : Up                Oper State           : Up
Hold Time          : 45                Hello Factor         : 3
Keepalive Timeout  : 40                Keepalive Factor     : 4
Passive Mode       : Disabled          Last Modified        : 03/03/2010 19:47:34
Active Adjacencies : 1                 Auto Created         : No
Tunneling          : Disabled
Lsp Name           : None
Local LSR          : None
BFD Status         : Disabled
-------------------------------------------------------------------------------
Peer 10.20.1.20
-------------------------------------------------------------------------------
Admin State        : Up                Oper State           : Up
Hold Time          : 45                Hello Factor         : 3
Keepalive Timeout  : 40                Keepalive Factor     : 4
Passive Mode       : Disabled          Last Modified        : 03/03/2010 19:47:34
Active Adjacencies : 1                 Auto Created         : No
Tunneling          : Disabled
Lsp Name           : None
Local LSR          : None
BFD Status         : Disabled
...
-------------------------------------------------------------------------------
Peer 220.220.1.6
-------------------------------------------------------------------------------
Admin State        : Up                Oper State           : Up
Hold Time          : 45                Hello Factor         : 3
Keepalive Timeout  : 40                Keepalive Factor     : 4
Passive Mode       : Disabled          Last Modified        : 03/03/2010 19:47:34
Active Adjacencies : 0                 Auto Created         : No
Tunneling          : Disabled
Lsp Name           : None
Local LSR          : None
BFD Status         : Disabled

===============================================================================
*A:SRU4>config>router>ldp#

*A:SRU4>config>router>ldp#    show router ldp peer 10.8.100.15 detail
===============================================================================
```

```
LDP Peers (Detail)
===============================================================================
-------------------------------------------------------------------------------
Peer 10.8.100.15
-------------------------------------------------------------------------------
Admin State         : Up              Oper State          : Up
Hold Time           : 45              Hello Factor        : 3
Keepalive Timeout   : 40              Keepalive Factor    : 4
Passive Mode        : Disabled        Last Modified       : 03/03/2010 19:47:34
Active Adjacencies  : 1               Auto Created        : No
Tunneling           : Disabled
Lsp Name            : None
Local LSR           : None
BFD Status          : Disabled
===============================================================================
*A:SRU4>config>router>ldp#
```

peer-parameters

Syntax **peer-parameters** *peer-ip-address*

Context show>router>ldp

Description This command displays LDP peer information.

Parameters *peer-ip-address* — Specify the peer IP address.

LDP peer-parameters output — The following table describes LDP peer-parameters output.

Label	Description
Peer	The IP address of the peer.
TTL security	Enabled — LDP peering sessions protected.
	Disabled — LDP peering sessions unprotected.
Min-TTL-Value	Displays the minimum TTL value for an incoming packet.
Auth	Enabled — Authentication using MD5 message based digest protocol is enabled.
	Disabled — No authentication is used.

Sample Output

```
*A:SRU4>config>router>ldp# show router ldp peer-parameters
===============================================================================
LDP Peers
===============================================================================
-------------------------------------------------------------------------------
Peer : 10.8.100.15
-------------------------------------------------------------------------------
```

```
TTL Security       : Disabled          Min-TTL            : n/a
Authentication Key : Disabled          DOD                : Disabled
Auth key chain     : n/a
FEC129 Cisco Inter*: Disabled
Import Policies    : None              Export Policies    : None
-------------------------------------------------------------------------------
Peer : 10.20.1.20
-------------------------------------------------------------------------------
TTL Security       : Disabled          Min-TTL            : n/a
Authentication Key : Disabled          DOD                : Disabled
Auth key chain     : n/a
FEC129 Cisco Inter*: Disabled
Import Policies    : None              Export Policies    : None
-------------------------------------------------------------------------------
...
-------------------------------------------------------------------------------
Peer : 220.220.1.6
-------------------------------------------------------------------------------
TTL Security       : Enabled           Min-TTL            : 255
Authentication Key : Enabled           DOD                : Disabled
Auth key chain     : n/a
FEC129 Cisco Inter*: Disabled
Import Policies    : None              Export Policies    : None
-------------------------------------------------------------------------------
No. of Peers: 17
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>config>router>ldp#
```

session

Syntax **session** [*ip-addr*[:*label-space*]] [**detail | statistics** [*packet-type*]] [*session-type*]

Context show>router>ldp

Description This command displays configuration information about LDP sessions.

Parameters *ip-address* — Specify the IP address of the LDP peer.

label-space — Specifies the label space identifier that the router is advertising on the interface.

Values 0 — 65535

detail — Displays detailed information.

statistics *packet-type* **—** Specify the packet type.

Values hello, keepalive, init, label, notification, address

session-type — Specifies to display the session type.

Values link, targeted, both

Output **LDP Session Output —** The following table describes LDP session output fields.

Label	Description
Peer LDP ID	The IP address of the LDP peer.
Adj Type	The adjacency type between the LDP peer and LDP session is targeted.
	Link — Specifies that this adjacency is a result of a link hello.
	Targeted — Specifies that this adjacency is a result of a targeted hello.
State	Established — The adjacency is established.
	Trying — The adjacency is not yet established.
Mesg Sent	The number of messages sent.
Mesg Rcvd	The number of messages received.
Up Time	The amount of time the adjacency has been enabled.

Sample Output

```
*A:SRU4>config>router>ldp#   show router ldp session
===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id         Adj Type   State         Msg Sent  Msg Recv  Up Time
-------------------------------------------------------------------------------
1.1.1.1:0           Link       Nonexistent   2         1         0d 00:00:04
10.8.100.15:0       Both       Nonexistent   14653     21054     0d 12:48:25
10.20.1.20:0        Both       Established   105187    84837     0d 12:48:27
```

```
10.20.1.22:0       Both       Established   144586    95148     0d 12:48:23
11.22.10.2:0       Link       Nonexistent   4         2         0d 00:00:16
11.22.11.2:0       Link       Nonexistent   4         4         0d 00:00:14
11.22.13.2:0       Link       Nonexistent   5         6         0d 00:00:20
33.66.33.1:0       Link       Nonexistent   6         7         0d 00:00:25
33.66.34.1:0       Link       Nonexistent   2         2         0d 00:00:05
33.66.35.1:0       Link       Nonexistent   4         4         0d 00:00:14
110.20.1.1:0       Targeted   Nonexistent   0         1         0d 00:00:04
110.20.1.3:0       Both       Established   94        97        0d 00:00:55
110.20.1.5:0       Both       Established   230866    286216    0d 12:48:27
110.20.1.110:0     Link       Nonexistent   2         2         0d 00:00:05
200.0.0.1:0        Link       Nonexistent   2         2         0d 00:00:05
-------------------------------------------------------------------------------
No. of Sessions: 15
===============================================================================
*A:SRU4>config>router>ldp#


*A:SRU4>config>router>ldp# show router ldp session 10.20.1.20:0
===============================================================================
LDP Sessions
===============================================================================
Peer LDP Id        Adj Type   State         Msg Sent  Msg Recv  Up Time
-------------------------------------------------------------------------------
10.20.1.20:0       Both       Established   105204    84859     0d 12:49:05
-------------------------------------------------------------------------------
No. of Sessions: 1
===============================================================================
*A:SRU4>config>router>ldp#


*A:SRU4>config>router>ldp# show router ldp session detail
================================================================================
LDP Sessions (Detail)
================================================================================

Legend:  DoD - Downstream on Demand (for address FEC's only)
         DU  - Downstream Unsolicited
================================================================================
--------------------------------------------------------------------------------
Session with Peer 1.1.1.1:0
--------------------------------------------------------------------------------
Adjacency Type    : Link           State                 : Nonexistent
Up Time           : 0d 00:00:22
Max PDU Length    : 4096           KA/Hold Time Remaining: 0
Link Adjacencies  : 1              Targeted Adjacencies  : 0
Local Address     : 110.20.1.4     Peer Address          : 1.1.1.1
Local TCP Port    : 0              Peer TCP Port         : 0
Local KA Timeout  : 30             Peer KA Timeout       : 30
Mesg Sent         : 5              Mesg Recv             : 2
FECs Sent         : 0              FECs Recv             : 0
GR State          : Capable        Label Distribution    : DU
Nbr Liveness Time : 0              Max Recovery Time     : 0
Number of Restart : 0              Last Restart Time     : Never
Advertise         : Address
--------------------------------------------------------------------------------
Session with Peer 10.8.100.15:0
--------------------------------------------------------------------------------
Adjacency Type    : Both           State                 : Nonexistent
Up Time           : 0d 12:49:26
Max PDU Length    : 4096           KA/Hold Time Remaining: 0
```

```
Link Adjacencies  : 1              Targeted Adjacencies  : 1
Local Address     : 110.20.1.4     Peer Address          : 10.8.100.15
Local TCP Port    : 0              Peer TCP Port         : 0
Local KA Timeout  : 30             Peer KA Timeout       : 30
Mesg Sent         : 14672          Mesg Recv             : 21081
FECs Sent         : 0              FECs Recv             : 0
GR State          : Capable        Label Distribution    : DU
Nbr Liveness Time : 0              Max Recovery Time     : 0
A:cpm-a#
...
-------------------------------------------------------------------------------
Session with Peer 200.0.0.1:0
-------------------------------------------------------------------------------
Adjacency Type    : Link           State                 : Nonexistent
Up Time           : 0d 00:00:02
Max PDU Length    : 4096           KA/Hold Time Remaining: 28
Link Adjacencies  : 1              Targeted Adjacencies  : 0
Local Address     : 110.20.1.4     Peer Address          : 200.0.0.1
Local TCP Port    : 0              Peer TCP Port         : 0
Local KA Timeout  : 30             Peer KA Timeout       : 30
Mesg Sent         : 1              Mesg Recv             : 1
FECs Sent         : 0              FECs Recv             : 0
GR State          : Capable        Label Distribution    : DU
Nbr Liveness Time : 0              Max Recovery Time     : 0
Number of Restart : 0              Last Restart Time     : Never
Advertise         : Address
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>config>router>ldp#
```

status

Syntax **status**

Context show>router>ldp

Description This command displays LDP status information.

Output **LDP Status Output —** The following table describes LDP status output fields.

Label	Description
Admin State	Up — The LDP is administratively enabled. Down — The LDP is administratively disabled.
Oper State	Up — The LDP is operationally enabled. Down — The LDP is operationally disabled.
Created at	The date and time when the LDP instance was created.
Up Time	The time, in hundreths of seconds, that the LDP instance has been operationally up.
Last Change	The date and time when the LDP instance was last modified.
Oper Down Events	The number of times the LDP instance has gone operationally down since the instance was created.
Active Adjacencies	The number of active adjacencies (i.e., established sessions) associated with the LDP instance.
Active Sessions	The number of active sessions (i.e., session in some form of creation) associated with the LDP instance.
Active Interfaces	The number of active (i.e., operationally up) interfaces associated with the LDP instance.
Inactive Interfaces	The number of inactive (i.e., operationally down) interfaces associated with the LDP instance.
Active Peers	The number of active LDP peers.
Inactive Peers	The number of inactive LDP peers.
Addr FECs Sent	The number of labels that have been sent to the peer associated with this FEC.
Addr FECs Recv	The number of labels that have been received from the peer associated with this FEC.
Serv FECs Sent	The number of labels that have been sent to the peer associated with this FEC.
Serv FECs Recv	The number of labels that have been received from the peer associated with this FEC.

Label	Description (Continued)
Attempted Sessions	The total number of attempted sessions for this LDP instance.
No Hello Err	The total number of “Session Rejected” or “No Hello Error” notification messages sent or received by this LDP instance.
Param Adv Err	The total number of “Session Rejected” or “Parameters Advertisement Mode Error” notification messages sent or received by this LDP instance.
Max PDU Err	The total number of “Session Rejected” or “Parameters Max PDU Length Error” notification messages sent or received by this LDP instance.
Label Range Err	The total number of “Session Rejected” or “Parameters Label Range Error” notification messages sent or received by this LDP instance.
Bad LDP Id Err	The number of bad LDP identifier fatal errors detected for sessions associated with this LDP instance.
Bad PDU Len Err	The number of bad PDU length fatal errors detected for sessions associated with this LDP instance.
Bad Mesg Len Err	The number of bad message length fatal errors detected for sessions associated with this LDP instance.
Bad TLV Len Err	The number of bad TLV length fatal errors detected for sessions associated with this LDP instance.
Malformed TLV Err	The number of malformed TLV value fatal errors detected for sessions associated with this LDP instance.
Shutdown Notif Sent	The number of shutdown notifications sent related to sessions associated with this LDP instance.
Keepalive Expired Err	The number of session Keepalive timer expired errors detected for sessions associated with this LDP instance.
Shutdown Notif Recv	The number of shutdown notifications received related to sessions associated with this LDP instance.

Sample Output

```
*A:SRU4>config>router>ldp#    show router ldp status
===============================================================================
LDP Status for LSR ID 110.20.1.4
===============================================================================
Admin State         : Up                     Oper State           : Up
Created at          : 03/03/2010 19:46:09  Up Time              : 0d 12:52:07
Oper Down Reason    : n/a                    Oper Down Events     : 1
Last Change         : 03/03/2010 19:46:09  Tunn Down Damp Time  : 20 sec
Label Withdraw Del*: 0 sec                   Implicit Null Label  : Enabled
Short. TTL Prop Lo*: Enabled                 Short. TTL Prop Tran*: Enabled
Import Policies     : None                   Export Policies      : None
```

```
Aggregate Prefix   : False
Agg Prefix Policies: None
Active Adjacencies : 30                   Active Sessions      : 4
Active Interfaces  : 33                   Inactive Interfaces  : 0
Active Peers       : 17                   Inactive Peers       : 0
Addr FECs Sent     : 666                  Addr FECs Recv       : 2994
Serv FECs Sent     : 0                    Serv FECs Recv       : 0
Attempted Sessions : 34431
No Hello Err       : 0                    Param Adv Err        : 0
Max PDU Err        : 0                    Label Range Err      : 0
Bad LDP Id Err     : 6534                 Bad PDU Len Err      : 0
Bad Mesg Len Err   : 0                    Bad TLV Len Err      : 0
Unknown TLV Err    : 0
Malformed TLV Err  : 0                    Keepalive Expired Err: 2748
Shutdown Notif Sent: 0                    Shutdown Notif Recv  : 194
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:SRU4>config>router>ldp#
```

Clear Commands

fec-egress-statistics

Syntax **fec-egress-statistics** [*ip-prefix/mask*]

Context clear>router>ldp

Description This command clears LDP FEC egress statistics..

ip-prefix — Specify information for the specified IP prefix and mask length. Host bits must be 0.

mask — Specifies the 32-bit address mask used to indicate the bits of an IP address that are being used for the subnet address.

Values 0 — 32

instance

Syntax **instance**

Context clear>router>ldp

Description This command resets the LDP instance.

interface

Syntax **interface** [*ip-int-name*]

Context clear>router>ldp

Description This command restarts or clears statistics for LDP interfaces.

Parameters *ip-int-name* — The name of an existing interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

peer

Syntax **peer** [*ip-address*] [**statistics**]

Context clear>router>ldp

Description This command restarts or clears statistics for LDP targeted peers.

Parameters *ip-address* — The IP address of a targeted peer.

statistics — Clears only the statistics for a targeted peer

session

Syntax **session** [*ip-addr*[:*label-space*]] [**statistics**]

Context clear>router>ldp

Description This command restarts or clears statistics for LDP sessions.

Parameters *label-space* — Specifies the label space identifier that the router is advertising on the interface.

Values 0 — 65535

statistics — Clears only the statistics for a session.

statistics

Syntax **statistics**

Context clear>router>ldp

Description This command clears LDP instance statistics.

Debug Commands

The following output shows debug LDP configurations discussed in this section.

```
A:ALA-12# debug router ldp peer 10.10.10.104
A:ALA-12>debug>router>ldp# show debug ldp
debug
    router "Base"
        ldp peer 10.10.10.104
            event
                bindings
                messages
            exit
            packet
                hello
                init
                keepalive
                label
            exit
        exit
    exit
exit
A:ALA-12>debug>router>ldp#
```

ldp

Syntax [**no**] **ldp**

Context debug>router

Description Use this command to configure LDP debugging.

interface

Syntax [**no**] **interface** *interface-name*

Context debug>router>ldp

Description Use this command for debugging an LDP interface.

Parameters *interface-name* — The name of an existing interface.

peer

Syntax [**no**] **peer** *ip-address*

Context debug>router>ldp

Description Use this command for debugging an LDP peer.

Parameters ***ip-address*** — The IP address of the LDP peer.

event

Syntax [**no**] **event**

Context debug>router>ldp>if
debug>router>ldp>peer

Description This command configures debugging for specific LDP events.

bindings

Syntax [**no**] **bindings**

Context debug>router>ldp>peer>event

Description This command displays debugging information about addresses and label bindings learned from LDP peers for LDP bindings.

The **no** form of the command disables the debugging output.

messages

Syntax [**no**] **messages**

Context debug>router>ldp>if>event
debug>router>ldp>peer>event

Description This command displays specific information (for example, message type, source, and destination) regarding LDP messages sent to and received from LDP peers.

The **no** form of the command disables debugging output for LDP messages.

packet

Syntax **packet** [**detail**]
no packet

Context debug>router>ldp>if
debug>router>ldp>peer

Description This command enables debugging for specific LDP packets.

The **no** form of the command disables the debugging output.

Parameters **detail —** Displays detailed information.

hello

Syntax **hello** [**detail**]
no hello

Context debug>router>ldp>if>packet
debug>router>ldp>peer>packet

Description This command enables debugging for LDP hello packets.

The **no** form of the command disables the debugging output.

Parameters **detail —** Displays detailed information.

init

Syntax **init** [**detail**]
no init

Context debug>router>ldp>peer>packet

Description This command enables debugging for LDP Init packets.

The **no** form of the command disables the debugging output.

Parameters **detail —** Displays detailed information.

keepalive

Syntax [**no**] **keepalive**

Context debug>router>ldp>peer>packet

Description This command enables debugging for LDP Keepalive packets.

The **no** form of the command disables the debugging output.

label

Syntax **label** [**detail**]
no label

Context debug>router>ldp>peer>packet

Description This command enables debugging for LDP Label packets.

The **no** form of the command disables the debugging output.

Parameters **detail —** Displays detailed information.

Standards and Protocol Support

Standards Compliance

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ah Provider Backbone Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.1ak Multiple MAC Registration Protocol
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ae 10Gbps Ethernet
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3x Flow Control
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
ITU-T G.8031 Ethernet linear protection switching

Protocol Support

OSPF

RFC 1765 OSPF Database Overflow
RFC 2328 OSPF Version 2
RFC 2370 Opaque LSA Support
RFC 2740 OSPF for IPv6 (OSPFv3) draft-ietf-ospf-ospfv3-update-14.txt
RFC 3101 OSPF NSSA Option
RFC 3137 OSPF Stub Router Advertisement
RFC 3623 Graceful OSPF Restart — GR helper
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV

BGP

RFC 1397 BGP Default Route Advertisement
RFC 1772 Application of BGP in the Internet
RFC 1965 Confederations for BGP
RFC 1997 BGP Communities Attribute
RFC 2385 Protection of BGP Sessions via MD5
RFC 2439 BGP Route Flap Dampening
RFC 2547bis BGP/MPLS VPNs
RFC 2918 Route Refresh Capability for BGP-4
RFC 3107 Carrying Label Information in BGP-4
RFC 3392 Capabilities Advertisement with BGP4
RFC 4271 BGP-4 (previously RFC 1771)
RFC 4360 BGP Extended Communities Attribute
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2547bis BGP/MPLS VPNs)
RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 & 2796)
RFC 4724 Graceful Restart Mechanism for BGP — GR helper
RFC 4760 Multi-protocol Extensions for BGP
RFC 4893 BGP Support for Four-octet AS Number Space
RFC 5065 Confederations for BGP (obsoletes 3065)

IS-IS

RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
RFC 2763 Dynamic Hostname Exchange for IS-IS
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
RFC 3567 Intermediate System to Intermediate System (ISIS) Cryptographic Authentication
RFC 3719 Recommendations for Interoperable Networks using IS-IS
RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
RFC 3787 Recommendations for Interoperable IP Networks
RFC 3847 Restart Signaling for IS-IS — GR helper
RFC 4205 for Shared Risk Link Group (SRLG) TLV
draft-ietf-isis-igp-p2p-over-lan-05.txt

LDP

RFC 3036 LDP Specification
RFC 3037 LDP Applicability
RFC 3478 Graceful Restart Mechanism for LDP — GR helper
RFC 5283 LDP extension for Inter-Area LSP
draft-jork-ldp-igp-sync-03

IPSec

RFC 2401 Security Architecture for the Internet Protocol
RFC 2409 The Internet Key Exchange (IKE)
RFC 3706 IKE Dead Peer Detection
RFC 3947 Negotiation of NAT-Traversal in the IKE
RFC 3948 UDP Encapsulation of IPsec ESP Packets

draft-ietf-ipsec-isakmp-xauth-06.txt — Extended Authentication within ISAKMP/Oakley (XAUTH)

draft-ietf-ipsec-isakmp-modecfg-05.txt — The ISAKMP Configuration Method

IPv6

RFC 1981 Path MTU Discovery for IPv6

RFC 2375 IPv6 Multicast Address Assignments

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

RFC 2461 Neighbor Discovery for IPv6

RFC 2462 IPv6 Stateless Address Auto configuration

RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification

RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels

RFC 2545 Use of BGP-4 Multiprotocol Extension for IPv6 Inter-Domain Routing

RFC 2710 Multicast Listener Discovery (MLD) for IPv6

RFC 2740 OSPF for IPv6

RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses

RFC 3315 Dynamic Host Configuration Protocol for IPv6

RFC 3587 IPv6 Global Unicast Address Format

RFC3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol

RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6

RFC 4007 IPv6 Scoped Address Architecture

RFC 4193 Unique Local IPv6 Unicast Addresses

RFC 4291 IPv6 Addressing Architecture

RFC 4552 Authentication/Confidentiality for OSPFv3

RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

RFC 5072 IP Version 6 over PPP

RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

draft-ietf-isis-ipv6-05

draft-ietf-isis-wg-multi-topology-xx.txt

Multicast

RFC 1112 Host Extensions for IP Multicasting (Snooping)

RFC 2236 Internet Group Management Protocol, (Snooping)

RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

RFC 2362 Protocol Independent Multicast-Sparse Mode (PIMSM)

RFC 3618 Multicast Source Discovery Protocol (MSDP)

RFC 3446 Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)

RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast

RFC 4607 Source-Specific Multicast for IP

RFC 4608 Source-Specific Protocol Independent Multicast in 232/8

RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)

draft-ietf-pim-sm-bsr-06.txt

draft-rosen-vpn-mcast-08.txt

draft-ietf-mboned-msdp-mib-01.txt

draft-ietf-l3vpn-2547bis-mcast-07: Multicast in MPLS/BGP IP VPNs

draft-ietf-l3vpn-2547bis-mcast-bgp-05: BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs

RFC 3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

MPLS

RFC 3031 MPLS Architecture

RFC 3032 MPLS Label Stack

Encoding (REV3443))

RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL

RFC 5332 MPLS Multicast Encapsulations

RIP

RFC 1058 RIP Version 1

RFC 2082 RIP-2 MD5 Authentication

RFC 2453 RIP Version 2

RSVP-TE

RFC 2430 A Provider Architecture DiffServ & TE

RFC 2702 Requirements for Traffic Engineering over MPLS

RFC2747 RSVP Cryptographic Authentication

RFC3097 RSVP Cryptographic Authentication

RFC 3209 Extensions to RSVP for Tunnels

RFC 3564 Requirements for Diff-Serv-aware TE

RFC 4090 Fast reroute Extensions to RSVP-TE for LSP Tunnels

RFC 4124 Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering

RFC 4125 Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering

RFC 4875 Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)

draft-ietf-mpls-soft-preemption-14 MPLS Traffic Engineering Soft Preemption

draft-ietf-ccamp-mpls-graceful-shutdown-06 Graceful Shutdown in GMPLS Traffic Engineering Networks

draft-ietf-mpls-p2mp-lsp-ping-06 Graceful Shutdown in GMPLS Traffic Engineering Networks

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)

RFC 2597 Assured Forwarding PHB Group (rev3260)

RFC 2598 An Expedited Forwarding PHB

RFC 3140 Per-Hop Behavior Identification Codes

TCP/IP

RFC 768 UDP
RFC 1350 The TFTP Protocol (Rev.
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 951 BootP (rev)
RFC 1519 CIDR
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer
Size option
RFC 2401 Security Architecture for Internet Protocol
draft-ietf-bfd-mib-00.txtBidirectional Forwarding Detection Management Information Base
draft-ietf-bfd-base-05.txt Bidirectional Forwarding Detection
draft-ietf-bfd-v4v6-1hop-06.txt BFD IPv4 and IPv6 (Single Hop)
draft-ietf-bfd-multihop-06.txt BFD for Multihop Paths

VRRP

RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768 Virtual Router Redundancy Protocol
draft-ietf-vrrp-unified-spec-02: Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

PPP

RFC 1332 PPP IPCP
RFC 1377 PPP OSINLCP
RFC 1638/2878PPP BCP
RFC 1661 PPP (rev RFC2151)
RFC 1662 PPP in HDLC-like Framing
RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2516 A Method for Transmitting PPP Over EthernetRFC 2615 PPP over SONET/SDH
RFC 2686 The Multi-Class Extension to Multi-Link PPP

Frame Relay

FRF.1.2 - PVC User-to-Network Interface (UNI) Implementation Agreement
FRF.5 - Frame Relay/ATM PVC Network Interworking Implementation
ANSI T1.617 Annex D, DSS1 — Signalling Specification For Frame Relay Bearer Service.
FRF2.2 -PVC Network-to- Network Interface (NNI) Implementation Agreement.
FRF.12 Frame Relay Fragmentation Implementation Agreement
FRF.16.1 Multilink Frame Relay UNI/NNI Implementation Agreement
ITU-T Q.933 Annex A-Additional procedures for Permanent Virtual Connection (PVC) status management

ATM

RFC 1626 Default IP MTU for use over ATM AAL5
RFC 2514 Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management
RFC 2515 Definition of Managed Objects for ATM Management RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
AF-TM-0121.000 Traffic Management Specification Version 4.1
ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95
ITU-T Recommendation I.432.1 — BISDN user-network interface — Physical layer specification: General characteristics
GR-1248-CORE - Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3
GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1
AF-ILMI-0065.000 Integrated Local Management Interface (ILMI) Version 4.0
AF-TM-0150.00 Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR
AF-PHY-0086.001,Inverse Multiplexing for ATM (IMA) Specification Version 1.1

DHCP

RFC 2131 Dynamic Host Configuration Protocol (REV)
RFC 3046 DHCP Relay Agent Information Option (Option 82)
RFC 1534 Interoperation between DHCP and BOOTP

VPLS

RFC 4762 Virtual Private LAN Services Using LDP
draft-ietf-l2vpn-vpls-mcast-reqts-04
draft-ietf-l2vpn-signaling-08

PSEUDO-WIRE

RFC 3985 Pseudo Wire Emulation Edge-to-Edge (pseudowireE3)
RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC 4717 Encapsulation Methods for Transport ATM over MPLS Networks (draft-ietf-pwe3-atm-encap-10.txt)
RFC 4816 PWE3 ATM Transparent Cell Transport Service (draft-ietf-pwe3-cell-transport-04.txt)
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)

RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks (draft-ietf-pwe3-frame-relay-07.txt)
RFC 4446 IANA Allocations for PWE3
RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)
RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV):A Control Channel for Pseudowires
draft-ietf-l2vpn-vpws-iw-oam-02.txt
draft-ietf-pwe3-oam-msg-map-05-txt
draft-ietf-l2vpn-arp-mediation-04.txt
draft-ietf-pwe3-ms-pw-arch-05.txt
draft-ietf-pwe3-segmented-pw-11.txt
draft-hart-pwe3-segmented-pw-vccv-02.txt
draft-muley-dutta-pwe3-redundancy-bit-02.txt
draft-muley-pwe3-redundancy-02.txt
MFA Forum 9.0.0 The Use of Virtual trunks for ATM/MPLS Control Plane Interworking
MFA Forum 12.0.0 Multiservice Interworking - Ethernet over MPLS
MFA forum 13.0.0 - Fault Management for Multiservice Interworking v1.0
MFA Forum 16.0.0 — Multiservice Interworking - IP over MPLS

ANCP/L2CP

draft-ietf-ancp-framework-01.txt
draft-ietf-ancp-protocol-00.txt

CIRCUIT EMULATION

RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
MEF-8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks, October 2004
RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks

SONET/SDH

ITU-G.841 Telecommunication Standardization Section of ITU, Types and Characteristics of
SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txtSSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

Timing

GR-253-CORE SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000
ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008
ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.
GR-1244-CORE Clocks for the Synchronized Network: Common Generic Criteria, Issue 3,May 2005
ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.
ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.
ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.

NETWORK MANAGEMENT

ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1657 BGP4-MIB
RFC 1724 RIPv2-MIB
RFC 1850 OSPF-MIB
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2206 RSVP-MIB
RFC 2452 IPv6 Management Information Base for the
Transmission Control Protocol
RFC 2454 IPv6 Management Information Base for the User Datagram Protocol
RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group
RFC 2558 SONET-MIB
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-
NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASEDACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB

RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 2987 VRRP-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 - Simple Network Management Protocol (SNMP) Applications
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 - SNMP MIB
RFC 5101 - Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information
draft-ietf-disman-alarm-mib-04.txt
draft-ietf-ospf-mib-update-04.txt
draft-ietf-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
draft-ietf-mpls-ldp-mib-07.txt
draft-ietf-isis-wg-mib-05.txt
IANA-IFType-MIB
IEEE8023-LAG-MIB

Proprietary MIBs

TIMETRA-APS-MIB.mib
TIMETRA-ATM-MIB.mib
TIMETRA-BGP-MIB.mib
TIMETRA-BSX-NG-MIB.mib
TIMETRA-CAPABILITY-7750-V4v0.mib
TIMETRA-CFLOWD-MIB.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IGMP-MIB.mib
TIMETRA-ISIS-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-NG-BGP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-OSPF-NG-MIB.mib
TIMETRA-OSPF-V3-MIB.mib
TIMETRA-PIM-NG-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-RIP-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SUBSCRIBER-MGMTMIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRRP-MIB.mib
TIMETRA-VRTR-MIB.mib

INDEX