NOKIA

7210 SERVICE ACCESS SWITCH

7210 SAS OS 7210 SAS-K 2F4T6C MPLS Guide
Release 9.0.R8

3HE12059AAAETQZZA

Issue: 01

September 2017

Table of Contents

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 7210 SAS-K2F4T6C Series 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.

NOTES:

- 7210 SAS-K5 stands for 7210 SAS-K 2F2T1C and 7210 SAS-K12 stands for 7210 SAS-K 2F4T6C platforms.
- 7210 SAS-E, 7210 SAS-D, and 7210 SAS-K 2F2T1C operate in access-uplink mode by default. There is no need of an explicit user configuration needed for this.
  7210 SAS-K 2F4T6C operates in Access-uplink mode and Network mode. There is no explicit BOF configuration required for it.

Audience

This manual is intended for network administrators responsible for configuring the 7210 SAS Series 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:

- Multi protocol Label Switching (MPLS)
- Resource Reservation Protocol (RSVP)

List of Technical Publications

The 7210- D, 7210 SAS-E, 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C documentation set is composed of the following books:

- 7210- D, 7210 SAS-E, 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C Basic System Configuration Guide

  This guide describes basic system configurations and operations.
- 7210- D, 7210 SAS-E, 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.
- 7210- D, 7210 SAS-E, 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.
- 7210- D, 7210 SAS-E, 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C 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.
- 7210- D and 7210 SAS-E OS Services Guide

  This guide describes how to configure service parameters such as customer information and user services.
- 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C OS Services Guide

  This guide describes how to configure service parameters such as customer information and user services.
- 7210- D, 7210 SAS-E, 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.
- 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C Quality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.
- 7210 SAS-K 2F4T6C OS MPLS Guide

  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).
- 7210 SAS-K 2F2T1C and 7210 SAS-K 2F4T6C OS Routing Protocols Guide
  This guide provides an overview of routing concepts and provides configuration examples for OSPF, IS-IS and route policies.

Getting Started

In This Chapter

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

Nokia 7210 SAS-K 2F4T6C 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 18
	• RSVP	RSVP on page 28
	• LDP	Label Distribution Protocol on page 153
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 239

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 connection less 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) and frame relay network protocols.

The 7210 SAS routers enable service providers to deliver virtual private networks (VPNs) and Internet access using MPLS tunnels, with Ethernet interfaces.

On the 7210 SAS-K 2F4T6C, is designed to fit into a network using the principles of seamless MPLS architecture which enable access devices with smaller IP routing scale (both control-plane RIB and FIB) and smaller MPLS scale (both control-plane and FIB) to be used to deploy MPLS end-to-end and benefit from the traffic engineering and resiliency mechanism that MPLS provides. The MPLS features and capabilities available on 7210 SAS-K2F4T6C is described in this user guide.

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.

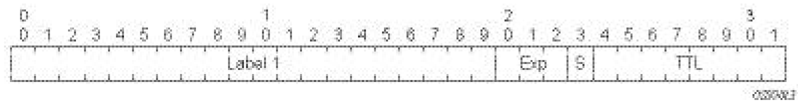


Figure 1: Label Placement

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).

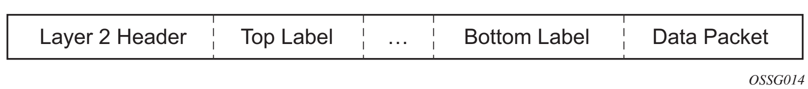


Figure 2: Label Packet Placement

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 21) 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 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 RSVP, so a value is reserved.
- Values 4-15 are reserved for future use.

7210 SAS devices 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 32768through 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 28.

→ 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.

7210 SAS-K2F4T6C supports the following functionality:

- MPLS LSR functionality.
- MPLS LER functionality with the following support:
  - → Static LSPs.
  - → RSVP signaled LSPs with support for both explicit-path LSP and constrained-path LSPs.
  - → LDP signaled LSPs are not supported.
- Support for FRR one-to-one and FRR facility bypass for RSVP signaled LSPs.

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

The 7210 SAS supports Manual bypass tunnels, on implementation of the Manual bypass feature a LSP can be pre-configured from a PLR which is used exclusively for bypass protection. If a path message for a new LSP requests for bypass protection, the node checks if a manual bypass tunnel satisfying the path constraints exists. If a tunnel is found, it is selected. If no such tunnel exists by default, the 7210 SAS dynamically signals a bypass LSP.

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.

PLR Bypass LSP Selection Rules

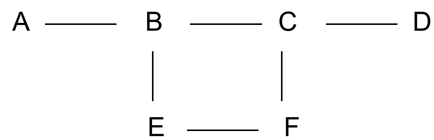


Figure 3: Bypass Tunnel Nodes

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:

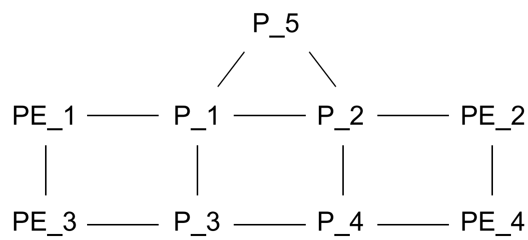


Figure 4: FRR Node-Protection Example

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_2.
- 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 signaled and LSP 1 will get associated with this new bypass tunnel.

Uniform FRR Failover Time

The failover time during FRR consists of a detection time and a switchover time. The detection time corresponds to the time it takes for the RSVP control plane protocol to detect that a network IP interface is down or that a neighbor/next-hop over a network IP interface is down. The control plane can be informed of an interface down event when event is due to a failure in a lower layer such in the physical layer. The control plane can also detect the failure of a neighbor/next-hop on its own by running a protocol such as Hello, Keep-Alive, or BFD.

The switchover time is measured from the time the control plane detected the failure of the interface or neighbor/next-hop to the time the IOM completed the reprogramming of all the impacted ILM or service records in the data path. This includes the time it takes for the control plane to send a down notification to all IOMs to request a switch to the backup NHLFE.

Uniform Fast-Reroute (FRR) failover enables the switchover of MPLS and service packets from the outgoing interface of the primary LSP path to that of the FRR backup LSP within the same amount of time regardless of the number of LSPs or service records. This is achieved by updating Ingress Label Map (ILM) records and service records to point to the backup Next-Hop Label to Forwarding Entry (NHLFE) in a single operation.

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.

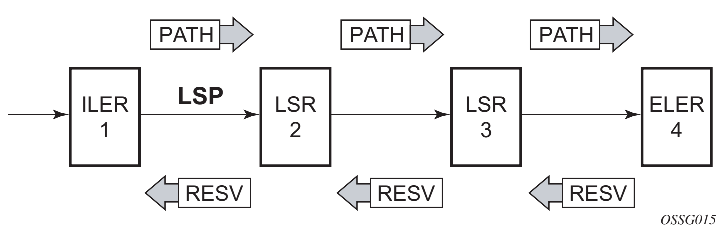


Figure 5: Establishing LSPs

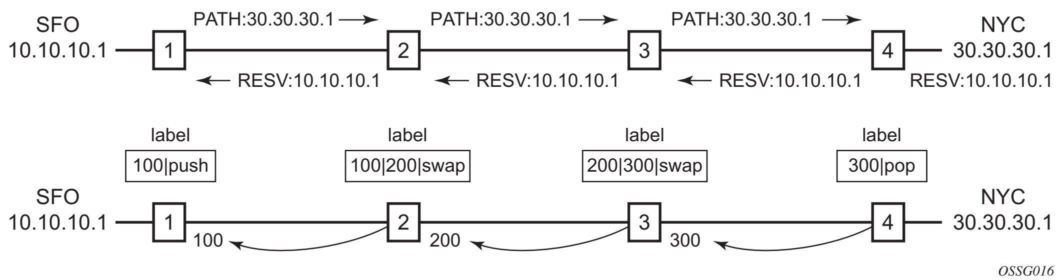


Figure 6: LSP Using RSVP Path Set Up

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 30
- MD5 Authentication of RSVP Interface on page 30

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 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:

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 PLR 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 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 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 node does not attempt to send summary refresh messages.

Configuring Implicit Null

The implicit null label option allows a router 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 implicit-null-label command in the config>router>rsvp context. The user must shutdown RSVP before being able to change the implicit null configuration option.

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 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>if>label-map>swap implicit-null-label nexthop ip-address

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

Advanced MPLS/RSVP Features

LSP Path Change

The **tools perform router mpls update-path** {**lsp** *lsp-name* **path** *current-pathname* **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.

Manual LSP Path Switch

This feature provides a new command to move the path of an LSP from a standby secondary to another standby secondary.
The base version of the command allows the path of the LSP to move from a standby (or an active secondary) to another standby of the same priority. If a new standby path with a higher priority or a primary path comes up after the tools perform command is executed, the path re-evaluation command runs and the path is moved to the path specified by the outcome of the re-evaluation.
The CLI command for the base version is:
tools perform router mpls switch-path lsp *lsp-name* **path** *path-name*
The sticky version of the command can be used to move from a standby path to any other standby path regardless of priority. The LSP remains in the specified path until this path goes down or the user performs the no form of the tools perform command.
The CLI commands for the sticky version are:
tools perform router mpls force-switch-path lsp *lsp-name* **path** *path-name*
tools perform router mpls no force-switch-path lsp *lsp-name*

Make-Before-Break (MBB) Procedures for LSP/Path Parameter Configuration Change

When an LSP is switched from an existing working path to a new path, it is desirable to perform this in a hitless fashion. The Make-Before-Break (MBB) procedure consist of first signaling the new path when it is up, and having the ingress LER move the traffic to the new path. Only then the ingress LER tears down the original path.

MBB procedure is raised during the following operations:

1. Timer based and manual re-signal of an LSP path.
2. Fast-ReRoute (FRR) global revertive procedures.
3. Traffic-Engineering (TE) graceful shutdown procedures.

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 7).

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 (For more information, see srlg-frr on page 77)
- 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.

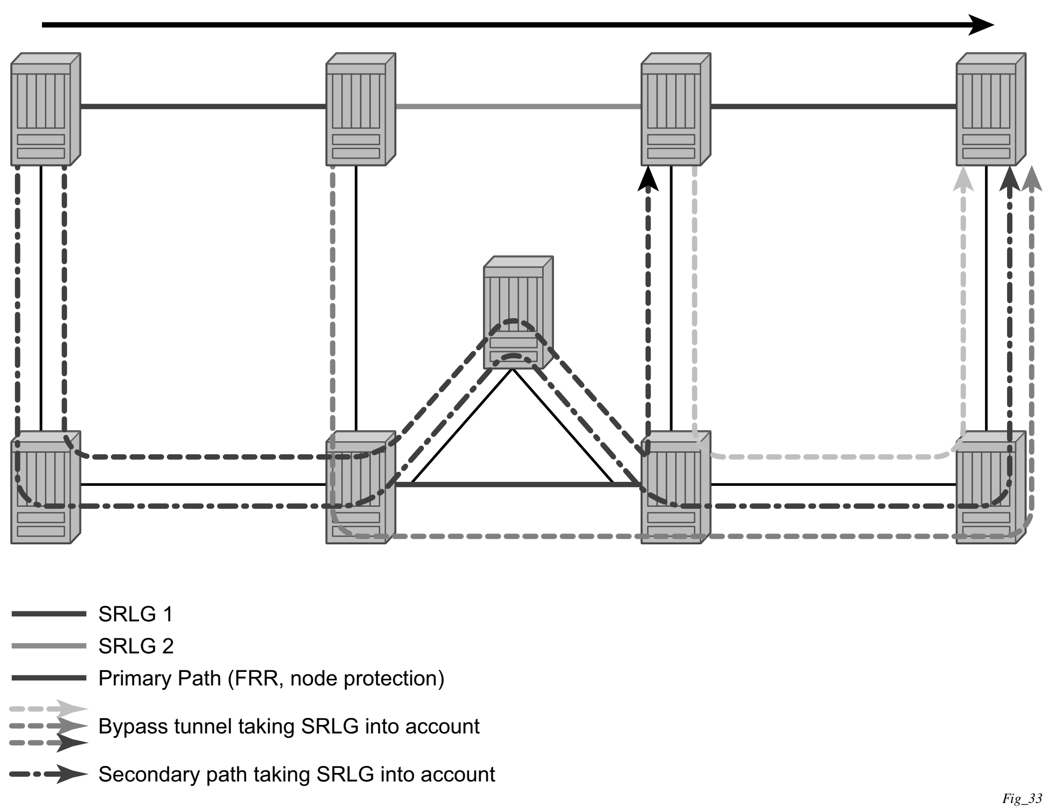


Figure 7: Shared Risk Link Groups

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 7210 SAS 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 7210 SAS will interpret with routers that do not implement the SRLG membership advertisement through 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 7210 SAS 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 RFC 5817, *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.

MPLS/RSVP Configuration Process Overview

Figure 8 displays the process to configure MPLS and RSVP parameters.

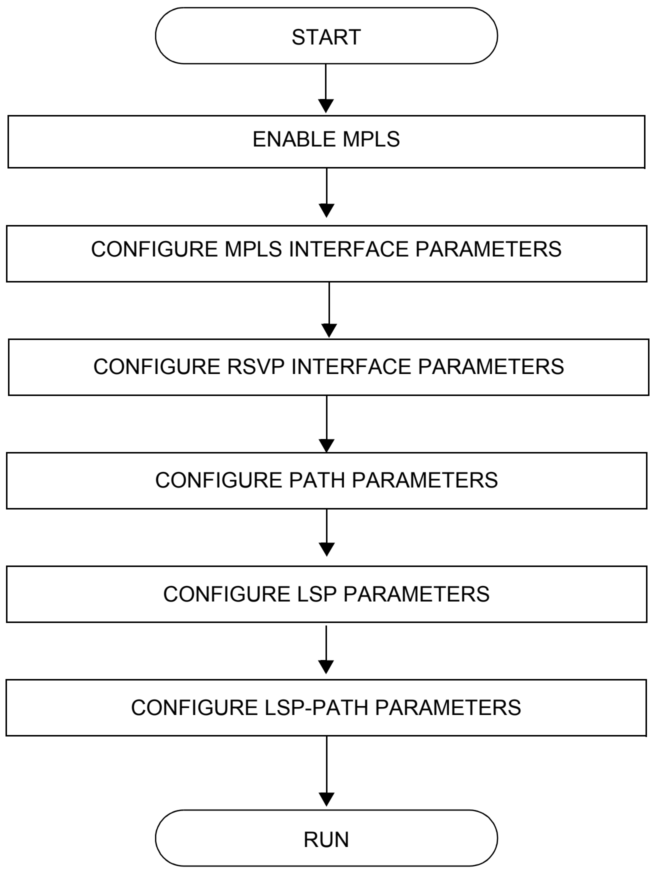


Figure 8: MPLS and RSVP Configuration and Implementation Flow

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

Multi protocol 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 46
- Paths on page 46
- Router Interface on page 47

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 automatically manages label values. Labels that are automatically assigned have values ranging from 1,024 through 1,048,575 (see Label Values on page 20).

A static LSP is a manually set up LSP where the next hop 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 if you are configuring static LSPs.

If dynamic LSP signaling is implemented in your network, then RSVP 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 must be enabled on the same routers.

When MPLS is enabled and either RSVP is also enabled, MPLS uses RSVP 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 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 50
- Configuring an MPLS Interface on page 51
- Configuring MPLS Paths on page 52
- Configuring an MPLS LSP on page 53
- Configuring a Static LSP on page 54
- Configuring RSVP Parameters on page 57
- Configuring RSVP Message Pacing Parameters on page 58

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.

Listed below are the steps to configure the manual bypass tunnels:

1. Configure the option to disable the dynamic bypass tunnels on the 7210 SAS node B (if required). The CLI for this configuration is:
   config>router>mpls>dynamic-bypass [disable | enable]
   The dynamic bypass tunnels are enabled by default.

2. Configure an LSP on node B, such as B-E-F-C which is 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:7210 SAS>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:7210 SAS >config>router>mpls>path#
```

3. Configure an LSP from A to D and indicate fast-reroute bypass protection, select the facility as “FRR method”. (Config>router>mpls>lsp>fast-reroute facility).

   Observe if the following criterions apply:

   → If the LSP passes through B

   → A bypass is requested

   → The next hop is C

   → A manually configured bypass-only tunnel exists from B to C (excluding link B to C)

Result: Node B uses the manually configured bypass-only tunnel from B to C.

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

Enable TE graceful shutdown on the maintenance interface using the **config>router>rsvp>interface>graceful-shutdown** command.

Disable graceful shutdown by executing the **no** form of the command at the RSVP interface level or at the RSVP level. This restores the user-configured TE parameters of the maintenance links, and the 7210 SAS maintenance node floods them.

MPLS Configuration Management Tasks

This section discusses the following MPLS configuration management tasks:

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 53.

```
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 52.

```
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 54.

```
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 65
- Modifying RSVP Message Pacing Parameters on page 66
- Deleting an Interface from RSVP on page 66

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 57.

```
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 64 for information on deleting an MPLS interface.

MPLS/RSVP Command Reference

Command Hierarchies

MPLS Commands

config
— **router**
— [**no**] **mpls**
— **dynamic-bypass** [**enable** | **disable**]
— [**no**] **frr-object**
— **hold-timer** *seconds*
— **no hold-timer**
— [**no**] **interface** *ip-int-name*
— [**no**] **admin-group** *group-name* [*group-name*...(up to 5 max)]
— **label-map** *in-label*
— **no label-map** *in-label*
— **no pop**
— **pop**
— **no shutdown**
— **shutdown**
— **swap** *out-label* **nexthop** *ip-address*
— **swap implicit-null-label nexthop** *ip-address*
— **no swap**
— **no shutdown**
— **shutdown**
— [**no**] **srlg-group** *group-name* [*group-name*...(up to 5 max)]
— **te-metric** *metric*
— **no te-metric**
— **resignal-timer** *minutes*
— **no resignal-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**]

— [**no**] **static-lsp** *lsp-name*
— **no push** *label*
— **push** *label* nexthop *ip-address*
— [**no**] **shutdown**
— **to** *ip-address*
— [**no**] **static-lsp-fast-retry** *seconds*
— **user-srlg-db** [**enable** | **disable**]

MPLS LSP Commands

config
— **router**
— [**no**] **mpls**
— [**no**] **lsp** *lsp-name* [bypass-only
— [**no**] **adaptive**
— [**no**] **adspec**
— **bgp-transport-tunnel** *include* | *exclude*
— [**no**] **cspf** [*use-te-metric*]
— [**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**] **include** *group-name* [*group-name*...(up to 5 max)]
— [**no**] **primary** *path-namex*
— [**no**] **adaptive**
— **bandwidth** *rate-in-mpbs*
— **no bandwidth**
— [**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)]
— [**no**] **record**
— [**no**] **record-label**
— [**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**
— [**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)]
— **[no] path-preference**
— [**no**] **record**
— [**no**] **record-label**
— [**no**] **shutdown**
— [**no**] **srlg**
— [**no**] **standby**

— [**no**] **shutdown**
— **to** *ip-address*

MPLS Path Commands

config
— **router**
— [**no**] **mpls**
— **[no] p2p-active-path-fast-retry**
— [**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**
— [**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**
— **hello-interval** *milli-seconds*
— **no hello-interval**
— [**no**] **refresh-reduction**
— [**no**] **reliable-delivery**
— [**no**] **shutdown**
— **subscription** *percentage*
— **no subscription**
— **keep-multiplier** *number*
— **no keep-multiplier**
— [**no**] **msg-pacing**
— **max-burst** *number*
— **no max-burst**
— **period** *milli-seconds*
— **no period**
— **rapid-retransmit-time** *hundred-milliseconds*
— **no rapid-retransmit-time**
— **rapid-retry-limit** *number*
— **no rapid-retry-limit**
— **refresh-time** *seconds*
— **no refresh-time**
— [**no**] **shutdown**

Show Commands

show
— **router**
— **mpls**
— **bypass-tunnel** [**to** *ip-address*] [**protected-lsp** *name*] [**dynamic** | **manual**] [**detail**]
— **interface** [*ip-int-name*|*ip-address*] [**label-map** *label*]
— **interface** [*ip-int-name*|*ip-address*]
— **label** *start-label* [*end-label* | *in-use* | *label-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**]
— **srlg-database** [**router-id** *ip-address*] [**interface** *ip-address*]
— **static-lsp** [*lsp-name*]
— **static-lsp** {**transit** | **terminate**}
— **static-lsp count**
— **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

- **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*...(upto 8 max)]] [**use-te-metric**] [**strict-srlg**] [**srlg-group** grp-id...(up to 8 max)] [**skip-interface** *interface-name*]
      - **force-switch-path** [**lsp** *lsp-name*] [**path** *path-name*]
      - [**no**] **force-switch-path** [**lsp** *lsp-name*]
      - **resignal** {**lsp** *lsp-name* **path** *path-name* | **delay** *minutes*}
      - **switch-path** **[lsp** *lsp-name***] [path** *path-name***]**
      - **trap-suppress** *number-of-traps time-interval*
      - **update-path** {**lsp** *lsp-name* **path** *current-path-name* **new-path** *new-path-name*}

Clear Commands

clear
- **router**
  - **mpls**
    - **interface** [*ip-int-name*]
    - **lsp** *lsp-name*
  - **rsvp**
    - **interface** [*ip-int-name*] [statistics]
    - **statistics**

Debug Commands

debug
- — **router**
  - — **mpls** [**lsp** ***lsp-name***] [**sender** ***source-address***] [**endpoint** ***endpoint-address***] [**tunnel-id** *tunnel-id*] [**lsp-id** *lsp-id*]
  - — **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**
      - — **auth**
      - — **no auth**
      - — **misc** [**detail**]
      - — **no misc**
      - — **nbr** [**detail**]
      - — **no nbr**
      - — **path** [**detail**]
      - — **no path**
      - — **resv** [**detail**]
      - — **no resv**
      - — **rr**
      - — **no rr**
    - — [**no**] **packet**
      - — **all** [**detail**]
      - — **no all**
      - — **ack**
      - — **bundle** [**detail**]
      - — **no bundle**
      - — **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**
— **srefresh** [**detail**]
— **no srefresh**

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** 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.

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.

Note :Implict NULL must be enabled for use of Manual Bypass or Dynamic Bypass (FRR facility) if the 7210 is used as a egress LER and/or is a Merge Point.

Default enable

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.

Default 1 second

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

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

srlg-frr

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

Context config>router>mpls

Description This command enables the use of the Shared Risk Link 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.

Enabling or disabling srlg-frr only takes effect after LSP paths are resignaled. This can be achieved by shutting down and re-enabling MPLS. Another option is using the **tools perform router mpls resignal** command. However, note that while the latter might be less service impacting, only originating LSPs can be resignaled with the **tools** command. If also local transit and bypass LSPs are to be resignaled, the **tools** command must be executed on all ingress nodes in the network. The same might be locally achieved by disabling and enabling using the **configure router mpls dynamic-bypass** command, but this can trigger the LSP to go down and traffic loss to occur in case detour or bypass LSP is in use.

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)

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.

Values [a.b.c.d]

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.

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 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.

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 setup 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 generates 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 **no push** *label*
push *label* **nexthop** *ip-address*

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 *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 staticLSP.

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. This command is required while creating an LSP. 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

static-lsp-fast-retry

Syntax **static-lsp-fast-retry seconds**
[no] static-lsp-fast-retry

Context config>router>mpls

Description This command specifies the value used as the fast retry timer for a static LSP.

When a static LSP is trying to come up, the MPLS request for the ARP entry of the LSP next-hop may fail when it is made while the next-hop is still down or unavailable. In that case, MPLS starts a retry timer before making the next request. This enhancement allows the user to configure the retry timer, so that the LSP comes up as soon as the next-hop is up.

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

Default no static-fast-retry-timer

Parameters *seconds* — Specifies the value, in seconds, used as the fast retry timer for a static LSP.

Values 1-30

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 configures the admin group membership of an interface. The user can apply admin groups to an IES, VPRN, network IP, or MPLS interface. Each single operation of the admin-group command allows a maximum of five (5) groups to be specified at a time. However, a maximum of 32 groups can be added to a given interface through multiple operations. Once an admin group is bound to one or more interface, its value cannot be changed until all bindings are removed. The configured admin-group membership will be applied in all levels/areas the interface is participating in. The same interface cannot have different memberships in different levels/areas. It should be noted that only the admin groups bound to an MPLS interface are advertised in TE link TLVs and sub-TLVs when the traffic-engineering option is enabled in IS-IS or OSPF. IES andVPRN interfaces do not have their attributes advertised in TE TLVs.

The no form of this command deletes one or more of the admin-group memberships of an interface.

The user can also delete all memberships of an interface by not specifying a group name.

Default no admin-group

Parameters *group-name* — Specifies the name of the group with up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain.

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

LSP Commands

lsp

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

Context config>router>mpls

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

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 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 selects it. If no manual bypass tunnel is found, the 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.

adaptive

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

Context config>router>mpls>lsp

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 for this LSP. The ADSPEC object is used by the ingress LER to discover the minimum value of the MTU for links in the path of the LSP. By default, the ingress LER derives the LSP MTU from that of the outgoing interface of the LSP path.

Note that a bypass LSP always signals the ADSPEC object since it protects both primary paths which signal the ADSPEC object and primary paths which do not. This means that MTU of LSP at ingress LER may change to a different value from that derived from the outgoing interface even if the primary path has ADSPEC disabled.

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

Parameters

bgp-transport-tunnel

Syntax **bgp-transport-tunnel** *include* | *exclude*

Context config>router>mpls>lsp

Description This command allows or blocks RSVP-TE LSP to be used as a transport LSP for BGP tunnel routes.

Default bgp-transport-tunnel *exclude*

Parameters *include* — Allows RSVP-TE LSP to be used as transport LSP from ingress PE to ASBR in the local AS.

exclude — Blocks RSVP-TE LSP to be used as transport LSP from ingress PE to ASBR in the local AS.

cspf

Syntax [**no**] **cspf** [*use-te-metric*]

Context config>router>mpls>lsp

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

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

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.

bandwidth

Syntax **bandwidth** *rate-in-mbps*
no bandwidth

Context config>router>mpls>lsp>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

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

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

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

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.

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.

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.

Default No default

Parameters *ip-address* — The system IP address of the egress router.

retry-limit

Syntax **retry-limit** *number*
no retry-limit

Context config>router>mpls>lsp

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.

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

Description This command configures the time, in seconds, for LSP re-establishment attempts after it has failed.

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

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**

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

bandwidth

Syntax **bandwidth** *rate-in-mbps*
no bandwidth

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

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

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 remains an 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.

Values 1–255

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:

1. A successful MBB of the standby SRLG path which makes it eligible again.
2. 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.
3. 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

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.

p2p-active-path-fast-retry

Syntax **p2p-active-path-fast-retry** *seconds*
no p2p-active-path-fast-retry

Context config>router>mpls

Description This command configures a global parameter to allow the user to apply a shorter retry timer for the first try after an active LSP path went down due to a local failure or the receipt of a RESVTear. This timer is used only in the first try. Subsequent retries will continue to be governed by the existing LSP level retry-timer.

Default 0 (disabled)

Parameters *seconds* — Specifies the length of time for retry timer, in seconds

Values 1 to 10 seconds

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* **nexthop** *ip-address*
no push {*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 **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 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.

Parameters *ip-address* — The system IP address of the egress router.

Default none

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

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).

NOTE: For more information to know the list of protocols that support BFD, see 7210 SAS Router Configuration Guide.

The no form of this command removes BFD from the associated RSVP protocol adjacency.

Default no bfd-enable

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

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 7210 SAS PLR node or terminating on this 7210 SAS 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, which-ever 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** *limit*
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 *limit* — 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

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 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 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.

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.

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

Description This command enables the use of the implicit null label for all LSPs signalled by RSVP on the node.

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.

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 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

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

Parameters *number —*

Values 100 — 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

Parameters *milli-seconds —*

Values 100 — 1000 milliseconds in increments of 10 milliseconds

Show Commands

bypass-tunnel

Syntax **bypass-tunnel** [**to** *ip-address*] [**protected-lsp** [*lsp-name*]] [**dynamic** | **manual**] [**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.

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:Dut-A>show>router>mpls# bypass-tunnel
===============================================================================
MPLS Bypass Tunnels
===============================================================================
Legend :  m - Manual      d - Dynamic
===============================================================================
To              State  Out I/F        Out Label     Reserved   Protected  Type
                                                    BW (Kbps)  LSP Count
-------------------------------------------------------------------------------
10.10.36.3      Up     lag-1:10       131066        0          2          d

10.10.23.2      Up     lag-1:10       130454        0          4          d

10.10.46.4      Up     lag-2          130592        0          4          d
```

```
10.10.36.6      Up     lag-2         130591        0          2          d
-------------------------------------------------------------------------------
Bypass Tunnels : 4
===============================================================================
*A:Dut-A>show>router>mpls#
```

interface

Syntax **interface** [*ip-int-name* **|** *ip-address*] [**label-map** *label*]
interface [*ip-int-name* **|** *ip-address*]

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

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.
Srlg Groups	Specifies the shared risk link group (SRLG) name(s).
Te-metric	Specifies the traffic engineering metric used on the interface.
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.

Label	Description (Continued)
Type	Specifies whether the label value is statically or dynamically assigned.

```
A:7210SAS# show router mpls interface

===============================================================================
MPLS Interfaces
===============================================================================
Interface                           Port-id           Adm    Opr    TE-metric
-------------------------------------------------------------------------------
system                              system            Up     Up     None
  Admin Groups                      None
  Srlg Groups                       None
ip-10.10.2.3                        1/1/15            Up     Up     None
  Admin Groups                      None
  Srlg Groups                       None
ip-10.10.5.3                        1/1/1             Up     Up     None
  Admin Groups                      None
  Srlg Groups                       None
ip-10.10.11.3                       1/1/3             Up     Up     None
  Admin Groups                      None
  Srlg Groups                       None
ip-10.10.12.3                       lag-1             Up     Up     None
  Admin Groups                      None
  Srlg Groups                       None
-------------------------------------------------------------------------------
Interfaces : 5
===============================================================================
*A:7210SAS#
```

label

Syntax **label** *start-label* [*end-label* | *in-use* | *label-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.

Label	Description
`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:Dut-A# show router mpls-labels label-range

============================================================================
Label Ranges
============================================================================
Label Type      Start Label End Label   Aging       Available   Total
----------------------------------------------------------------------------
Static          32          18431       -           18399       18400
Dynamic         18432       131071      0           112635      112640
    Seg-Route   0           0           -           0           112640
============================================================================
```

```
*A:Dut-A#
```

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.
`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.

Label	Description (Continued)
`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.
`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.

Label	Description (Continued)
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.
VprnAutoBind	Displays the status on VPRN auto-bind feature as enabled or disabled.

Sample Output

```
*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:7210-SAS>show>router>mpls# lsp A detail

===============================================================================
MPLS LSPs (Originating) (Detail)
===============================================================================
-------------------------------------------------------------------------------
Type : Originating
-------------------------------------------------------------------------------
LSP Name    : A                              LSP Tunnel ID  : 1
From        : 2.2.2.2                        To             : 100.100.100.100
Adm State   : Up                             Oper State     : Down
LSP Up Time : 0d 00:00:00                    LSP Down Time  : 0d 00:05:42
Transitions : 2                              Path Changes   : 2
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         : Disabled                         ADSPEC         : Disabled
Metric       : 0
Include Grps:                                   Exclude Grps   :
None                                            None
Type         : RegularLsp                       Least Fill     : Disabled
LdpOverRsvp  : Enabled                          VprnAutoBind   : Enabled
Oper Metric  : 65535

Primary      : A                                Down Time      : 0d 00:05:42
Bandwidth    : 0 Mbps
===============================================================================
*A:7210-SAS>show>router>mpls# lsp 2 detail
```

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.

Label	Description (Continued)
`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#
```

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#
```

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.

```
*A:7210SAS# show router mpls status

===============================================================================
MPLS Status
===============================================================================
Admin Status       : Up                  Oper Status        : Up
Oper Down Reason   : n/a
FR Object          : Enabled             Resignal Timer     : Disabled
Hold Timer         : 1 seconds           Next Resignal      : N/A
Srlg Frr           : Disabled            Srlg Frr Strict    : Disabled
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
```

```
AB Sample Multipli*: 1                  AB Adjust Multipli*: 288
Exp Backoff Retry  : Disabled           CSPF On Loose Hop  : Disabled
Lsp Init RetryTime*: 30 seconds
Logger Event Bundl*: Disabled

Sec FastRetryTimer : Disabled           Static LSP FR Timer: 30 seconds
P2P Max Bypass Ass*: 1000
P2PActPathFastRetry: Disabled
In Maintenance Mode: No

LSP Counts          Originate           Transit             Terminate
-------------------------------------------------------------------------------
Static LSPs         0                   0                   0
Dynamic LSPs        0                   0                   1
Detour LSPs         0                   0                   0
===============================================================================
* indicates that the corresponding row element may have been truncated.
```

```
*A:7210SAS#
```

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.
`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.
`Active Resvs`	The total number of active RSVP sessions that have reserved bandwidth.

Label	Description (Continued)
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.
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.
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.

Label	Description (Continued)
`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.
`Hellos`	Total RSVP RESV HELLO REQ messages received on the interface.

Sample Output

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, manual-bypass

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#
```

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.

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
===============================================================================
*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**] [**srlggroup** grp-id...(up to 8 max)] [**skip-interface** *interface-name*]

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 Link Groups (SRLGs). An SRLG group represents a set of interfaces which could be subject to the same failures or defects and therefore, share the same risk of failing.

Values 0 — 4294967295

skip-interface *interface-name* — Specifies an interface name that should be skipped during setup.

resignal

Syntax **resignal** {**lsp** *lsp-name* **path** *path-name* | **delay** *minutes*}

Context tools>perform>router>mpls

Description This command resignal is 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.

switch-path

Syntax **switch-path** [**lsp** *lsp-name*] [**path** *path-name*]

Context tools>perform>router>mpls

Description Use this command to move from a standby (or an active secondary) to another standby of the same priority. If a new standby path with a higher priority or a primary path comes up after the **tools perform** command is executed, the path re-evaluation command runs and the path is moved to the path specified by the outcome of the re-evaluation.

Parameters *lsp-name* — Specifies an existing LSP name to move.

path-name — Specifies the path name to which to move the specified LSP.

Clear Commands

interface

Syntax **interface** *ip-int-name*

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.

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.

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*]
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.

auth

Syntax **auth**
no auth

Context debug>router>rsvp>event

Description This command debugs authentication events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about authentication 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.

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.

rr

Syntax **rr**
no rr

Context debug>router>rsvp>event

Description This command debugs refresh reduction events.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about refresh reduction events.

packet

Syntax [**no**] **packet**

Context debug>router>rsvp>

Description This command enters the syntax to debug packets.

ack

Syntax **ack [detail]**
no ack

Context debug>router>rsvp>packet

Description This command debugs ack packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about RSVP-TE ack packets.

bundle

Syntax **bundle [detail]**
no bundle

Context debug>router>rsvp>packet

Description This command debugs bundle packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about RSVP-TE bundle 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.

srefresh

Syntax srefresh [detail]
no srefresh

Context debug>router>rsvp>packet

Description This command debugs srefresh packets.

The **no** form of the command disables the debugging.

Parameters **detail —** Displays detailed information about RSVP-TE srefresh 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

NOTE: 7210 SAS-K 2F4T6C supports only TLDP for the purposes of exchanging the service labels. It does not support link LDP. The following sections explain the generic LDP behavior. It does not imply that link LDP is supported on 7210 SAS-K2F4T6C.

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 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 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 9. 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.

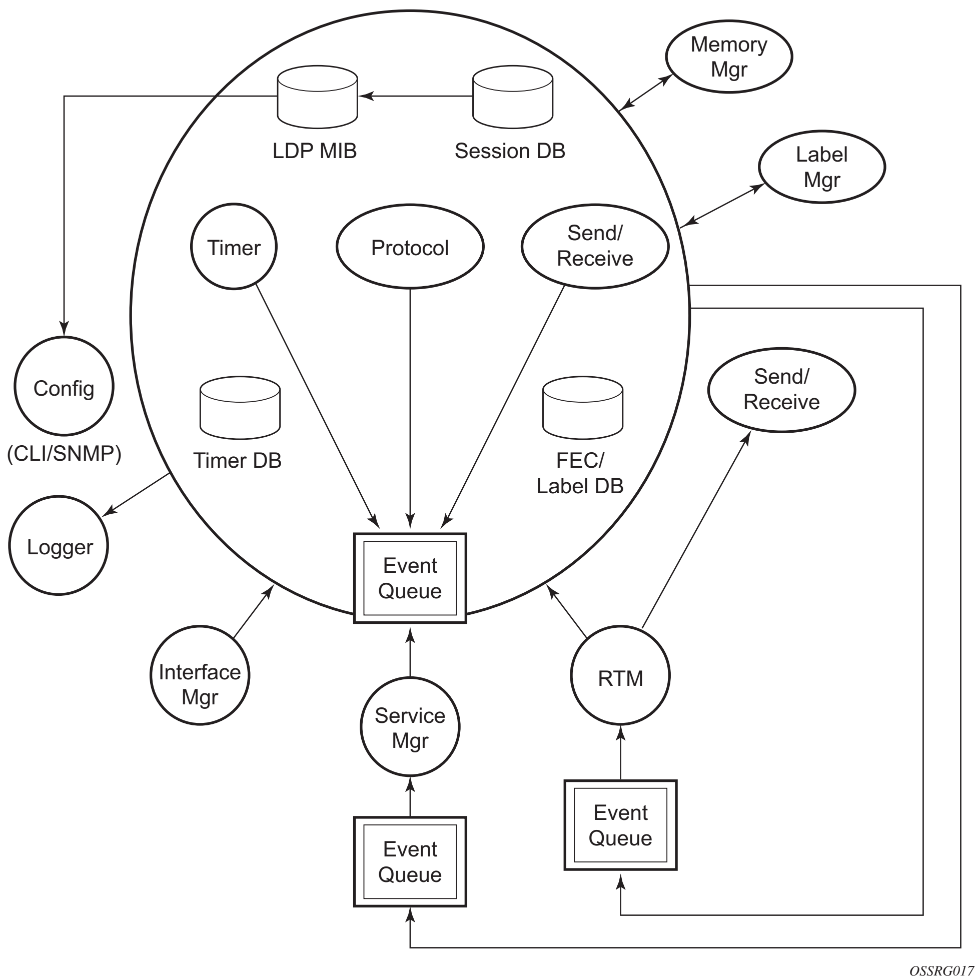


Figure 9: Subsystem Interrelationships

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 7210 devices 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 7210 devices 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 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 router, the adjacency management is done through the establishment of a Service Distribution Path (SDP) object, which is a service entity in the Nokia service model. The Nokia 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 the local routers
- Service Distribution Points (SDPs) that connect to one or more remote routers.

An SDP is the network-side termination point for a tunnel to a remote 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, MPLS
- 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 unidirectional 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 keep-alive 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.

Configuring Implicit Null Label

The implicit null label option allows an egress LER to receive MPLS packets from the previous hop without the outer LSP label. The user can configure to signal the implicit 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.

Enable the use of 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 re-advertises them using the new label value.

Global

Outbound filtering is performed by way of the configuration of an export policy. The Global LDP export policy can be used to explicitly originate label bindings for local interfaces. The Global LDP export policy does not filter out or stop propagation of any FEC received from neighbors. Use the LDP peer export prefix policy for this purpose.

The system IP address AND static FECs cannot be blocked using an export policy.

ed. Finally, the 'neighbor interface' statement inside a global import policy is not considered by LDP.

Per LDP Peer FEC Import and Export Policies

The FEC prefix export policy provides a way to control which FEC prefixes received from prefixes received from other LDP and T-LDP peers are re-distributed to this LDP peer.

The user configures the FEC prefix export policy using the following command:

config>router>ldp>session-params>peer>export-prefixes policy-name

By default, all FEC prefixes are exported to this peer.

The FEC prefix import policy provides a mean of controlling which FEC prefixes received from this LDP peer are imported and installed by LDP on this node. If resolved these FEC prefixes are then re-distributed to other LDP and T-LDP peers.

The user configures the FEC prefix export policy using the following command:

config>router>ldp>session-params>peer>import-prefixes policy-name

By default, all FEC prefixes are imported from this peer.

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).

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.

LDP Fast-Reroute for IS-IS and OSPF Prefixes

LDP Fast Re-Route (FRR) is a feature which allows the user to provide local protection for an LDP FEC by pre-computing and downloading to IOM both a primary and a backup NHLFE for this FEC.

The primary NHLFE corresponds to the label of the FEC received from the primary next-hop as per standard LDP resolution of the FEC prefix in RTM. The backup NHLFE corresponds to the label received for the same FEC from a Loop-Free Alternate (LFA) next-hop.

The LFA next-hop pre-computation by IGP is described in RFC 5286 – “Basic Specification for IP Fast Reroute: Loop-Free Alternates”. LDP FRR relies on using the label-FEC binding received from the LFA next-hop to forward traffic for a given prefix as soon as the primary next-hop is not available. This means that a node resumes forwarding LDP packets to a destination prefix without waiting for the routing convergence. The label-FEC binding is received from the loop-free alternate next-hop ahead of time and is stored in the Label Information Base since LDP on the router operates in the liberal retention mode.

This feature requires that IGP performs the Shortest Path First (SPF) computation of an LFA next-hop, in addition to the primary next-hop, for all prefixes used by LDP to resolve FECs. IGP also populates both routes in the Routing Table Manager (RTM).

LDP FRR Configuration

The user enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS or OSPF routing protocol level:

config>**router**>**isis**>**loopfree-alternate**
config>**router**>**ospf**>**loopfree-alternate**.

The above commands instruct the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. When found, the LFA next-hop is populated into the RTM along with the primary next-hop for the prefix.

Next the user enables the use by LDP of the LFA next-hop by configuring the following option:

config>**router**>**ldp**>**fast-reroute**

When this command is enabled, LDP will use both the primary next-hop and LFA next-hop, when available, for resolving the next-hop of an LDP FEC against the corresponding prefix in the RTM. This will result in LDP programming a primary NHLFE and a backup NHLFE into the IOMXCM for each next-hop of a FEC prefix for the purpose of forwarding packets over the LDP FEC.

Note that because LDP can detect the loss of a neighbor/next-hop independently, it is possible that it switches to the LFA next-hop while IGP is still using the primary next-hop. In order to avoid this situation, it is recommended to enable IGP-LDP synchronization on the LDP interface:

config>**router**>**interface**>**ldp-sync-timer** *seconds*

Reducing the Scope of the LFA Calculation by SPF

The user can instruct IGP to not include all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

config>**router**>**isis**>**level**>**loopfree-alternate-exclude**
config>**router**>**ospf**>**area**>**loopfree-alternate-exclude**

Note that if IGP shortcut are also enabled in LFA SPF, LSPs with destination address in that IS-IS level or OSPF area are also not included in the LFA SPF calculation.

The user can also exclude a specific IP interface from being included in the LFA SPF computation by IS-IS or OSPF:

config>**router**>**isis**>**interface**> **loopfree-alternate-exclude**
config>**router**>**ospf**>**area**>**interface**> **loopfree-alternate-exclude**

Note that when an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When the user excludes an interface from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

LDP FRR Procedures

The LDP FEC resolution when LDP FRR is not enabled operates as follows. When LDP receives a *FEC, label* binding for a prefix, it will resolve it by checking if the exact prefix, or a longest match prefix when the **aggregate-prefix-match option** is enabled in LDP, exists in the routing table and is resolved against a next-hop which is an address belonging to the LDP peer which advertized the binding, as identified by its LSR-id. When the next-hop is no longer available, LDP de-activates the FEC and de-programs the NHLFE in the data path. LDP will also immediately withdraw the labels it advertised for this FEC and deletes the ILM in the data path unless the user configured the **label-withdrawal-delay** option to delay this operation. Traffic that is received while the ILM is still in the data path is dropped. When routing computes and populates the routing table with a new next-hop for the prefix, LDP resolves again the FEC and programs the data path accordingly.

When LDP FRR is enabled and an LFA backup next-hop exists for the FEC prefix in RTM, or for the longest prefix the FEC prefix matches to when **aggregate-prefix-match** option is enabled in LDP, LDP will resolve the FEC as above but will program the data path with both a primary NHLFE and a backup NHLFE for each next-hop of the FEC.

In order perform a switchover to the backup NHLFE in the fast path, LDP follows the uniform FRR failover procedures which are also supported with RSVP FRR.

When any of the following events occurs, LDP instructs in the fast path the IOM to enable the backup NHLFE for each FEC next-hop impacted by this event. The IOM do that by simply flipping a single state bit associated with the failed interface or neighbor/next-hop:

1. An LDP interface goes operationally down, or is admin shutdown. In this case, LDP sends a neighbor/next-hop down message to the IOM for each LDP peer it has adjacency with over this interface.
2. An LDP session to a peer went down as the result of the Hello or Keep-Alive timer expiring over a specific interface. In this case, LDP sends a neighbor/next-hop down message to the IOM for this LDP peer only.
3. The TCP connection used by a link LDP session to a peer went down, due say to next-hop tracking of the LDP transport address in RTM, which brings down the LDP session. In this case, LDP sends a neighbor/next-hop down message to the IOM for this LDP peer only.
4. A BFD session, enabled on a T-LDP session to a peer, times-out and as a result the link LDP session to the same peer and which uses the same TCP connection as the T-LDP session goes also down. In this case, LDP sends a neighbor/next-hop down message to the IOM for this LDP peer only.
5. A BFD session enabled on the LDP interface to a directly connected peer, times-out and brings down the link LDP session to this peer. In this case, LDP sends a neighbor/next-hop down message to the IOM for this LDP peer only. BFD support on LDP interfaces is a

new feature introduced for faster tracking of link LDP peers. See Section 1.2.1 for more details.

The tunnel-down-dump-time option or the label-withdrawal-delay option, when enabled, does not cause the corresponding timer to be activated for a FEC as long as a backup NHLFE is still available.

Link LDP Hello Adjacency Tracking with BFD

LDP can only track an LDP peer with which it established a link LDP session with using the Hello and Keep-Alive timers. If an IGP protocol registered with BFD on an IP interface to track a neighbor, and the BFD session times out, the next-hop for prefixes advertised by the neighbor are no longer resolved. This however does not bring down the link LDP session to the peer since the LDP peer is not directly tracked by BFD. More importantly the LSR-id of the LDP peer may not coincide with the neighbor's router-id IGP is tracking by way of BFD.

In order to properly track the link LDP peer, LDP needs to track the Hello adjacency to its peer by registering with BFD. This way, the peer next-hop is tracked.

The user enables Hello adjacency tracking with BFD by enabling BFD on an LDP interface:

config>**router**>**ldp**>**interface-parameters**>**interface>bfd-enable**

The parameters used for the BFD session, i.e., transmit-interval, receive-interval, and multiplier, are those configured under the IP interface in existing implementation:

config>**router**>**interface**>**bfd**

When multiple links exist to the same LDP peer, a Hello adjacency is established over each link but only a single LDP session will exist to the peer and will use a TCP connection over one of the link interfaces. Also, a separate BFD session should be enabled on each LDP interface. If a BFD session times out on a specific link, LDP will immediately bring down the Hello adjacency on that link. In addition, if the there are FECs which have their primary NHLFE over this link, LDP triggers the LDP FRR procedures by sending to IOM the neighbor/next-hop down message. This will result in moving the traffic of the impacted FECs to an LFA next-hop on a different link to the same LDP peer or to an LFA backup next-hop on a different LDP peer depending on the lowest backup cost path selected by the IGP SPF.

As soon as the last Hello adjacency goes down due to BFD timing out, the LDP session goes down and the LDP FRR procedures will be triggered. This will result in moving the traffic to an LFA backup next-hop on a different LDP peer.

LDP FRR and RSVP Shortcut (IGP Shortcut)

When an RSVP LSP is used as a shortcut by IGP, it is included by SPF as a P2P link and can also be optionally advertised into the rest of the network by IGP. Thus the SPF is able of using a tunneled next-hop as the primary next-hop for a given prefix. LDP is also able of resolving a FEC to a tunneled next-hop when the IGP shortcut feature is enabled.

NOTE: Use of RSVP shortcut is supported only with LDR FRR LFA. It is not supported in the main SFP.

When both IGP shortcut and LFA are enabled in IS-IS or OSPF, and LDP FRR is also enabled, then the following additional LDP FRR capabilities are supported:

1. A FEC which is resolved to a direct primary next-hop can be backed up by a LFA tunneled next-hop.
2. A FEC which is resolved to a tunneled primary next-hop will not have an LFA next-hop. It will rely on RSVP FRR for protection.

The LFA SPF is extended to use IGP shortcuts as LFA next-hops as explained inIS-IS and OSPF Support for Loop-Free Alternate Calculation on page 166.

IS-IS and OSPF Support for Loop-Free Alternate Calculation

SPF computation in IS-IS and OSPF is enhanced to compute LFA alternate routes for each learned prefix and populate it in RTM.

Figure 10 illustrates a simple network topology with point-to-point (P2P) interfaces and highlights three routes to reach router R5 from router R1.

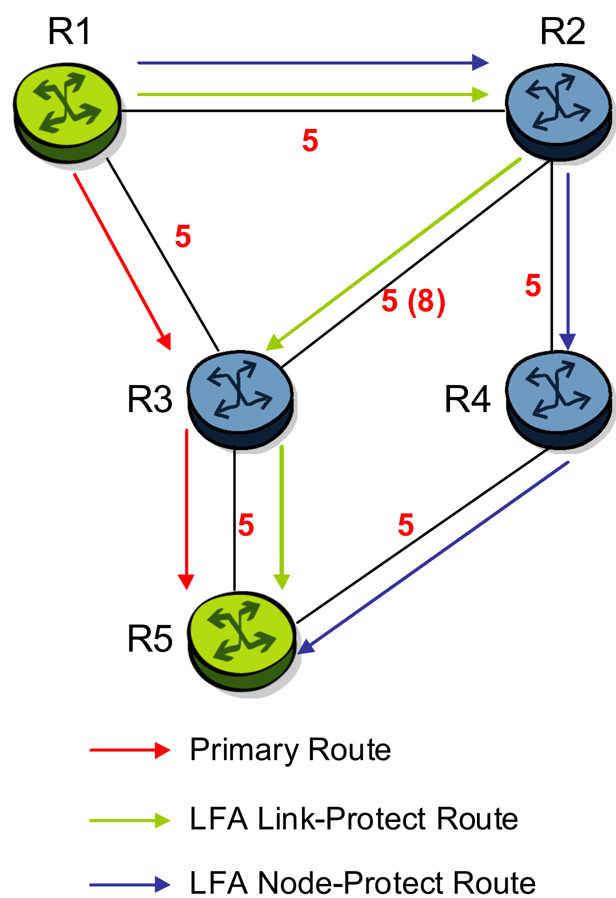


Figure 10: Topology with Primary and LFA Routes

The primary route is by way of R3. The LFA route by way of R2 has two equal cost paths to reach R5. The path by way of R3 protects against failure of link R1-R3. This route is computed by R1 by checking that the cost for R2 to reach R5 by way of R3 is lower than the cost by way of routes R1 and R3. This condition is referred to as the *loop-free criterion*. R2 must be loop-free with respect to source node R1.

The path by way of R2 and R4 can be used to protect against the failure of router R3. However, with the link R2-R3 metric set to 5, R2 sees the same cost to forward a packet to R5 by way of R3 and R4. Thus R1 cannot guarantee that enabling the LFA next-hop R2 will protect against R3 node failure. This means that the LFA next-hop R2 provides link-protection only for prefix R5. If the metric of link R2-R3 is changed to 8, then the LFA next-hop R2 provides node protection since a packet to R5 will always go over R4. In other words it is required that R2 becomes loop-free with respect to both the source node R1 and the protected node R3.

Consider the case where the primary next-hop uses a broadcast interface as illustrated in Figure 11

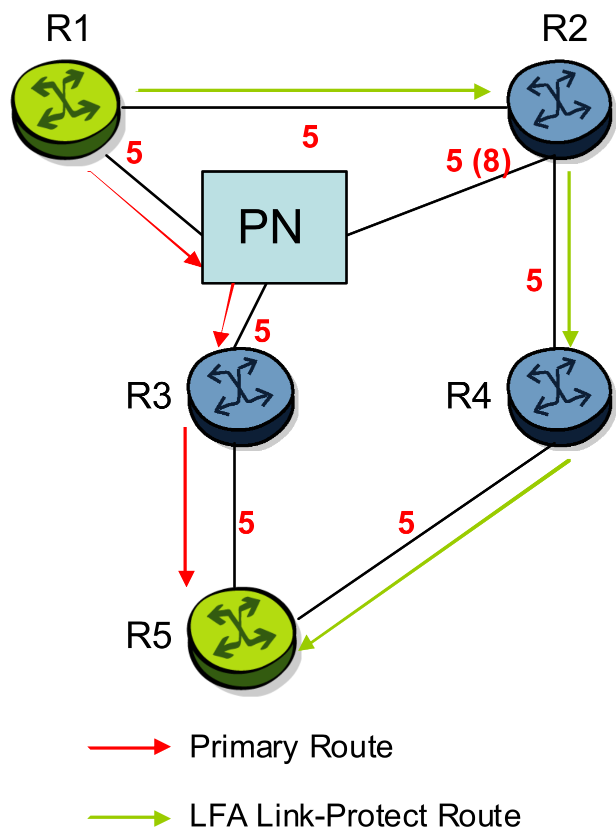


Figure 11: Example Topology with Broadcast Interfaces

In order for next-hop R2 to be a link-protect LFA for route R5 from R1, it must be loop-free with respect to the R1-R3 link's Pseudo-Node (PN). However, since R2 has also a link to that PN, its cost to reach R5 by way of the PN or router R4 are the same. Thus R1 cannot guarantee that enabling the LFA next-hop R2 will protect against a failure impacting link R1-PN since this may cause the entire subnet represented by the PN to go down. If the metric of link R2-PN is changed to 8, then R2 next-hop will be an LFA providing link protection.

The following are the detailed rules for this criterion as provided in RFC 5286:

- **Rule 1**: Link-protect LFA backup next-hop (primary next-hop R1-R3 is a P2P interface):
  ```
  Distance_opt(R2, R5) < Distance_opt(R2, R1) + Distance_opt(R1, R5)
  and,
  Distance_opt(R2, R5) >= Distance_opt(R2, R3) + Distance_opt(R3, R5)
  ```
- **Rule 2**: Node-protect LFA backup next-hop (primary next-hop R1-R3 is a P2P interface):
  ```
  Distance_opt(R2, R5) < Distance_opt(R2, R1) + Distance_opt(R1, R5)
  and,
  Distance_opt(R2, R5) < Distance_opt(R2, R3) + Distance_opt(R3, R5)
  ```

- **Rule 3**: Link-protect LFA backup next-hop (primary next-hop R1-R3 is a broadcast interface):
  `Distance_opt(R2, R5) < Distance_opt(R2, R1) + Distance_opt(R1, R5)`
  `and,`
  `Distance_opt(R2, R5) < Distance_opt(R2, PN) + Distance_opt(PN, R5)`
  where; PN stands for the R1-R3 link Pseudo-Node.

For the case of P2P interface, if SPF finds multiple LFA next-hops for a given primary next-hop, it follows the following selection algorithm:

A) It will pick the node-protect type in favor of the link-protect type.

B) If there is more than one LFA next-hop within the selected type, then it will pick one based on the least cost.

C) If more than one LFA next-hop with the same cost results from Step B, then SPF will select the first one. This is not a deterministic selection and will vary following each SPF calculation.

For the case of a broadcast interface, a node-protect LFA is not necessarily a link protect LFA if the path to the LFA next-hop goes over the same PN as the primary next-hop. Similarly, a link protect LFA may not guarantee link protection if it goes over the same PN as the primary next-hop.

The selection algorithm when SPF finds multiple LFA next-hops for a given primary next-hop is modified as follows:

A) The algorithm splits the LFA next-hops into two sets:
  → The first set consists of LFA next-hops which *do not* go over the PN used by primary next-hop.
  → The second set consists of LFA next-hops which *do* go over the PN used by the primary next-hop.

B) If there is more than one LFA next-hop in the first set, it will pick the node-protect type in favor of the link-protect type.

C) If there is more than one LFA next-hop within the selected type, then it will pick one based on the least cost.

D) If more than one LFA next-hop with equal cost results from Step C, SPF will select the first one from the remaining set. This is not a deterministic selection and will vary following each SPF calculation.

E) If no LFA next-hop results from Step D, SPF will rerun Steps B-D using the second set.

Note this algorithm is more flexible than strictly applying Rule 3 above; the link protect rule in the presence of a PN and specified in RFC 5286. A node-protect LFA which does not avoid the PN;

does not guarantee link protection, can still be selected as a last resort. The same thing, a link-protect LFA which does not avoid the PN may still be selected as a last resort.Both the computed primary next-hop and LFA next-hop for a given prefix are programmed into RTM.

Loop-Free Alternate Calculation in the Presence of IGP shortcuts

In order to expand the coverage of the LFA backup protection in a network, RSVP LSP based IGP shortcuts can be placed selectively in parts of the network and be used as an LFA backup next-hop.

When IGP shortcut is enabled in IS-IS or OSPF on a given node, all RSVP LSP originating on this node and with a destination address matching the router-id of any other node in the network are included in the main SPF by default. Use of RSVP tunnel as an IGP shortcut in the main SFP is not supported on 7210 SAS-K 2F4T6C.

In order to limit the time it takes to compute the LFA SPF, the user must explicitly enable the use of an IGP shortcut as LFA backup next-hop using one of a couple of new optional argument for the existing LSP level IGP shortcut command:

config>**router**>**mpls**>**lsp**>**igp-shortcut** [**lfa-protect** | **lfa-only**]

The **lfa-protect** option allows an LSP to be included in both the main SPF and the LFA SPFs. For a given prefix, the LSP can be used either as a primary next-hop or as an LFA next-hop but not both. If the main SPF computation selected a tunneled primary next-hop for a prefix, the LFA SPF will not select an LFA next-hop for this prefix and the protection of this prefix will rely on the RSVP LSP FRR protection. If the main SPF computation selected a direct primary next-hop, then the LFA SPF will select an LFA next-hop for this prefix but will prefer a direct LFA next-hop over a tunneled LFA next-hop.

NOTE: The lfa-protect option is not supported on 7210 SAS-K 2F4T6C. It is described here for clarity and completeness.

The **lfa-only** option allows an LSP to be included in the LFA SPFs only such that the introduction of IGP shortcuts does not impact the main SPF decision. For a given prefix, the main SPF always selects a direct primary next-hop. The LFA SPF will select a an LFA next-hop for this prefix but will prefer a direct LFA next-hop over a tunneled LFA next-hop. Only this option is supported on 7210 SAS-K 2F4T6C to improve coverage.

Thus the selection algorithm in Section 1.3 when SPF finds multiple LFA next-hops for a given primary next-hop is modified as follows:

A) The algorithm splits the LFA next-hops into two sets:
   - → the first set consists of direct LFA next-hops
   - → the second set consists of tunneled LFA next-hops. after excluding the LSPs which use the same outgoing interface as the primary next-hop.

B) The algorithms continues with first set if not empty, otherwise it continues with second set.

C) If the second set is used, the algorithm selects the tunneled LFA next-hop which endpoint corresponds to the node advertising the prefix.

→ If more than one tunneled next-hop exists, it selects the one with the lowest LSP metric.

→ If still more than one tunneled next-hop exists, it selects the one with the lowest tunnel-id.

→ If none is available, it continues with rest of the tunneled LFAs in second set.

D) Within the selected set, the algorithm splits the LFA next-hops into two sets:

→ The first set consists of LFA next-hops which do not go over the PN used by primary next-hop.

→ The second set consists of LFA next-hops which go over the PN used by the primary next-hop.

E) If there is more than one LFA next-hop in the selected set, it will pick the node-protect type in favor of the link-protect type.

F) If there is more than one LFA next-hop within the selected type, then it will pick one based on the least total cost for the prefix. For a tunneled next-hop, it means the LSP metric plus the cost of the LSP endpoint to the destination of the prefix.

G) If there is more than one LFA next-hop within the selected type (ecmp-case) in the first set, it will select the first direct next-hop from the remaining set. This is not a deterministic selection and will vary following each SPF calculation.

H) If there is more than one LFA next-hop within the selected type (ecmp-case) in the second set, it will pick the tunneled next-hop with the lowest cost from the endpoint of the LSP to the destination prefix. If there remains more than one, it will pick the tunneled next-hop with the lowest tunnel-id.

Loop-Free Alternate Shortest Path First (LFA SPF) Policies

An LFA SPF policy allows the user to apply specific criteria, such as admin group and SRLG constraints, to the selection of a LFA backup next-hop for a subset of prefixes that resolve to a specific primary next-hop. See more details in the section titled *“Loop-Free Alternate Shortest Path First (LFA SPF) Policies”* in the *Routing Protocols Guide*.

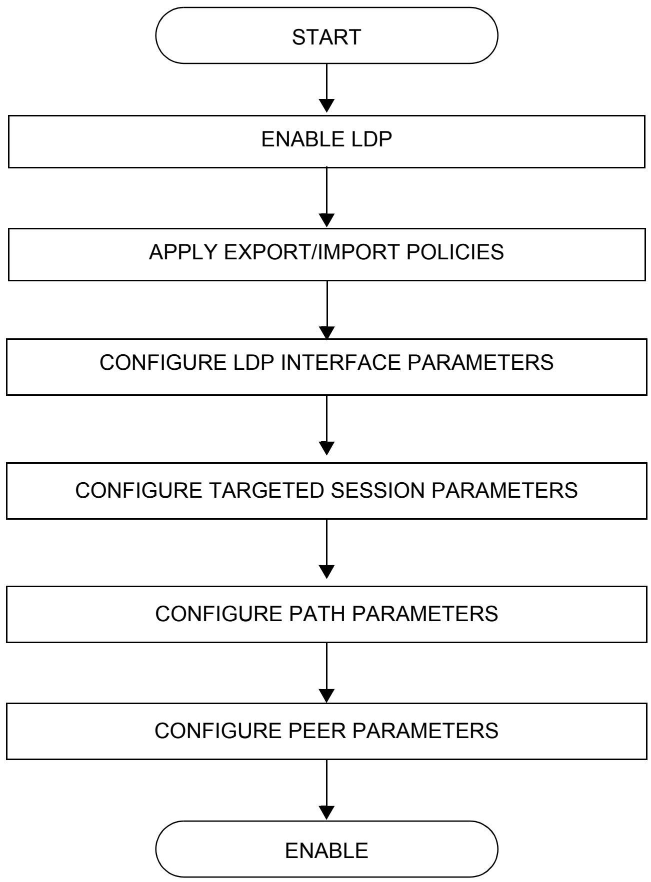
Multi-Area and Multi-Instance Extensions to LDP

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 the /32 prefixes of PEs be leaked between the areas or instances. This is because an exact match of the prefix in the routing table has to install the prefix binding in the LDP Forwarding Information Base (FIB).

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). The ABR is 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 Process Overview

Figure 12 displays the process to provision basic LDP parameters.



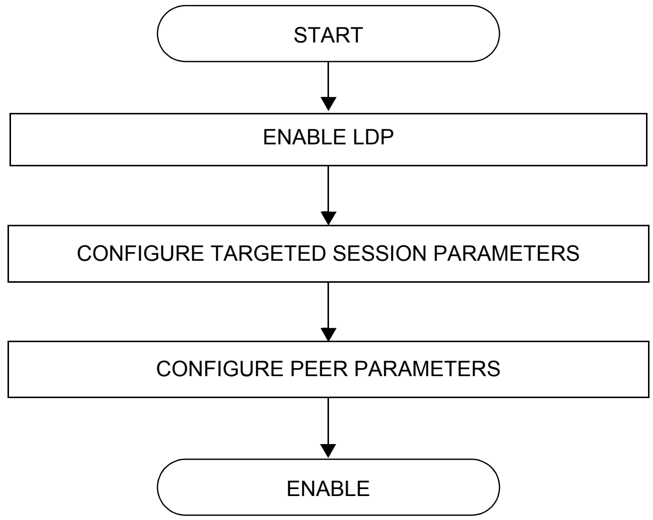


Figure 12: LDP Configuration and Implementation

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 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*.

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.

Common Configuration Tasks

This section provides information to configure:

- Enabling LDP on page 178
- Targeted Session Parameters on page 181
- Peer Parameters on page 199

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 router:

CLI Syntax: `ldp`

Example: `config>router#` **`ldp`**

The following displays the enabled LDP configuration.

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. Nokia'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
       [no] maximum-recovery-time interval
       [no] neighbor-liveness-time interval
```

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.

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)]
```

Targeted Session Parameters

Use the following syntax to specify **targeted-session** parameters:

CLI Syntax:
```
config>router# ldp
  targeted-session
     disable-targeted-session
     hello timeout factor
     keepalive timeout factor
     peer ip-address
        no bfd-enable
        hello timeout factor
        keepalive timeout factor
        no shutdown
```

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:ALU_SIM11>config>router>ldp# info
----------------------------------------------
     aggregate-prefix-match
          prefix-exclude "sample"
          exit
     graceful-restart
          exit
     session-parameters
     peer 1.1.1.1
               ttl-security 1
          exit
     exit
     interface-parameters
               interface "a"
          exit
     exit
     targeted-session
     exit
----------------------------------------------
```

Session Parameters

Use the following syntax to specify session parameters:

CLI Syntax:
```
config>router# ldp
    session-parameters
        peer ip-address
            auth-keychain name
            authentication-key [authentication-key|hash-key]
            [hash|hash2]
```

```
A:ALA-1>config>router>ldp# info
----------------------------------------------
     session-parameters
          peer 10.10.10.104
          authentication-key "3WErEDozxyQ" hash
          exit
     exit
     targeted-session
          hello 5000 255
          keepalive 5000 255
          peer 10.10.10.104
     no bfd-enable
          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 following example displays the command syntax usage to configure enable LDP on an MPLS SDP:

CLI Syntax: `config>service>sdp#`
`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
            lsp A_D_1
            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#
```

LDP Configuration Management Tasks

This section discusses the following LDP configuration management tasks:

- Disabling LDP on page 185
- Modifying Targeted Session Parameters on page 186

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

The modification of LDP targeted session parameters does not take effect until the next time the session goes down and is re-establishes. 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

The modification of LDP targeted session parameters does not take effect until the next time the session goes down and is re-establishes. 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:

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**
    - — **export** *policy-name* [*policy-name*...(up to 5 max)]
    - — **no export**
    - — **fast-reroute**
    - — **no fast-reroute**
    - — **fec-originate** *ip-prefix/mask* [**advertised-label** *in-label*] [**swap-label** *out-label*] **interface interface-name**
    - — **fec-originate** *ip-prefix/mask* [**advertised-label** *i in-label*] **next-hop** *ip-address* [**swap-label** *out-label*]
    - — **fec-originate** *ip-prefix/mask* [**advertised-label** *in-label*] **next-hop** *ip-address* [**swap-label** *out-label*] **interface interface-name**
    - — **fec-originate** *ip-prefix/mask* [**advertised-label** *in-label*] **pop**
    - — **no fec-originate** *ip-prefix/mask* **interface interface-name**
    - — **no fec-originate** *ip-prefix/mask* **next-hop** *ip-address*
    - — **no fec-originate** *ip-prefix/mask* **next-hop** *ip-address* **interface interface-name**
    - — **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*...(up to 5 max)]
    - — **interface-parameters**
      - — [**no**] **interface** *ip-int-name*
        - — **bfd-enable**
        - — **no bfd-enable**
        - — **ipv4**
          - — **fec-type-capability**
            - —**prefix-ipv4** {**enable** | **disable**}
          - — **hello** *timeout factor*
          - — **no hello**
          - — **keepalive** *timeout factor*

— **no keepalive**
— [**no**] **shutdown**
— **transport-address** {**system** | **interface**}
— **label-withdrawal-delay** *seconds*
— **[no] prefer-tunnel-in-tunnel**
— **session-parameters**
— [**no**] **peer** *ip-address*
— [**no**] **export-addresses**
— **export-addresses** *policy-name* [*policy-name* ... (up to 5 max)]
— **no export-addresses**
— **export-prefixes** *policy-name* [*policy-name* ... (up to 5 max)]
— **no export-prefixes**
— **fec-limit** *limit* [**log-only**] [**threshold** *percentage*]
— **no fec-limit**
— **fec-type-capability**
— **prefix-ipv4** {**enable** | **disable**}
— **fec129-cisco-interop** {**enable** | **disable**}
— [**no**] **fec129-cisco-interop**
— **import-prefixes** *policy-name* [*policy-name* ... (up to 5 max)]
— **no import-prefixes**
— [**no**] **shutdown**
— **targeted-session**
— [**no**] **disable-targeted-session**
— **ipv4**
— **hello** *timeout factor*
— **no hello**
— **hello-reduction** {**enable** *factor* | **disable**}
— **no hello-reduction**
— **keepalive** *timeout factor*
— **no keepalive**
— **peer** *ip-address*
— **no peer** *ip-address*
— **bfd-enable**
— **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**

Show Commands

show
— **router**
— **ldp**
— **auth-keychain** [*keychain*]
— **bindings active [fec-type prefixes] [prefix** *ip-prefix/mask*] **[egress-nh i***p-address* | **egress-if** *port-id* | **egress-lsp** *tunnel-id*] **[summary]**
— **bindings active**
— **bindings active prefixes** [*family*] [{**summary** | **detail**}] [**egress-if** *port-id*]
— **bindings active prefixes** [*family*] [{**summary** | **detail**}] [**egress-lsp** *tunnel-id*]

— **bindings active prefixes** [**egress-nh** *ip-address*] [*family*] [{**summary** | **detail**}]
— **bindings active prefixes prefix** *ip-prefix/ip-prefix-length* [{**summary** | **detail**}] [**egress-if** *port-id*]
— **bindings active prefixes prefix** *ip-prefix/ip-prefix-length* [{**summary** | **detail**}] [**egress-lsp** *tunnel-id*]
— **bindings active prefixes prefix** *ip-prefix/ip-prefix-length* [**egress-nh** *ip-address*] [{**summary** | **detail**}]
— **bindings fec-type {prefixes|services} [session** *ip-addr* **4c5]] [su mary| detail]**
— **bindings**[**fec-type** *fec-type* [**detail**]] [**session** *ip-addr*[:*label-space*]]
— **bindings** [*label-type*] [*start-label* [*end-label*]
— **bindings** {**prefix** *ip-prefix/mask* [**detail**]}[**session** *ip-addr*[:*label-space*]]
— **bindings prefixes prefix** *ip-prefix/ip-prefix-length* [{**summary** | **detail**}] [**session** *ip-addr*[:*label-space*]]
— **bindings prefixes** [*family*] [{**summary** | **detail**}] [**session** *ip-addr*[:*label-space*]]
— **bindings active** [**prefix** *ip-prefix/mask*]
— **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**]
— **fec-originate** *ip-prefix/mask* [*operation-type*]
— **fec-originate** [**operation-type**] [**family**]
— [*ip-int-name* | *ip-address*] [**detail**]
— **parameters**
— **session** [*ip-addr*[*label-space*]] [*session-type*] [**state** *state*] [**summary** | **detail**]
— **session** [*ip-addr*[*label-space*]] **local-addresses** [**sent** | **recv**] [**family**]
— **session** [*ip-addr*[*label-space*]][**sent** | **recv**] **overload** [**fec-type** *fec-type*]
— **session** [**sent** | **recv**] **overload** [**fec-type** *fec-type*] [**family**]
— **session** [*ip-addr*[*label-space*]] **statistics** [*packet-type*] [*session-type*]
— **session statistics** [*packet-type*] [*session-type*] [**family**]
— **session** [*session-type*] [**state** *state*] [**summary** | **detail**] [**family**]
— **session-parameters** [*family*]
— **session-parameters** *peer-ip-address*
— **statistics**
— **status**
— **targ-peer** [*ip-address*] [**detail**]
— **targ-peer** [**detail**] *family*
— **targ-peer resource-failures** [*family*]
— **targ-peer-template** [*peer-template*]
— **targ-peer-template-map** [*template-name* [**peers**]]
— **tcp-session-parameters** [*family*]
— **tcp-session-parameters** [**keychain** *keychain*]
— **tcp-session-parameters** [*transport-peer-ip-address*]

Clear Commands

clear
— **router**
— **ldp**
— **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**

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)

shutdown

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

Context config>router>ldp
config>router>ldp>targ-session>peer
config>router>ldp>interface-parameters>interface>ipv4
config>router>ldp>interface-parameters>interface>ipv6
config>router>ldp>interface-parameters>ipv4
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.

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 control 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.

fast-reroute

Syntax **fast-reroute**
no fast-reroute

Context config>router>ldp

Description This command enables LDP Fast-Reroute (FRR) procedures. When enabled, LDP uses both the primary next-hop and LFA next-hop, when available, for resolving the next-hop of an LDP FEC against the corresponding prefix in the routing table. This will result in LDP programming a primary NHLFE and a backup NHLFE into the forwarding engine for each next-hop of a FEC prefix for the purpose of forwarding packets over the LDP FEC.

When any of the following events occurs, LDP instructs in the fast path the forwarding engines to enable the backup NHLFE for each FEC next-hop impacted by this event:

- An LDP interface goes operationally down, or is admin shutdown. In this case, LDP sends a neighbor/next-hop down message to the IOM for each LDP peer it has adjacency with over this interface.
- An LDP session to a peer went down as the result of the Hello or Keep-Alive timer expiring over a specific interface. In this case, LDP sends a neighbor/next-hop down message to the IOM for this LDP peer only.

- The TCP connection used by a link LDP session to a peer went down, due say to next-hop tracking of the LDP transport address in RTM, which brings down the LDP session. In this case, LDP sends a neighbor/next-hop down message to the IOM for this LDP peer only.
- A BFD session, enabled on a T-LDP session to a peer, times-out and as a result the link LDP session to the same peer and which uses the same TCP connection as the T-LDP session goes also down. In this case, LDP sends a neighbor/next-hop down message to the IOM for this LDP peer only.
- A BFD session enabled on the LDP interface to a directly connected peer, times-out and brings down the link LDP session to this peer. In this case, LDP sends a neighbor/nexthop down message to the IOM for this LDP peer only. BFD support on LDP interfaces is a new feature introduced for faster tracking of link LDP peers.

The **tunnel-down-dump-time** option or the **label-withdrawal-delay** option, when enabled, does not cause the corresponding timer to be activated for a FEC as long as a backup NHLFE is still available.

Note that because LDP can detect the loss of a neighbor/next-hop independently, it is possible that it switches to the LFA next-hop while IGP is still using the primary next-hop. Also, when the interface for the previous primary next-hop is restored, IGP may re-converge before LDP completed the FEC exchange with it neighbor over that interface. This may cause LDP to de-program the LFA next-hop from the FEC and blackhole traffic. In order to avoid this situation, it is recommended to enable IGP-LDP synchronization on the LDP interface.

When the SPF computation determines there is more than one primary next-hop for a prefix, it will not program any LFA next-hop in RTM. Thus, the LDP FEC will resolve to the multiple primary next-hops that provide the required protection.

The **no** form of this command disables LDP FRR.

Default no fast-reroute

fec-originate

Syntax

fec-originate *ip-prefix/mask* [**advertised-label** *in-label*] [**swap-label** *out-label*] **interface interface-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*] **next-hop** *ip-address* [**swap-label** *out-label*] **interface interface-name**
fec-originate *ip-prefix/mask* [**advertised-label** *in-label*] **pop**
no fec-originate *ip-prefix/mask* **interface interface-name**
no fec-originate *ip-prefix/mask* **next-hop** *ip-address*
no fec-originate *ip-prefix/mask* **next-hop** *ip-address* **interface interface-name**
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 originate 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.

Values

<ip-address/mask>	ipv4-prefix - a.b.c.d	
	ipv4-prefix-le - [0..32]	
	ipv6-prefix	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x - [0..FFFF]H
		d - [0..255]D
		ipv6-prefix-le - [0..128]

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.

The next-hop, advertised-label, swap-label parameters are all optional. If next-hop is configured but no swap label specified, 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, a pop and route is performed.

Values 16 to 1048575

in-label — Specifies the number of labels to send to the peer associated with this FEC.

Values 32 to 1023

pop — Specifies to pop the label and transmit without the label.

interface *interface-name* **—** Specifies the name of the interface the label for the originated FEC is swapped to. For an unnumbered interface, this parameter is mandatory since there is no address for the next-hop. For a numbered interface, it is optional.

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>graceful-restart

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>graceful-restart

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 label bindings (FECs) are accepted from LDP neighbors. Policies are configured in the **config>router>policy-options** context.

If no import policy is specified, LDP accepts all label bindings 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

keepalive

Syntax **keepalive** *timeout factor*
no keepalive

Context config>router>ldp>interface-parameters>interface>ipv4
config>router>ldp>interface-parameters>ipv4
config>router>ldp>targ-session>ipv4
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 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.

Note that the session needs to be flapped for the new args to operate.

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 3 — 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** 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* — 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.

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.

prefix-ipv4

Syntax **prefix-ipv4** {**enable | disable**}

Context config>router>ldp>interface-params>interface>ipv4>fec-type-capability

Description This command enables and disables IPv4 prefix FEC capability on the interface.

enable — Keyword to enable IPv4FEC capability.

disable — Keyword to disable IPv4FEC capability.

hello

Syntax **hello** *timeout factor*
no hello

Context config>router>ldp>interface-parameters>interface>ipv4
config>router>ldp>interface-parameters>interface>ipv6
config>router>ldp>interface-parameters>ipv4
config>router>ldp>targ-session>ipv4
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.

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 targeted-session level sets the **hello timeout** and the **hello factor** to the default values.

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.

Note that the session needs to be flapped for the new args to operate.

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 3 — 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

hello-reduction

Syntax **hello-reduction** {**enable** *factor* **| disable**}
no hello-reduction

Context config>router>ldp>targ-session>ipv4

Description This command enables the suppression of periodic targeted Hello messages between LDP peers once the targeted LDP session is brought up.

When this feature is enabled, the target Hello adjacency is brought up by advertising the Hold-Time value the user configured in the “hello timeout” parameter for the targeted session. The LSR node will then start advertising an exponentially increasing Hold-Time value in the Hello message as soon as the targeted LDP session to the peer is up. Each new incremented Hold-Time value is sent in a number of Hello messages equal to the value of the argument factor, which represents the dampening factor, before the next exponential value is advertised. This provides time for the two peers to settle on the new value. When the Hold-Time reaches the maximum value of 0xffff (binary 65535), the two peers will send Hello messages at a frequency of every [(65535-1)/local helloFactor] seconds for the lifetime of the targeted-LDP session (for example, if the local Hello Factor is three (3), then Hello messages will be sent every 21844 seconds.

The LSR node continues to compute the frequency of sending the Hello messages based on the minimum of its local Hold-time value and the one advertised by its peer as in RFC 5036. Thus for the targeted LDP session to suppress the periodic Hello messages, both peers must bring their advertised Hold-Time to the maximum value. If one of the LDP peers does not, the frequency of the Hello messages sent by both peers will continue to be governed by the smaller of the two Hold-Time values.

When the user enables the hello reduction option on the LSR node while the targeted LDP session to the peer is operationally up, the change will take effect immediately. In other words, the LSR node will start advertising an exponentially increasing Hold-Time value in the Hello message, starting with the current configured Hold-Time value.

When the user disables the hello reduction option while the targeted LDP session to the peer is operationally up, the change in the Hold-Time from 0xffff (binary 65535) to the user configured value for this peer will take effect immediately. The local LSR will immediately advertise the value of the user configured Hold-Time value and will not wait until the next scheduled time to send a Hello to make sure the peer adjusts its local hold timeout value immediately.

In general, any configuration change to the parameters of the T-LDP Hello adjacency (modifying the hello adjacency Hello Timeout or factor, enabling/disabling hello reduction, or modifying hello reduction factor) will cause the LSR node to trigger immediately an updated Hello message with the updated Hold Time value without waiting for the next scheduled time to send a Hello.

The **no** form of this command disables the hello reduction feature.

Default no hello-reduction

Parameters **disable —** Keyword to disable hello reduction.

factor — Specifies the hello reduction dampening factor.

Values 3 to 20

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.

bfd-enable

Syntax **bfd-enable**
no bfd-enable

Context config>router>ldp>interface-parameters>interface

This command enables tracking of the Hello adjacency to an LDP peer using BFD.

When this command is enabled on an LDP interface, LDP registers with BFD and starts tracking the LSR-id of all peers it formed Hello adjacencies with over that LDP interface. The LDP hello mechanism is used to determine the remote address to be used for the BFD session. The parameters used for the BFD session, that is, transmit-interval, receive-interval, and multiplier are those configured under the IP interface in existing implementation: config>router>interface>bfd

When multiple links exist to the same LDP peer, a Hello adjacency is established over each link and a separate BFD session is enabled on each LDP interface. If a BFD session times out on a specific link, LDP will immediately associate the LDP session with one of the remaining Hello adjacencies and trigger the LDP FRR procedures. As soon as the last Hello adjacency goes down due to BFD timing out, the LDP session goes down and the LDP FRR procedures will be triggered.

NOTE: For more information to know the list of protocols that support BFD, see 7210 SAS Router Configuration Guide.

The no form of this command disables BFD on the LDP interface.

Default no bfd-enable

ipv4

Syntax **ipv4**

Context config>router>ldp>interface-parameters>interface
config>router>ldp>interface-parameters
config>router>ldp>targeted-session

Description This command enables the context to configure IPv4 LDP parameters for the interface.

Default n/a

transport-address

Syntax **transport-address** {**interface** | **system**}
no transport-address

Context config>router>ldp>interface-parameters>interface>ipv4
config>router>ldp>interface-parameters>interface>ipv6
config>router>ldp>interface-parameters>ipv4

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.

Session Parameters Commands

session-parameters

Syntax **session-parameters**

Context config>router>ldp

Description This command enables the context to configure peer-specific parameters.

Default n/a

peer

Syntax [**no**] **peer** *ip-address*

Context config>router>ldp>session-parameters

Description This command configures parameters for an LDP peer.

Default n/a

Parameters *ip-address* — The IP address of the LDP peer in dotted decimal notation.

export-addresses

Syntax **export-addresses** *policy-name* [*policy-name* ... (up to 5 max)]
no export-addresses

Context config>router>ldp>session-params>peer

Description This command specifies the export prefix policy to local addresses advertised to this peer.

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-addresses

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

export-prefixes

Syntax **export-prefixes** *policy-name* [*policy-name* ... (up to 5 max)]
no export-prefixes

Context config>router>ldp>session-params>peer

Description This command specifies the export route policy used to determine which prefixes received from other LDP and T-LDP peers are re-distributed to this LDP peer via the LDP/T-LDP session to this peer. 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 will be exported to this LDP peer. This policy is applied in addition to the global LDP policy and targeted session policy.

Policies are configured in the **config**>**router**>**policy-options** context. A maximum of five policy names can be specified. Peer address has to be the peer LSR-ID address.

The **no** form of the command removes the policy from the configuration.

Default no export-prefixes

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

fec-type-capability

Syntax **fec-type-capability**

Context config>router>ldp>session-params>peer
config>router>ldp>interface-params>interface>ipv4

Description This command enables the context to configure FEC type capabilities for the session or interface.

Default n/a

prefix-ipv4

Syntax **prefix-ipv4** {**enable | disable**}

Context config>router>ldp>session-params>peer>fec-type-capability

Description This command enables or disables IPv4 prefix FEC capability on the session or interface

Default prefix-ipv4 enable

fec129-cisco-interop

Syntax [**no**] **fec129-cisco-interop**

Context config>router>ldp>session-params>peer

Description This command configures whether LDP will provide translation between non-compliant FEC 129 Cisco formats. 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. The FEC129 SAII and TAII fields will be reversed.

The **no** form of the command disables use and support of Cisco non-compliant forms. The peer address must be the peer LSR-ID address.

Default no fec129-cisco-interop

import-prefixes

Syntax **import-prefixes** *policy-name* [*policy-name* ... (up to 5 max)]
no import-prefixes

Context config>router>ldp>session-params>peer

Description This command configures the import FEC prefix policy to determine which prefixes received from this LDP peer are imported and installed by LDP on this node. If resolved, these FEC prefixes are then re-distributed to other LDP and T-LDP peers. 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 import all prefixes received from this LDP/T-LDP peer. This policy is applied in addition to the global LDP policy and targeted session policy. Policies are configured in the **config>router>policy-options** context. A maximum of five policy names can be specified. Peer address has to be the peer LSR-ID address.

The **no** form of the command removes the policy from the configuration.

Default no import-prefixes

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

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

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.

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.

Default **no tunneling**

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 active
bindings active prefixes [*family*] [{**summary | detail**}] [**egress-if** *port-id*]
bindings active prefixes [*family*] [{**summary | detail**}] [**egress-lsp** *tunnel-id*]
bindings active prefixes [**egress-nh** *ip-address*] [*family*] [{**summary | detail**}]
bindings prefix *ip-prefixlip-prefix-length* [{**summary | detail**}] [**egress-if** *port-id*]
bindings prefix *ip-prefixlip-prefix-length* [{**summary | detail**}] [**egress-lsp** *tunnel-id*]
bindings prefix *ip-prefixlip-prefix-length* [**egress-nh** *ip-address*] [{**summary | detail**}]
bindings fec-type {prefixes|services} [session *ip-addr* 4c5]] [summary| detail]
[summary|detail] source *ip-address* **group *mcast-address***
bindings [fec-type *fec-type* [detail]] [session *ip-addr*[:*label-space*]]
bindings [**fec-type** *fec-type* [**detail**]] [**session** *ip-addr*[:*label-space*]]
bindings *label-type start-label* [*end-label*]
bindings {**prefix** *ip-prefix/mask* [detail]} [session *ip-addr*[:*label-space*]]

show>router>ldp **Context**

Description This command displays the contents of the label information base.

Parameters **family —** Specifies the family type.

Values ipv4, ipv6

summary — Displays information in a summarized format.

detail — Displays detailed information.

active-ecmp — Displays the LDP active bindings with ECMP routes that have been successfully installed in the hardware FIB.

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.

ip-prefix-length — Specifies the length of the IP prefix.

label-space — Specifies the label space identifier that the router is advertising on the interface.

Values 0 — 65535

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

ip-address — Specifies the egress IP address.

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

group multicast-address — Displays the P2MP group multicast address bindings.

Values a.b.c.d

service-id — Specifies the service ID number to display.

Values 1 — 2147483647

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 WP: Label Withdraw Pending C: Cpipe service TLV: (Type, Length: Value)

Label	Description
Type	The service type exchanging labels. 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.
SvcID	The unique service identification number identifying the service in the service domain.
Peer	The IP address of the peer.
Op	Label Operation carried out (can be one of pop | swap | push).
EgrNextHop	The nexthop gateway's IP address.
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:7210SAS# show router ldp bindings

===============================================================================
LDP LSR ID: 2.2.2.2
===============================================================================
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
        BU - Alternate Next-hop for Fast Re-Route, TLV - (Type, Length: Value)
===============================================================================
LDP Prefix Bindings
===============================================================================
Prefix              IngLbl       EgrLbl     EgrIntf/         EgrNextHop
   Peer                                     LspId
-------------------------------------------------------------------------------
1.1.1.1/32            --         262143     1/1/3:12         10.11.12.1
   1.1.1.1
1.1.1.1/32          131069U      131069       --               --
   6.6.6.6
2.2.2.2/32          131071U        --         --               --
   1.1.1.1
```

```
2.2.2.2/32          131071U        --         --                --
   6.6.6.6
..........
6.6.6.6/32            --         131071     1/1/9:26         10.11.26.6
   6.6.6.6
-------------------------------------------------------------------------------
No. of Prefix Bindings: 10
===============================================================================

===============================================================================
LDP Generic P2MP Bindings
===============================================================================
P2MP-Id            RootAddr
Interface          Peer            IngLbl    EgrLbl EgrIntf/    EgrNextHop
                                                    LspId
-------------------------------------------------------------------------------
8193               1.1.1.1
73732              1.1.1.1         131065U     --     --           --

8193               2.2.2.2
73728              1.1.1.1           --      262139 1/1/3:12    10.11.12.1

88194               6.6.6.6
73738              6.6.6.6         131054U     --     --           --

8195               6.6.6.6
73739              6.6.6.6         131053U     --     --           --

-------------------------------------------------------------------------------
No. of Generic P2MP Bindings: 13
===============================================================================

===============================================================================
LDP In-Band-SSM P2MP Bindings
===============================================================================
Source
Group
Interface          RootAddr
                   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:7210SAS#



A:7210SAS# show router ldp bindings p2mp-id 8193 root 2.2.2.2 detail

===============================================================================
LDP LSR ID: 2.2.2.2
===============================================================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
        WP - Label Withdraw Pending, BU - Alternate Next-hop for Fast Re-Route
===============================================================================
LDP Generic P2MP Bindings
===============================================================================
-------------------------------------------------------------------------------
P2MP Type          : 1                    P2MP-Id             : 8193
                                          Root-Addr           : 2.2.2.2
-------------------------------------------------------------------------------
Ing Lbl            :   --                 Peer                : 1.1.1.1
Egr Lbl            : 262139
Egr Int/LspId      : 1/1/3:12
EgrNextHop         : 10.11.12.1
Egr. Flags         : None                 Ing. Flags          : None
Metric             : 1                    Mtu                 : 1560
-------------------------------------------------------------------------------
P2MP Type          : 1                    P2MP-Id             : 8193
                                          Root-Addr           : 2.2.2.2
-------------------------------------------------------------------------------
Ing Lbl            :   --                 Peer                : 6.6.6.6
Egr Lbl            : 131059
Egr Int/LspId      : 1/1/9:26
EgrNextHop         : 10.11.26.6
Egr. Flags         : None                 Ing. Flags          : None
Metric             : 1                    Mtu                 : 1560
===============================================================================
No. of Generic P2MP Bindings: 2
===============================================================================
A:7210SAS#
A:7210SAS# show router ldp bindings active fec-type p2mp

===============================================================================
LDP Generic P2MP Bindings (Active)
===============================================================================
P2MP-Id         RootAddr
Interface       Op               IngLbl    EgrLbl EgrIntf/       EgrNextHop
                                                  LspId
-------------------------------------------------------------------------------
8193            1.1.1.1
73731           Pop              131064      --     --              --

8193            1.1.1.1
7
8195            6.6.6.6
73738           Pop              131058      --     --              --

-------------------------------------------------------------------------------
No. of Generic P2MP Active Bindings: 15
===============================================================================
```

```
===============================================================================
LDP In-Band-SSM P2MP Bindings (Active)
===============================================================================
Source
Group
Interface       RootAddr
                Op              IngLbl    EgrLbl EgrIntf/       EgrNextHop
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
A:7210SAS#

A:7210SAS# show router ldp bindings fec-type p2mp detail

===============================================================================
LDP LSR ID: 2.2.2.2
===============================================================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
        WP - Label Withdraw Pending, BU - Alternate Next-hop for Fast Re-Route
===============================================================================
LDP Generic P2MP Bindings
===============================================================================
-------------------------------------------------------------------------------
P2MP Type          : 1                  P2MP-Id            : 8193
                                        Root-Addr          : 1.1.1.1
-------------------------------------------------------------------------------
Ing Lbl            : 131053U            Peer               : 6.6.6.6
Egr Lbl            :   --
Egr Int/LspId      :   --
EgrNextHop         :   --
Egr. Flags         : None               Ing. Flags         : None
===============================================================================
No. of Generic P2MP Bindings: 13
===============================================================================

===============================================================================
LDP In-Band-SSM P2MP Bindings
===============================================================================
No Matching Entries Found
===============================================================================
A:7210SAS#

A:7210SAS# show router ldp bindings p2mp-id 8193 root 2.2.2.2 detail

===============================================================================
LDP LSR ID: 2.2.2.2
===============================================================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
        WP - Label Withdraw Pending, BU - Alternate Next-hop for Fast Re-Route
===============================================================================
LDP Generic P2MP Bindings
===============================================================================
-------------------------------------------------------------------------------
P2MP Type          : 1                  P2MP-Id            : 8193
                                        Root-Addr          : 2.2.2.2
-------------------------------------------------------------------------------
Ing Lbl            :   --               Peer               : 1.1.1.1
Egr Lbl            : 262139
Egr Int/LspId      : 1/1/3:12
```

```
EgrNextHop          : 10.11.12.1
Egr. Flags          : None                  Ing. Flags          : None
Metric              : 1                     Mtu                 : 1560
-------------------------------------------------------------------------------
P2MP Type           : 1                     P2MP-Id             : 8193
                                            Root-Addr           : 2.2.2.2
-------------------------------------------------------------------------------
Ing Lbl             :   --                  Peer                : 6.6.6.6
Egr Lbl             : 131059
Egr Int/LspId       : 1/1/9:26
EgrNextHop          : 10.11.26.6
Egr. Flags          : None                  Ing. Flags          : None
Metric              : 1                     Mtu                 : 1560
===============================================================================
No. of Generic P2MP Bindings: 2
===============================================================================
A:7210SAS#
```

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.

Label	Description (Continued)
`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.

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 to 32

operation-type — Specify the operation type to display.

Values pop, swap

Output FEC Originate Output

Table 46 describes the FEC originate parameters output fields.

Table 3: FEC Originate Output Fields

Label	Description
Prefix	Specifies the static prefix FEC.
NHType	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.
NHIfName	The name 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.
OprInLbl OperIngLabel	Specifies the actual or operational value of the label that was advertised to the upstream peer.

Sample Output

```
A:Dut-C# show router ldp fec-originate 150.1.1.1/32

===============================================================================
LDP IPv4 Static Prefix FECs
===============================================================================
Prefix                  NHType    NextHop             IngLbl    EgrLbl    OprInLbl
 NHIfName
-------------------------------------------------------------------------------
150.1.1.1/32            Pop       n/a                   --        --      131066
    --
-------------------------------------------------------------------------------
No. of IPv4 Static Prefix FECs: 1
====================================================================================
*A:Dut-C>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

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 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#
```

session

Syntax **session [***ip-addr[label-space***] local-addresses [sent|recv] ip-addr** *ip-address*
session [*ip-addr[label-space***] [session-type] [state** *state***] [summary|detail]**
session [*ip-addr[label-space***] local-addresses [sent|recv] [family]**
session [*ip-addr[label-space***] [sent|recv] overload [fec-type** *fec-type***]**
session [sent|recv] overload [fec-type *fec-type***] [family]**
session [*ip-addr[label-space***] statistics [packet-type] [session-type]**
session statistics [packet-type] [session-type] [family]
session [session-type] [state *state***] [summary|detail] [family]**

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.

family — Displays either IPv4 or IPv6 LDP session information.

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#


*7210SAS# show router ldp session detail

===============================================================================
LDP Sessions (Detail)
===============================================================================
Legend:  DoD - Downstream on Demand (for address FEC's only)
         DU  - Downstream Unsolicited
===============================================================================
-------------------------------------------------------------------------------
Session with Peer 2.2.2.2:0, Local 1.1.1.1:0
-------------------------------------------------------------------------------
Adjacency Type    : Both           State                 : Established
Up Time           : 0d 00:07:48
Max PDU Length    : 4096           KA/Hold Time Remaining: 29
Link Adjacencies  : 1              Targeted Adjacencies  : 1
Local Address     : 1.1.1.1        Peer Address          : 2.2.2.2
Local TCP Port    : 646            Peer TCP Port         : 50980
Local KA Timeout  : 30             Peer KA Timeout       : 30
```

```
Mesg Sent          : 478            Mesg Recv              : 480
FECs Sent          : 182            FECs Recv              : 170
Addrs Sent         : 13             Addrs Recv             : 16
GR State           : Capable        Label Distribution     : DU
Nbr Liveness Time : 0               Max Recovery Time      : 0
MP MBB                 : Not Capable
Dynamic Capability: Not Capable
Advertise          : Address/Servi* BFD Operational Status: inService
-------------------------------------------------------------------------------
Session with Peer 3.3.3.3:0, Local 1.1.1.1:0
-------------------------------------------------------------------------------
Adjacency Type     : Both           State                  : Established
Up Time            : 0d 00:07:48
Max PDU Length     : 4096           KA/Hold Time Remaining: 29
Link Adjacencies   : 1              Targeted Adjacencies   : 1
Local Address      : 1.1.1.1        Peer Address           : 3.3.3.3
Local TCP Port     : 646            Peer TCP Port          : 49823
Local KA Timeout   : 30             Peer KA Timeout        : 30
Mesg Sent          : 502            Mesg Recv              : 418
FECs Sent          : 124            FECs Recv              : 124
Addrs Sent         : 13             Addrs Recv             : 5
GR State           : Capable        Label Distribution     : DU
Nbr Liveness Time : 0               Max Recovery Time      : 0
MP MBB                 : Not Capable
Dynamic Capability: Not Capable
Advertise          : Address/Servi* BFD Operational Status: inService
-------------------------------------------------------------------------------
Session with Peer 4.4.4.4:0, Local 1.1.1.1:0
-------------------------------------------------------------------------------
Adjacency Type     : Targeted       State                  : Established
Up Time            : 0d 00:07:47
Max PDU Length     : 4096           KA/Hold Time Remaining: 36
Link Adjacencies   : 0              Targeted Adjacencies   : 1
Local Address      : 1.1.1.1        Peer Address           : 4.4.4.4
Local TCP Port     : 646            Peer TCP Port          : 51307
Local KA Timeout   : 40             Peer KA Timeout        : 40
Mesg Sent          : 122            Mesg Recv              : 124
FECs Sent          : 36             FECs Recv              : 36
Addrs Sent         : 13             Addrs Recv             : 3
GR State           : Capable        Label Distribution     : DU
Nbr Liveness Time : 0               Max Recovery Time      : 0
MP MBB                 : Not Capable
Dynamic Capability: Not Capable
Advertise          : Service        BFD Operational Status: inService
===============================================================================
* indicates that the corresponding row element may have been truncated.
```

session-parameters

Syntax **session-parameters** [*family*]
session-parameters [*peer-ip-address*]

Context show>router>ldp

Description This command displays LDP peer information.

Parameters *family* — Specifies a peer family for which to display information.

Values ipv4, ipv6

ip-address — Specifies the IP address of a targeted LDP peer for which to display information.

ipv4-address — a.b.c.d

Values

ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — [0 to FFFF]H
d — [0 to 255]D

Output

Sample Output

```
===============================================================================
LDP IPv4 Session Parameters
===============================================================================
-------------------------------------------------------------------------------
Peer : 12.12.12.12
-------------------------------------------------------------------------------
DOD                 : Disabled           Adv Adj Addr Only  : Disabled
FEC129 Cisco Inter*: Disabled
PE-ID MAC Flush In*: Disabled
Fec Limit           : 0                  Fec Limit Threshold: 90
Fec Limit Log Only : Disabled
Import Policies     : None               Export Policies    : None
IPv4 Prefix Fec Cap: Enabled             IPv6 Prefix Fec Cap: Disabled
P2MP Fec Cap        : Disabled
Address Export      : None
===============================================================================
No. of IPv4 Peers: 1
===============================================================================
* indicates that the corresponding row element may have been truncated.

===============================================================================
LDP IPv6 Session Parameters
===============================================================================
No Matching Entries Found
===============================================================================
```

statistics

Syntax **statistics**

Context show>router>ldp

Description This command displays LDP statistics information.

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 Adjacen-cies	The number of active adjacencies (established sessions) associated with the LDP instance.
Active Sessions	The number of active sessions (session in some form of creation) associated with the LDP instance.
Active Interfaces	The number of active (operationally up) interfaces associated with the LDP instance.
Inactive Inter-faces	The number of inactive (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.

targ-peer

Syntax **targ-peer** [*ip-address*] [**detail**]
targ-peer [**detail**] *family*
targ-peer resource-failures [*family*]

Context show>router>ldp

Description This command displays targeted LDP peer information.

Parameters **detail —** Keyword to display detailed information.

family — Specifies a peer family for which to display information.

Values ipv4, ipv6

ip-address — Specifies the IP address of a targeted LDP peer for which to display information.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — [0 to FFFF]H
d — [0 to 255]D

resource-failures — Keyword to display resource failure information for targeted LDP peers.

Output

Sample Output

```
===============================================================================
LDP IPv4 Targeted Peers
===============================================================================
Peer                                      Adm/     Hello Hold  KA   KA    Auto
                                          Opr      Fctr  Time  Fctr Time  Created
-------------------------------------------------------------------------------
1.1.1.1                                   Up/Up    3     45    4    40    yes

2.2.2.2                                   Up/Up    3     45    4    40    yes

3.3.3.3                                   Up/Up    3     45    4    40    yes

5.5.5.5                                   Up/Up    3     45    4    40    yes

6.6.6.6                                   Up/Up    3     45    4    40    yes

-------------------------------------------------------------------------------
No. of IPv4 Targeted Peers: 5
===============================================================================

===============================================================================
LDP IPv6 Targeted Peers
===============================================================================
Peer                                      Adm/     Hello Hold  KA   KA    Auto
                                          Opr      Fctr  Time  Fctr Time  Created
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
```

targ-peer-template

Syntax **targ-peer-template** [*peer-template*]

Context show>router>ldp

Description This command displays information about targeted LDP peer templates.

Parameters *peer-template* — Specifies the name of a peer template. 32 characters maximum.

targ-peer-template-map

Syntax **targ-peer-template-map** [*template-name* [**peer**]]

Context show>router>ldp

Description This command displays information about targeted LDP peer template mapping.

Parameters *template-name* — Specifies the name of a template map. 32 characters maximum.

peer — Keyword to display peer information.

tcp-session-parameters

Syntax **tcp-session-parameters** [**family**]
tcp-session-parameters [**keychain** *keychain*]
tcp-session-parameters [*transport-peer-ip-address*]

Context show>router>ldp

Description This command displays information about the TCP transport session of an LDP peer.

Parameters *family* — Specifies a peer family for which to display information.

Values ipv4, ipv6

keychain — Specifies the name of an auth-keychain. 32 characters maximum.

transport-peer-ip-address — Specifies the IP address of a TCP transport peer for which to display information.

Values ipv4-address — a.b.c.d
ipv6-address — x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x — [0 to FFFF]H
d — [0 to 255]D

Clear Commands

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 and other special characters), 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>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>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>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>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

Note: The information presented is subject to change without notice.

Nokia assumes no responsibility for inaccuracies contained herein.

M(A,N) means 7210 SAS-M in both Access-uplink mode and Network mode; Similarly M(N) means 7210 SAS-M in network mode only

T(A,N) means 7210 SAS-M in both Access-uplink mode and Network mode; Similarly T(N) means 7210 SAS-T in network mode only

K5 means 7210 SAS-K 2F2T1C

K12 means 7210 SAS-K 2F4T6C

Sx/S-1/10GE means all variants of 7210 SAS-Sx 1/10GE and 7210 SAS-S 1/10GE platforms

Sx-1/10GE means only the variants of 7210 SAS-Sx 1/10G

R6 means 7210 SAS-R6

R12 means 7210 SAS-R12

D means 7210 SAS-D and 7210 SAS-D ETR; if a line item applies to 7210 SAS-D ETR, then it is indicated as D-ETR

E means 7210 SAS-E

X means 7210 SAS-X

BGP

draft-ietf-idr-add-paths-04, Advertisement of Multiple Paths in BGP is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-sidr-origin-validation-signaling-04, BGP Prefix Origin Validation State Extended Community is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1772, Application of the Border Gateway Protocol in the Internet is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1997, BGP Communities Attribute is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2439, BGP Route Flap Damping is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2858, Multiprotocol Extensions for BGP-4 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2918, Route Refresh Capability for BGP-4 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx-10/100GE, R6, and R12

RFC 3107, Carrying Label Information in BGP-4 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3392, Capabilities Advertisement with BGP-4 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4271, A Border Gateway Protocol 4 (BGP-4) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4360, BGP Extended Communities Attribute is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4456, BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4659, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4724, Graceful Restart Mechanism for BGP (Helper Mode) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4760, Multiprotocol Extensions for BGP-4 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4798, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4893, BGP Support for Four-octet AS Number Space is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5004, Avoid BGP Best Path Transitions from One External to Another is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5291, Outbound Route Filtering Capability for BGP-4 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5668, 4-Octet AS Specific BGP Extended Community is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6811, Prefix Origin Validation is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Circuit Emulation

RFC 4553, Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP) is supported on M(N)

RFC 5086, Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN) is supported on M(N)

RFC 5287, Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks is supported on M(N)

Ethernet

IEEE 802.1AB, Station and Media Access Control Connectivity Discovery is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1ad, Provider Bridges is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, R6, and R12

IEEE 802.1ag, Connectivity Fault Management is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1ah, Provider Backbone Bridges is supported on M(N), X, and T(N)

IEEE 802.1ax, Link Aggregation is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1D, MAC Bridges is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1p, Traffic Class Expediting is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1Q, Virtual LANs is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1s, Multiple Spanning Trees is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1w, Rapid Reconfiguration of Spanning Tree is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.1X, Port Based Network Access Control is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3ab, 1000BASE-T is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3ac, VLAN Tag is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3ad, Link Aggregation is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3ae, 10 Gb/s Ethernet is supported on M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3ah, Ethernet in the First Mile is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3ba, 40 Gb/s and 100 Gb/s Ethernet is supported on R6 and R12

IEEE 802.3i, Ethernet is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3u, Fast Ethernet is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 802.3z, Gigabit Ethernet is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ITU-T G.8032, Ethernet Ring Protection Switching is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ITU-T Y.1731, OAM functions and mechanisms for Ethernet based networks is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, Operational management of Loop Free Alternates is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IP — General

draft-grant-tacacs-02, The TACACS+ Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 768, User Datagram Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 793, Transmission Control Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 854, TELNET Protocol Specifications is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 951, Bootstrap Protocol (BOOTP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1034, Domain Names - Concepts and Facilities is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1035, Domain Names - Implementation and Specification is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1350, The TFTP Protocol (revision 2) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1534, Interoperation between DHCP and BOOTP is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1542, Clarifications and Extensions for the Bootstrap Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2131, Dynamic Host Configuration Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2347, TFTP Option Extension is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2348, TFTP Blocksize Option is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2349, TFTP Timeout Interval and Transfer Size Options is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2428, FTP Extensions for IPv6 and NATs is supported on D, E, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2865, Remote Authentication Dial In User Service (RADIUS) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2866, RADIUS Accounting is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3046, DHCP Relay Agent Information Option (Option 82) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3596, DNS Extensions to Support IP version 6 is supported on D, E, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3768, Virtual Router Redundancy Protocol (VRRP) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4250, The Secure Shell (SSH) Protocol Assigned Numbers is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4251, The Secure Shell (SSH) Protocol Architecture is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4254, The Secure Shell (SSH) Connection Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5880, Bidirectional Forwarding Detection (BFD) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5881, Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5883, Bidirectional Forwarding Detection (BFD) for Multihop Paths is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6528, Defending against Sequence Number Attacks is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IP — Multicast

RFC 1112, Host Extensions for IP Multicasting is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2236, Internet Group Management Protocol, Version 2 is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3376, Internet Group Management Protocol, Version 3 is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3446, Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4604, Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4607, Source-Specific Multicast for IP is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4608, Source-Specific Protocol Independent Multicast in 232/8 is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5059, Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5384, The Protocol Independent Multicast (PIM) Join Attribute Format is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6513, Multicast in MPLS/BGP IP VPNs is supported on T(N), Mxp, R6, and R12

RFC 6514, BGP Encodings and Procedures for Multicast in MPLS/IP VPNs is supported on T(N), Mxp, R6, and R12

RFC 6515, IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs is supported on T(N), Mxp, R6, and R12

RFC 6625, Wildcards in Multicast VPN Auto-Discover Routes is supported on T(N), Mxp, R6, and R12

RFC 6826, Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path is supported on T(N), Mxp, R6, and R12

RFC 7385, IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points is supported on T(N), Mxp, R6, and R12

IP — Version 4

RFC 791, Internet Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 792, Internet Control Message Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 826, An Ethernet Address Resolution Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1812, Requirements for IPv4 Routers is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1981, Path MTU Discovery for IP version 6 is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2401, Security Architecture for Internet Protocol is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IP — Version 6

RFC 2464, Transmission of IPv6 Packets over Ethernet Networks is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3021, Using 31-Bit Prefixes on IPv4 Point-to-Point Links is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3122, Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3587, IPv6 Global Unicast Address Format is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4007, IPv6 Scoped Address Architecture is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4193, Unique Local IPv6 Unicast Addresses is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4291, Internet Protocol Version 6 (IPv6) Addressing Architecture is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4861, Neighbor Discovery for IP version 6 (IPv6) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4862, IPv6 Stateless Address Autoconfiguration (Router Only) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5095, Deprecation of Type 0 Routing Headers in IPv6 is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5952, A Recommendation for IPv6 Address Text Representation is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6106, IPv6 Router Advertisement Options for DNS Configuration is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6164, Using 127-Bit IPv6 Prefixes on Inter-Router Links is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IPsec

RFC 2401, Security Architecture for the Internet Protocol is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2406, IP Encapsulating Security Payload (ESP) is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IS-IS

draft-ietf-isis-mi-02, IS-IS Multi-Instance is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-kaplan-isis-ext-eth-02, Extended Ethernet Frame Size Support is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ISO/IEC 10589:2002, Second Edition, Nov. 2002, Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3359, Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3719, Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3787, Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4971, Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5120, M-ISIS: Multi Topology (MT) Routing in IS-IS is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5130, A Policy Control Mechanism in IS-IS Using Administrative Tags is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5301, Dynamic Hostname Exchange Mechanism for IS-IS is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5302, Domain-wide Prefix Distribution with Two-Level IS-IS is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5303, Three-Way Handshake for IS-IS Point-to-Point Adjacencies is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5304, IS-IS Cryptographic Authentication is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5305, IS-IS Extensions for Traffic Engineering TE is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5306, Restart Signaling for IS-IS (Helper Mode) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5308, Routing IPv6 with IS-IS is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5310, IS-IS Generic Cryptographic Authentication is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6232, Purge Originator Identification TLV for IS-IS is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6233, IS-IS Registry Extension for Purges is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Management

draft-ieft-snmpv3-update-mib-05, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-idr-bgp4-mib-05, Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-isis-wg-mib-06, Management Information Base for Intermediate System to Intermediate System (IS-IS) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-mpls-ldp-mib-07, Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-mpls-lsr-mib-06, Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-mpls-te-mib-04, Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-ospf-mib-update-08, OSPF Version 2 Management Information Base is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ianaaddressfamilynumbers-mib, IANA-ADDRESS-FAMILY-NUMBERS-MIB is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ianaiftype-mib, IANAifType-MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ianaiprouteprotocol-mib, IANA-RTPROTO-MIB is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE8021-CFM-MIB, IEEE P802.1ag(TM) CFM MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE8021-PAE-MIB, IEEE 802.1X MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE8023-LAG-MIB, IEEE 802.3ad MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

LLDP-MIB, IEEE P802.1AB(TM) LLDP MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1157, A Simple Network Management Protocol (SNMP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1215, A Convention for Defining Traps for use with the SNMP is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1724, RIP Version 2 MIB Extension is supported on Mxp

RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2 is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2115, Management Information Base for Frame Relay DTEs Using SMIv2 is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2138, Remote Authentication Dial In User Service (RADIUS) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2206, RSVP Management Information Base using SMIv2 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2213, Integrated Services Management Information Base using SMIv2 is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2494, Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type is supported on M(N)

RFC 2571, An Architecture for Describing SNMP Management Frameworks is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2573, SNMP Applications is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2578, Structure of Management Information Version 2 (SMIv2) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2579, Textual Conventions for SMIv2 is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2819, Remote Network Monitoring Management Information Base is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2856, Textual Conventions for Additional High Capacity Data Types is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2863, The Interfaces Group MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2864, The Inverted Stack Table Extension to the Interfaces Group MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2933, Internet Group Management Protocol MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3014, Notification Log MIB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3164, The BSD syslog Protocol is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3165, Definitions of Managed Objects for the Delegation of Management Scripts is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3231, Definitions of Managed Objects for Scheduling Management Operations is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3273, Remote Network Monitoring Management Information Base for High Capacity Networks is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3416. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3419, Textual Conventions for Transport Addresses is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3593, Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals is supported on K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3635, Definitions of Managed Objects for the Ethernet-like Interface Types is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3877, Alarm Management Information Base (MIB) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3895, Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types is supported on M(N)

RFC 4001, Textual Conventions for Internet Network Addresses is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4022, Management Information Base for the Transmission Control Protocol (TCP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4113, Management Information Base for the User Datagram Protocol (UDP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4220, Traffic Engineering Link Management Information Base is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4292, IP Forwarding Table MIB is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4293, Management Information Base for the Internet Protocol (IP) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6241, Network Configuration Protocol (NETCONF) is supported on K5, K12, R6, and R12

RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH) is supported on K5, K12, R6, and R12

MPLS — General

RFC 3031, Multiprotocol Label Switching Architecture is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3032, MPLS Label Stack Encoding is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3443, Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4182, Removing a Restriction on the use of MPLS Explicit NULL is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5332, MPLS Multicast Encapsulations is supported on T(N), Mxp, R6, and R12

MPLS — GMPLS

draft-ietf-ccamp-rsvp-te-srlg-collect-04, RSVP-TE Extensions for Collecting SRLG Information is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

MPLS — LDP

draft-pdutta-mpls-ldp-adj-capability-00, LDP Adjacency Capabilities is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-pdutta-mpls-ldp-v2-00, LDP Version 2 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-pdutta-mpls-tldp-hello-reduce-04, Targeted LDP Hello Reduction is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3037, LDP Applicability is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3478, Graceful Restart Mechanism for Label Distribution Protocol (Helper Mode) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5036, LDP Specification is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5283, LDP Extension for Inter-Area Label Switched Paths (LSPs) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5443, LDP IGP Synchronization is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5561, LDP Capabilities is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

MPLS — MPLS-TP

RFC 5586, MPLS Generic Associated Channel is supported on T(N), R6, and R12

RFC 5921, A Framework for MPLS in Transport Networks is supported on T(N), R6, and R12

RFC 5960, MPLS Transport Profile Data Plane Architecture is supported on T(N), R6, and R12

RFC 6370, MPLS Transport Profile (MPLS-TP) Identifiers is supported on T(N), R6, and R12

RFC 6378, MPLS Transport Profile (MPLS-TP) Linear Protection is supported on T(N), R6, and R12

RFC 6426, MPLS On-Demand Connectivity and Route Tracing is supported on T(N), R6, and R12

RFC 6428, Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile is supported on T(N), R6, and R12

RFC 6478, Pseudowire Status for Static Pseudowires is supported on T(N), R6, and R12

RFC 7213, MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing is supported on T(N), R6, and R12

MPLS — OAM

RFC 6424, Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6425, Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping is supported on T(N), Mxp, R6, and R12

MPLS — RSVP-TE

RFC 2702, Requirements for Traffic Engineering over MPLS is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2747, RSVP Cryptographic Authentication is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2961, RSVP Refresh Overhead Reduction Extensions is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3097, RSVP Cryptographic Authentication -- Updated Message Type Value is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3477, Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE) is supported on M(N), T(N), X, Mxp, R6, and R12

RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4561, Definition of a Record Route Object (RRO) Node-Id Sub-Object is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4875, Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs) is supported on T(N), Mxp, R6, and R12

RFC 4950, ICMP Extensions for Multiprotocol Label Switching is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5712, MPLS Traffic Engineering Soft Preemption is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5817, Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

OSPF

draft-ietf-ospf-prefix-link-attr-06, OSPFv2 Prefix/Link Attribute Advertisement is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1765, OSPF Database Overflow is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2328, OSPF Version 2 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3509, Alternative Implementations of OSPF Area Border Routers is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3623, Graceful OSPF Restart Graceful OSPF Restart (Helper Mode) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3630, Traffic Engineering (TE) Extensions to OSPF Version 2 is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4222, Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4552, Authentication/Confidentiality for OSPFv3 is supported on M(N), T(N), X, Mxp, R6, and R12

RFC 4576, Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4970, Extensions to OSPF for Advertising Optional Router Capabilities is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5185, OSPF Multi-Area Adjacency is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5187, OSPFv3 Graceful Restart (Helper Mode) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5243, OSPF Database Exchange Summary List Optimization is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5250, The OSPF Opaque LSA Option is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5340, OSPF for IPv6 is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5838, Support of Address Families in OSPFv3 is supported on M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6987, OSPF Stub Router Advertisement is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, OAM Procedures for VPWS Interworking is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3916, Requirements for Pseudo- Wire Emulation Edge-to-Edge (PWE3) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3985, Pseudo Wire Emulation Edge-to-Edge (PWE3) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4385, Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4446, IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5659, An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6073, Segmented Pseudowire is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6310, Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6391, Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network is supported on Mxp, R6, and R12

RFC 6718, Pseudowire Redundancy is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6870, Pseudowire Preferential Forwarding Status bit is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 7023, MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 7267, Dynamic Placement of Multi-Segment Pseudowires is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Quality of Service

RFC 2430, A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 2598, An Expedited Forwarding PHB is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3140, Per Hop Behavior Identification Codes is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 3260, New Terminology and Clarifications for Diffserv is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RIP

RFC 1058, Routing Information Protocol is supported on Mxp

RFC 2082, RIP-2 MD5 Authentication is supported on Mxp

RFC 2453, RIP Version 2 is supported on Mxp

Timing

GR-1244-CORE, Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

GR-253-CORE, SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

IEEE 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx-1/10GE, R6, and R12

ITU-T G.781, Synchronization layer functions, issued 09/2008 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ITU-T G.813, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ITU-T G.8261, Timing and synchronization aspects in packet networks, issued 04/2008 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ITU-T G.8262, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ITU-T G.8264, Distribution of timing information through packet networks, issued 10/2008 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

ITU-T G.8265.1, Precision time protocol telecom profile for frequency synchronization, issued 10/2010 is supported on D-ETR, K5, K12, M(A,N), T(A,N), X, Mxp, Sx-1/10GE, R6, and R12

ITU-T G.8275.1, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014 is supported on X, Mxp, R6, and R12

RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification is supported on D, E, K5, K12, M(A,N), T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

VPLS

RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5501, Requirements for Multicast Support in Virtual Private LAN Services is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 6074, Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs) is supported on K12, M(N), T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

INDEX

Customer Document and Product Support

Customer documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation feedback

Customer Documentation Feedback