

MPLS Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 26.1.x, 26.2.x, 26.3.x

First Published: 2026-02-28

Last Modified: 2026-09-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



Preface

From Release 6.1.2 onwards, Cisco introduces support for the 64-bit Linux-based IOS XR operating system. Extensive feature parity is maintained between the 32-bit and 64-bit environments. Unless explicitly marked otherwise, the contents of this document are applicable for both the environments. For more details on Cisco IOS XR 64 bit, refer to the Release Notes for Cisco ASR 9000 Series Routers, Release 6.1.2 document.

The preface contains these sections:

- Changes to This Document, on page iii
- Communications, Services, and Additional Information, on page iii

Changes to This Document

This table lists the technical changes made to this document since it was first released.

Table 1: Changes to This Document

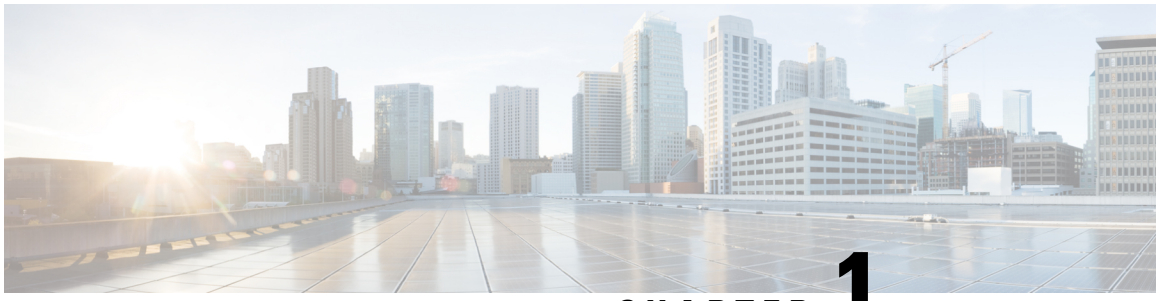
Date	Change Summary
September 2026	Republished for Release 26.3.1
June 2026	Republished for Release 26.2.1
February 2026	Initial release of this document

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

New and Changed MPLS Features

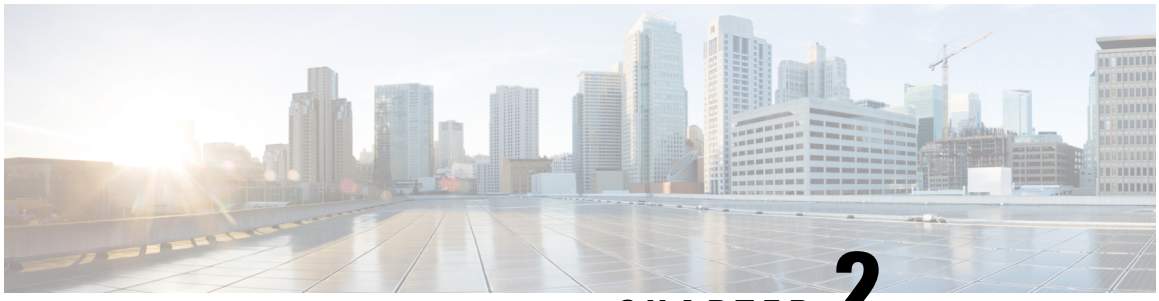
This table summarizes the new and changed feature information for the *Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide* and tells you where they are documented.

- New and Changed MPLS Feature Information, on page 1

New and Changed MPLS Feature Information

Table 2: New and Changed Features

Feature	Description	Changed in Release	Where Documented
Regular expressions in MPLS-TE tunnel names	This feature was introduced	Release 26.2.1	Regular expressions in MPLS-TE tunnel names



CHAPTER 2

YANG Data Models for MPLS Features

This chapter provides information about the YANG data models for MPLS features.

• Using YANG Data Models, on page 3

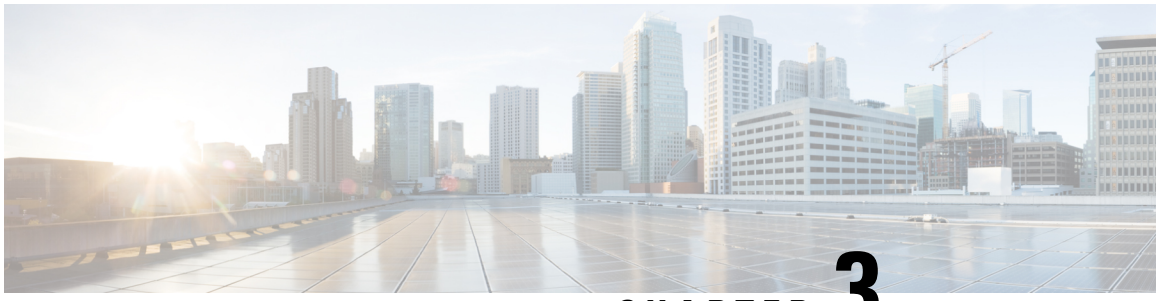
Using YANG Data Models

Cisco IOS XR supports a programmatic way of configuring and collecting operational data of a network device using YANG data models. Although configurations using CLIs are easier and human-readable, automating the configuration using model-driven programmability results in scalability.

The data models are available in the release image, and are also published in the Github repository. Navigate to the release folder of interest to view the list of supported data models and their definitions. Each data model defines a complete and cohesive model, or augments an existing data model with additional XPaths. To view a comprehensive list of the data models supported in a release, navigate to the **Available-Content.md** file in the repository.

You can also view the data model definitions using the YANG Data Models Navigator tool. This GUI-based and easy-to-use tool helps you explore the nuances of the data model and view the dependencies between various containers in the model. You can view the list of models supported across Cisco IOS XR releases and platforms, locate a specific model, view the containers and their respective lists, leaves, and leaf lists presented visually in a tree structure. This visual tree form helps you get insights into nodes that can help you automate your network.

To get started with using the data models, see the *Programmability Configuration Guide*.



CHAPTER 3

Implementing MPLS Label Distribution Protocol

The Multiprotocol Label Switching (MPLS) is a standards-based solution driven by the Internet Engineering Task Force (IETF) that was devised to convert the Internet and IP backbones from best-effort networks into business-class transport mediums.

MPLS, with its label switching capabilities, eliminates the need for an IP route look-up and creates a virtual circuit (VC) switching function, allowing enterprises the same performance on their IP-based network services as with those delivered over traditional networks such as Frame Relay or ATM.

Label Distribution Protocol (LDP) performs label distribution in MPLS environments. LDP provides the following capabilities:

- LDP performs hop-by-hop or dynamic path setup; it does not provide end-to-end switching services.
- LDP assigns labels to routes using the underlying Interior Gateway Protocols (IGP) routing protocols.
- LDP provides constraint-based routing using LDP extensions for traffic engineering.

Finally, LDP is deployed in the core of the network and is one of the key protocols used in MPLS-based Layer 2 and Layer 3 virtual private networks (VPNs).

Feature History for Implementing MPLS LDP

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.0	No modification.
Release 4.0.1	Support was added for these features: • IP LDP Fast Reroute Loop Free Alternate • Downstream on Demand
Release 4.2.1	Support was added for LDP Implicit Null for IGP Routes.
Release 5.1	Support was added for MPLS over IRB.
Release 5.1.1	The feature MPLS LDP Carrier Supporting Carrier for Multiple VRFs was introduced.
Release 5.3.0	IPv6 Support in MPLS LDP was introduced.

Release	Modification
Release 6.0.1	Dual-Stack Capability TLV feature was introduced.
Release 7.0.1	The UDP Decapsulation of MPLS-Over-UDP Traffic feature was introduced.
Release 7.1.1	Multiple MPLS-TE tunnel end points can be enabled on an LER using the TLV 132 function in IS-IS.

- Prerequisites for Implementing Cisco MPLS LDP, on page 6
- Information About Implementing Cisco MPLS LDP, on page 6
- How to Implement MPLS LDP, on page 37
- Configuration Examples for Implementing MPLS LDP, on page 102
- Entropy Label Support for Transit Routers, on page 126
- Additional References, on page 128

Prerequisites for Implementing Cisco MPLS LDP

These prerequisites are required to implement MPLS LDP:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- You must be running Cisco IOS XR software.
- You must install a composite mini-image and the MPLS package.
- You must activate IGP.
- We recommend to use a lower session holdtime bandwidth such as neighbors so that a session down occurs before an adjacency-down on a neighbor. Therefore, the following default values for the hello times are listed:
  - Holdtime is 15 seconds.
  - Interval is 5 seconds.

  For example, the LDP session holdtime can be configured as 30 seconds by using the **holdtime** command.

Information About Implementing Cisco MPLS LDP

To implement MPLS LDP, you should understand these concepts:

Overview of Label Distribution Protocol

LDP performs label distribution in MPLS environments. LDP uses hop-by-hop or dynamic path setup, but does not provide end-to-end switching services. Labels are assigned to routes that are chosen by the underlying IGP routing protocols. The Label Switched Paths (LSPs) that result from the routes, forward labeled traffic across the MPLS backbone to adjacent nodes.

Label Switched Paths

LSPs are created in the network through MPLS. They can be created statically, by RSVP traffic engineering (TE), or by LDP. LSPs created by LDP perform hop-by-hop path setup instead of an end-to-end path.

LDP Control Plane

The control plane enables label switched routers (LSRs) to discover their potential peer routers and to establish LDP sessions with those peers to exchange label binding information.

Related Topics

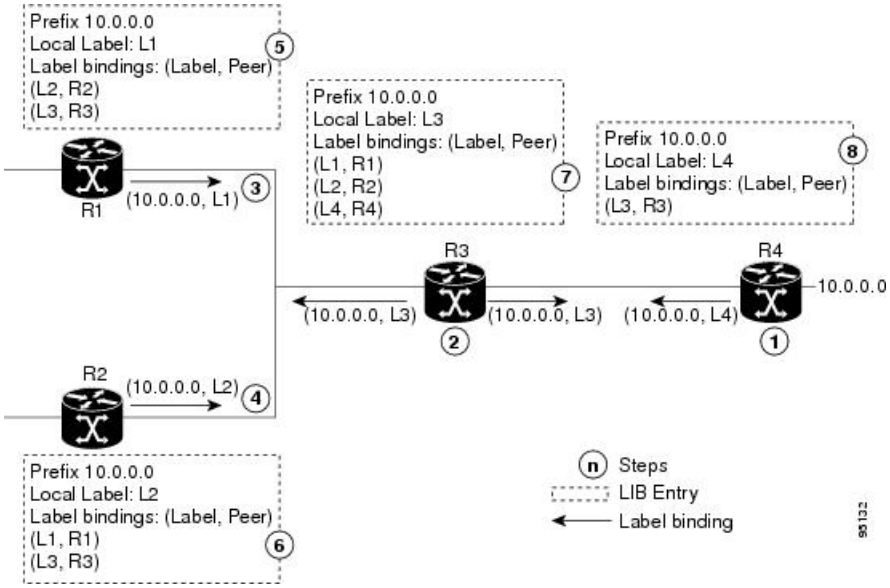
Configuring LDP Discovery Parameters, on page 37
Configuring LDP Discovery Over a Link, on page 40
Configuring LDP Link: Example, on page 102
Configuring LDP Discovery for Active Targeted Hellos, on page 42
Configuring LDP Discovery for Passive Targeted Hellos, on page 44
Configuring LDP Discovery for Targeted Hellos: Example, on page 102

Exchanging Label Bindings

LDP creates LSPs to perform the hop-by-hop path setup so that MPLS packets can be transferred between the nodes on the MPLS network.

Figure 1: Setting Up Label Switched Paths

This figure illustrates the process of label binding exchange for setting up LSPs.



For a given network (10.0.0.0), hop-by-hop LSPs are set up between each of the adjacent routers (or, nodes) and each node allocates a local label and passes it to its neighbor as a binding:

1. R4 allocates local label L4 for prefix 10.0.0.0 and advertises it to its neighbors (R3).
2. R3 allocates local label L3 for prefix 10.0.0.0 and advertises it to its neighbors (R1, R2, R4).
3. R1 allocates local label L1 for prefix 10.0.0.0 and advertises it to its neighbors (R2, R3).

4. R2 allocates local label L2 for prefix 10.0.0.0 and advertises it to its neighbors (R1, R3).
5. R1's label information base (LIB) keeps local and remote labels bindings from its neighbors.
6. R2's LIB keeps local and remote labels bindings from its neighbors.
7. R3's LIB keeps local and remote labels bindings from its neighbors.
8. R4's LIB keeps local and remote labels bindings from its neighbors.

Related Topics

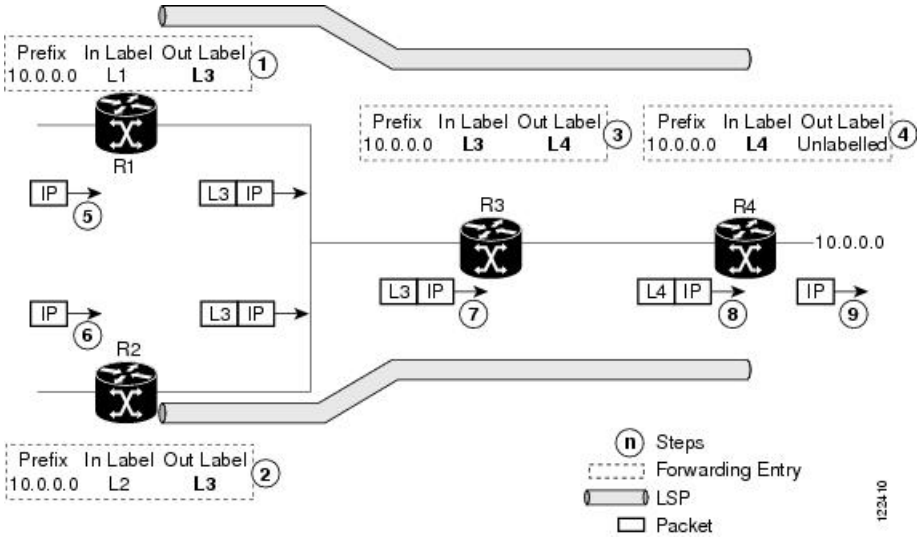
Setting Up LDP Neighbors, on page 47
Configuring LDP Neighbors: Example, on page 104

LDP Forwarding

Once label bindings are learned, the LDP control plane is ready to setup the MPLS forwarding plane as shown in the following figure.

Figure 2: Forwarding Setup

Once label bindings are learned, the LDP control plane is ready to setup the MPLS forwarding plane as shown in this figure.



1. Because R3 is next hop for 10.0.0.0 as notified by the FIB, R1 selects label binding from R3 and installs forwarding entry (label L1, label L3).
2. Because R3 is next hop for 10.0.0.0 (as notified by FIB), R2 selects label binding from R3 and installs forwarding entry (label L2, label L3).
3. Because R4 is next hop for 10.0.0.0 (as notified by FIB), R3 selects label binding from R4 and installs forwarding entry (label L3, label L4).
4. Because next hop for 10.0.0.0 (as notified by FIB) is beyond R4, R4 uses NO-LABEL as the outbound and installs the forwarding entry (label L4); the outbound packet is forwarded IP-only.
5. Incoming IP traffic on ingress LSR R1 gets label-imposed and is forwarded as an MPLS packet with label L3.

6. Incoming IP traffic on ingress LSR R2 gets label-imposed and is forwarded as an MPLS packet with label L3.
7. R3 receives an MPLS packet with label L3, looks up in the MPLS label forwarding table and switches this packet as an MPLS packet with label L4.
8. R4 receives an MPLS packet with label L4, looks up in the MPLS label forwarding table and finds that it should be Unlabeled, pops the top label, and passes it to the IP forwarding plane.
9. IP forwarding takes over and forwards the packet onward.



Note For local labels, only up to 12000 rewrites are supported. If the rewrites exceed this limit, MPLS LSD or MPLS LDP or both the processes may crash.

Related Topics

Setting Up LDP Forwarding, on page 50
Configuring LDP Forwarding: Example, on page 104

LDP Graceful Restart

LDP (Label Distribution Protocol) graceful restart provides a control plane mechanism to ensure high availability and allows detection and recovery from failure conditions while preserving Nonstop Forwarding (NSF) services. Graceful restart is a way to recover from signaling and control plane failures without impacting forwarding.

Without LDP graceful restart, when an established session fails, the corresponding forwarding states are cleaned immediately from the restarting and peer nodes. In this case LDP forwarding restarts from the beginning, causing a potential loss of data and connectivity.

The LDP graceful restart capability is negotiated between two peers during session initialization time, in FT SESSION TLV. In this typed length value (TLV), each peer advertises the following information to its peers:

Reconnect time

Advertises the maximum time that other peer will wait for this LSR to reconnect after control channel failure.

Recovery time

Advertises the maximum time that the other peer has on its side to reinstate or refresh its states with this LSR. This time is used only during session reestablishment after earlier session failure.

FT flag

Specifies whether a restart could restore the preserved (local) node state for this flag.

Once the graceful restart session parameters are conveyed and the session is up and running, graceful restart procedures are activated.

When configuring the LDP graceful restart process in a network with multiple links, targeted LDP hello adjacencies with the same neighbor, or both, make sure that graceful restart is activated on the session before any hello adjacency times out in case of neighbor control plane failures. One way of achieving this is by configuring a lower session hold time between neighbors such that session timeout occurs before hello adjacency timeout. It is recommended to set LDP session hold time using the following formula:

```
Session Holdtime <= (Hello holdtime - Hello interval) * 3
```

This means that for default values of 15 seconds and 5 seconds for link Hello holdtime and interval respectively, session hold time should be set to 30 seconds at most.

For more information about LDP commands, see *MPLS Label Distribution Protocol Commands* module of the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Related Topics

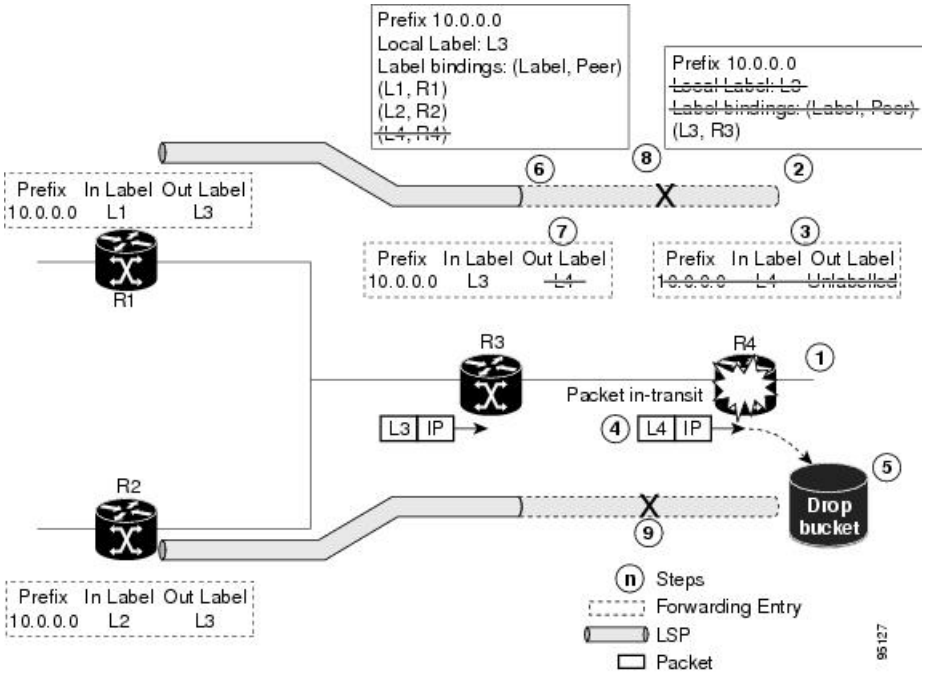
Phases in Graceful Restart, on page 11
Recovery with Graceful-Restart, on page 11
Setting Up LDP NSF Using Graceful Restart, on page 54
Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 104

Control Plane Failure

When a control plane failure occurs, connectivity can be affected. The forwarding states installed by the router control planes are lost, and the in-transit packets could be dropped, thus breaking NSF.

Figure 3: Control Plane Failure

This figure illustrates a control plane failure and shows the process and results of a control plane failure leading to loss of connectivity.



1. The R4 LSR control plane restarts.
2. LIB is lost when the control plane restarts.
3. The forwarding states installed by the R4 LDP control plane are immediately deleted.
4. Any in-transit packets flowing from R3 to R4 (still labeled with L4) arrive at R4.

5. The MPLS forwarding plane at R4 performs a lookup on local label L4 which fails. Because of this failure, the packet is dropped and NSF is not met.
6. The R3 LDP peer detects the failure of the control plane channel and deletes its label bindings from R4.
7. The R3 control plane stops using outgoing labels from R4 and deletes the corresponding forwarding state (rewrites), which in turn causes forwarding disruption.
8. The established LSPs connected to R4 are terminated at R3, resulting in broken end-to-end LSPs from R1 to R4.
9. The established LSPs connected to R4 are terminated at R3, resulting in broken LSPs end-to-end from R2 to R4.

Phases in Graceful Restart

The graceful restart mechanism is divided into different phases:

Control communication failure detection

Control communication failure is detected when the system detects either:

- Missed LDP hello discovery messages
- Missed LDP keepalive protocol messages
- Detection of Transmission Control Protocol (TCP) disconnection a with a peer

Forwarding state maintenance during failure

Persistent forwarding states at each LSR are achieved through persistent storage (checkpoint) by the LDP control plane. While the control plane is in the process of recovering, the forwarding plane keeps the forwarding states, but marks them as stale. Similarly, the peer control plane also keeps (and marks as stale) the installed forwarding rewrites associated with the node that is restarting. The combination of local node forwarding and remote node forwarding plane states ensures NSF and no disruption in the traffic.

Control state recovery

Recovery occurs when the session is reestablished and label bindings are exchanged again. This process allows the peer nodes to synchronize and to refresh stale forwarding states.

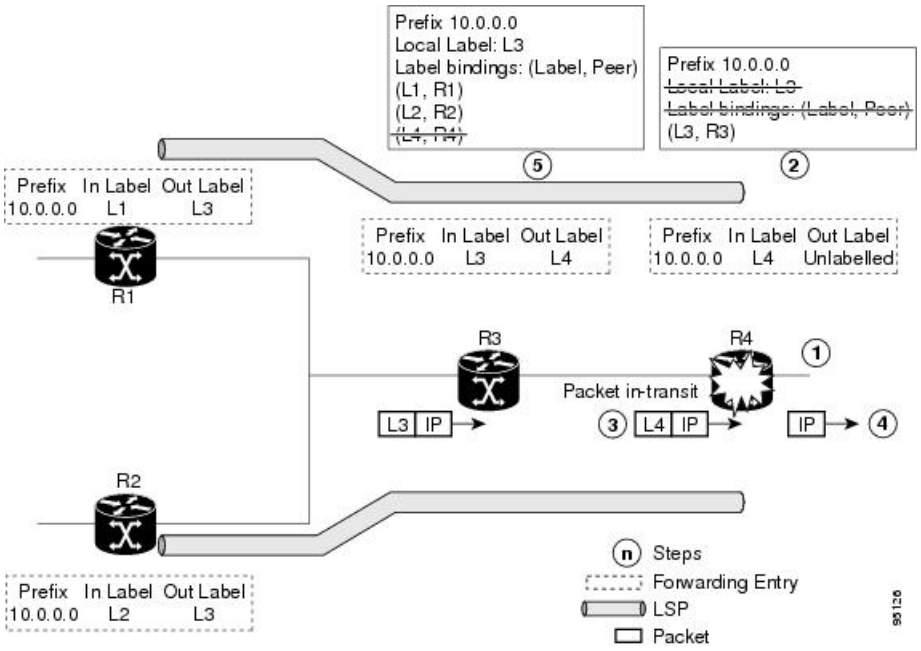
Related Topics

LDP Graceful Restart, on page 9
Recovery with Graceful-Restart, on page 11
Setting Up LDP NSF Using Graceful Restart, on page 54
Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 104

Recovery with Graceful-Restart

Figure 4: Recovering with Graceful Restart

This figure illustrates the process of failure recovery using graceful restart.



1. The router R4 LSR control plane restarts.
2. With the control plane restart, LIB is gone but forwarding states installed by R4's LDP control plane are not immediately deleted but are marked as stale.
3. Any in-transit packets from R3 to R4 (still labeled with L4) arrive at R4.
4. The MPLS forwarding plane at R4 performs a successful lookup for the local label L4 as forwarding is still intact. The packet is forwarded accordingly.
5. The router R3 LDP peer detects the failure of the control plane and channel and deletes the label bindings from R4. The peer, however, does not delete the corresponding forwarding states but marks them as stale.
6. At this point there are no forwarding disruptions.
7. The peer also starts the neighbor reconnect timer using the reconnect time value.
8. The established LSPs going toward the router R4 are still intact, and there are no broken LSPs.

When the LDP control plane recovers, the restarting LSR starts its forwarding state hold timer and restores its forwarding state from the checkpointed data. This action reinstates the forwarding state and entries and marks them as old.

The restarting LSR reconnects to its peer, indicated in the FT Session TLV, that it either was or was not able to restore its state successfully. If it was able to restore the state, the bindings are resynchronized.

The peer LSR stops the neighbor reconnect timer (started by the restarting LSR), when the restarting peer connects and starts the neighbor recovery timer. The peer LSR checks the FT Session TLV if the restarting peer was able to restore its state successfully. It reinstates the corresponding forwarding state entries and receives binding from the restarting peer. When the recovery timer expires, any forwarding state that is still marked as stale is deleted.

If the restarting LSR fails to recover (restart), the restarting LSR forwarding state and entries will eventually timeout and is deleted, while neighbor-related forwarding states or entries are removed by the Peer LSR on expiration of the reconnect or recovery timers.

Related Topics

LDP Graceful Restart, on page 9
Phases in Graceful Restart, on page 11
Setting Up LDP NSF Using Graceful Restart, on page 54
Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 104

Label Advertisement Control (Outbound Filtering)

By default, LDP advertises labels for all the prefixes to all its neighbors. When this is not desirable (for scalability and security reasons), you can configure LDP to perform outbound filtering for local label advertisement for one or more prefixes to one more peers. This feature is known as *LDP outbound label filtering*, or *local label advertisement control*.

Related Topics

Configuring Label Advertisement Control (Outbound Filtering), on page 46
Configuring Label Advertisement (Outbound Filtering): Example, on page 103

Label Acceptance Control (Inbound Filtering)

By default, LDP accepts labels (as remote bindings) for all prefixes from all peers. LDP operates in liberal label retention mode, which instructs LDP to keep remote bindings from all peers for a given prefix. For security reasons, or to conserve memory, you can override this behavior by configuring label binding acceptance for set of prefixes from a given peer.

The ability to filter remote bindings for a defined set of prefixes is also referred to as *LDP inbound label filtering*.



Note Inbound filtering can also be implemented using an outbound filtering policy; however, you may not be able to implement this system if an LDP peer resides under a different administration domain. When both inbound and outbound filtering options are available, we recommend that you use outbound label filtering.

Related Topics

Configuring Label Acceptance Control (Inbound Filtering), on page 57
Configuring Label Acceptance (Inbound Filtering): Example, on page 105

Local Label Allocation Control

By default, LDP allocates local labels for all prefixes that are not Border Gateway Protocol (BGP) prefixes[1]. This is acceptable when LDP is used for applications other than Layer 3 virtual private networks (L3VPN) core transport. When LDP is used to set up transport LSPs for L3VPN traffic in the core, it is not efficient or even necessary to allocate and advertise local labels for, potentially, thousands of IGP prefixes. In such a case, LDP is typically required to allocate and advertise local label for loopback /32 addresses for PE routers. This

[1] For L3VPN Inter-AS option C, LDP may also be required to assign local labels for some BGP prefixes.

is accomplished using LDP local label allocation control, where an access list can be used to limit allocation of local labels to a set of prefixes. Limiting local label allocation provides several benefits, including reduced memory usage requirements, fewer local forwarding updates, and fewer network and peer updates.

Tip You can configure label allocation using an IP access list to specify a set of prefixes that local labels can allocate and advertise.

Related Topics

Configuring Local Label Allocation Control, on page 58
Configuring Local Label Allocation Control: Example, on page 105

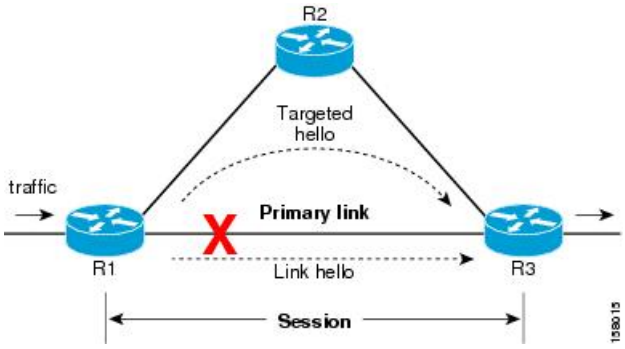
Session Protection

When a link comes up, IP converges earlier and much faster than MPLS LDP and may result in MPLS traffic loss until MPLS convergence. If a link flaps, the LDP session will also flap due to loss of link discovery. LDP session protection minimizes traffic loss, provides faster convergence, and protects existing LDP (link) sessions by means of "parallel" source of targeted discovery hello. An LDP session is kept alive and neighbor label bindings are maintained when links are down. Upon reestablishment of primary link adjacencies, MPLS convergence is expedited as LDP need not relearn the neighbor label bindings.

LDP session protection lets you configure LDP to automatically protect sessions with all or a given set of peers (as specified by peer-acl). When configured, LDP initiates backup targeted hellos automatically for neighbors for which primary link adjacencies already exist. These backup targeted hellos maintain LDP sessions when primary link adjacencies go down.

The Session Protection figure illustrates LDP session protection between neighbors R1 and R3. The primary link adjacency between R1 and R3 is directly connected link and the backup; targeted adjacency is maintained between R1 and R3. If the direct link fails, LDP link adjacency is destroyed, but the session is kept up and running using targeted hello adjacency (through R2). When the direct link comes back up, there is no change in the LDP session state and LDP can converge quickly and begin forwarding MPLS traffic.

Figure 5: Session Protection



Note When LDP session protection is activated (upon link failure), protection is maintained for an unlimited period time.

Related Topics

Configuring Session Protection, on page 59
Configuring LDP Session Protection: Example, on page 105

IGP Synchronization

Lack of synchronization between LDP and IGP can cause MPLS traffic loss. Upon link up, for example, IGP can advertise and use a link before LDP convergence has occurred; or, a link may continue to be used in IGP after an LDP session goes down.

LDP IGP synchronization synchronizes LDP and IGP so that IGP advertises links with regular metrics only when MPLS LDP is converged on that link. LDP considers a link converged when at least one LDP session is up and running on the link for which LDP has sent its applicable label bindings and received at least one label binding from the peer. LDP communicates this information to IGP upon link up or session down events and IGP acts accordingly, depending on sync state.

In the event of an LDP graceful restart session disconnect, a session is treated as converged as long as the graceful restart neighbor is timed out. Additionally, upon local LDP restart, a checkpointed recovered LDP graceful restart session is used and treated as converged and is given an opportunity to connect and resynchronize.

Under certain circumstances, it might be required to delay declaration of resynchronization to a configurable interval. LDP provides a configuration option to delay declaring synchronization up for up to 60 seconds. LDP communicates this information to IGP upon linkup or session down events.

From the 7.1.1 release, you can configure multiple MPLS-TE tunnel end points on an LER using the TLV 132 function in IS-IS. You can configure a maximum of 63 IPv4 addresses or 15 IPv6 addresses on an LER.

Note The configuration for LDP IGP synchronization resides in respective IGPs (OSPF and IS-IS) and there is no LDP-specific configuration for enabling of this feature. However, there is a specific LDP configuration for IGP sync delay timer.

Related Topics

Configuring LDP IGP Synchronization: OSPF, on page 60
Configuring LDP IGP Synchronization—OSPF: Example, on page 106
Configuring LDP IGP Synchronization: ISIS, on page 64
Configuring LDP IGP Synchronization—ISIS: Example, on page 106

IGP Auto-configuration

To enable LDP on a large number of interfaces, IGP auto-configuration lets you automatically configure LDP on all interfaces associated with a specified IGP interface; for example, when LDP is used for transport in the core network. However, there needs to be one IGP set up to enable LDP auto-configuration.

Typically, LDP assigns and advertises labels for IGP routes and must often be enabled on all active interfaces by an IGP. Without IGP auto-configuration, you must define the set of interfaces under LDP, a procedure that is time-intensive and error-prone.

Note LDP auto-configuration is supported for IPv4 unicast family in the default VRF. The IGP is responsible for verifying and applying the configuration.

You can also disable auto-configuration on a per-interface basis. This permits LDP to enable all IGP interfaces except those that are explicitly disabled and prevents LDP from enabling an interface when LDP auto-configuration is configured under IGP.

Related Topics

Enabling LDP Auto-Configuration for a Specified OSPF Instance, on page 65
Enabling LDP Auto-Configuration in an Area for a Specified OSPF Instance, on page 66
Disabling LDP Auto-Configuration, on page 67
Configuring LDP Auto-Configuration: Example, on page 106

LDP Nonstop Routing

LDP nonstop routing (NSR) functionality makes failures, such as Route Processor (RP) or Distributed Route Processor (DRP) failover, invisible to routing peers with minimal to no disruption of convergence performance. By default, NSR is globally enabled on all LDP sessions except AToM.

A disruption in service may include any of these events:

- Route processor (RP) or distributed route processor (DRP) failover
- LDP process restart
- In-service system upgrade (ISSU)
- Minimum disruption restart (MDR)

Note Unlike graceful restart functionality, LDP NSR does not require protocol extensions and does not force software upgrades on other routers in the network, nor does LDP NSR require peer routers to support NSR.

Process failures of active TCP or LDP results in session loss and, as a result, NSR cannot be provided unless RP switchover is configured as a recovery action. For more information about how to configure switchover as a recovery action for NSR, see *Configuring Transports* module in *IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers*.

Related Topics

Configuring LDP Nonstop Routing, on page 68

IP LDP Fast Reroute Loop Free Alternate

The IP Fast Reroute is a mechanism that enables a router to rapidly switch traffic, after an adjacent link failure, node failure, or both, towards a pre-programmed loop-free alternative (LFA) path. This LFA path is used to switch traffic until the router installs a new primary next hop again, as computed for the changed network topology.

The goal of LFA FRR is to reduce failure reaction time to 50 milliseconds by using a pre-computed alternate next hop, in the event that the currently selected primary next hop fails, so that the alternate can be rapidly used when the failure is detected.

This feature targets to address the fast convergence ability by detecting, computing, updating or enabling prefix independent pre-computed alternate loop-free paths at the time of failure.

IGP pre-computes a backup path per IGP prefix. IGP selects one and only one backup path per primary path. RIB installs the best path and download path protection information to FIB by providing correct annotation for protected and protecting paths. FIB pre-installs the backup path in dataplane. Upon the link or node failure, the routing protocol detects the failure, all the backup paths of the impacted prefixes are enabled in a prefix-independent manner.

Prerequisites

The Label Distribution Protocol (LDP) can use the loop-free alternates as long as these prerequisites are met:

The Label Switching Router (LSR) running LDP must distribute its labels for the Forwarding Equivalence Classes (FECs) it can provide to all its neighbors, regardless of whether they are upstream, or not.

There are two approaches in computing LFAs:

- **Link-based (per-link)**--In link-based LFAs, all prefixes reachable through the primary (protected) link share the same backup information. This means that the whole set of prefixes, sharing the same primary, also share the repair or fast reroute (FRR) ability. The per-link approach protects only the next hop address. The per-link approach is suboptimal and not the best for capacity planning. This is because all traffic is redirected to the next hop instead of being spread over multiple paths, which may lead to potential congestion on link to the next hop. The per-link approach does not provide support for node protection.
- **Prefix-based (per-prefix)**--Prefix-based LFAs allow computing backup information per prefix. It protects the destination address. The per-prefix approach is the preferred approach due to its greater applicability, and the greater protection and better bandwidth utilization that it offers.



Note The repair or backup information computed for a given prefix using prefix-based LFA may be different from the computed by link-based LFA.

The per-prefix LFA approach is preferred for LDP IP Fast Reroute LFA for these reasons:

- Better node failure resistance
- Better capacity planning and coverage

Features Not Supported

These interfaces and features are not supported for the IP LDP Fast Reroute Loop Free Alternate feature:

- BVI interface (IRB) is not supported either as primary or backup path.
- GRE tunnel is not supported either as primary or backup path.
- Cisco ASR 9000 Series SPA Interface Processor-700 POS line card on Cisco ASR 9000 Series Router is not supported as primary link. It can be used as LFA backup only on main interface.

- In a multi-topology scenerio, the route in topology T can only use LFA within topology T. Hence, the availability of a backup path depends on the topology.

For more information about configuring the IP Fast Reroute Loop-free alternate , see Implementing IS-IS on Cisco IOS XR Software module of the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Related Topics

Configure IP LDP Fast Reroute Loop Free Alternate: Examples, on page 107
Verify IP LDP Fast Reroute Loop Free Alternate: Example, on page 109

Downstream on Demand

This Downstream on demand feature adds support for downstream-on-demand mode, where the label is not advertised to a peer, unless the peer explicitly requests it. At the same time, since the peer does not automatically advertise labels, the label request is sent whenever the next-hop points out to a peer that no remote label has been assigned.

To enable downstream-on-demand mode, this configuration must be applied at mpls ldp configuration mode:

```
mpls ldp downstream-on-demand with ACL
```

The ACL contains a list of peer IDs that are configured for downstream-on-demand mode. When the ACL is changed or configured, the list of established neighbors is traversed. If a session's downstream-on-demand configuration has changed, the session is reset in order that the new down-stream-on-demand mode can be configured. The reason for resetting the session is to ensure that the labels are properly advertised between the peers. When a new session is established, the ACL is verified to determine whether the session should negotiate for downstream-on-demand mode. If the ACL does not exist or is empty, downstream-on-demand mode is not configured for any neighbor.

For it to be enabled, the Downstream on demand feature has to be configured on both peers of the session. If only one peer in the session has downstream-on-demand feature configured, then the session does not use downstream-on-demand mode.

If, after, a label request is sent, and no remote label is received from the peer, the router will periodically resend the label request. After the peer advertises a label after receiving the label request, it will automatically readvertise the label if any label attribute changes subsequently.

Related Topics

Configuring LDP Downstream on Demand mode, on page 71

Explicit-Null and Implicit-Null Labels

Cisco MPLS LDP uses null label, implicit or explicit, as local label for routes or prefixes that terminate on the given LSR. These routes include all local, connected, and attached networks. By default, the null label is **implicit-null** that allows LDP control plane to implement penultimate hop popping (PHOP) mechanism. When this is not desirable, you can configure **explicit-null** that allows LDP control plane to implement ultimate hop popping (UHOP) mechanism. You can configure this explicit-null feature on the ultimate hop LSR. This configuration knob includes an access-list to specify the IP prefixes for which PHOP is desired.

This new enhancement allows you to configure implicit-null local label for **non-egress (ultimate hop LSR)** prefixes by using the **implicit-null-override** command. This enforces implicit-null local label for a specific prefix even if the prefix requires a non-null label to be allocated by default. For example, by default, an LSR

allocates and advertises a non-null label for an IGP route. If you wish to terminate LSP for this route on penultimate hop of the LSR, you can enforce implicit-null label allocation and advertisement for this prefix using **implicit-null-override** feature.

Note If a given prefix is permitted in both explicit-null and implicit-null-override feature, then implicit-null-override supercedes and an implicit-null label is allocated and advertised for the prefix.

In order to enable implicit-null-override mode, this configuration must be applied at MPLS LDP label configuration mode:

```
mpls ldp
   label
     implicit-null-override for <prefix><ACL>

  !
```

This feature works with any prefix including static, IGP, and BGP, when specified in the ACL.

MPLS over IRB

The Integrated Routing and Bridging (IRB) feature in Cisco IOS XR Software enables routing of a given protocol between routed interfaces and bridge groups within a single router. IRB support for MPLS introduces these capabilities:

- Bridge-Group Virtual Interface (BVI) support under MPLS LDP
- Targeted LDP session to BVI neighbor
- MPLS OAM for BVI interfaces
- Netflow for BVI interfaces while MPLS is enabled
- L2VPN using targeted MPLS LDP to BVI destination
- L3VPN
- 6PE/6VPE

MPLS over IRB is supported completely on ASR 9000 Enhanced Ethernet Line Card and Cisco ASR 9001. MPLS over IRB is not supported on ASR 9000 Ethernet Line Card.

For more information on MPLS over IRB, see the *Implementing MPLS Label Distribution Protocol* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on MPLS over IRB commands, see the *MPLS Label Distribution Protocol Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

MPLS LDP Carrier Supporting Carrier for Multiple VRFs

The carrier supporting carrier (CSC) support for MPLS LDP feature enables MPLS label distribution protocol (LDP) to provide CSC support for Layer 3 Virtual Private Networks (L3VPN). To support LDP as label distribution protocol between PE-CE devices in an MPLS CSC L3VPN, LDP is required to operate in multiple Virtual Private Network routing and forwarding (VRF) contexts.

MPLS Carrier Supporting Carrier L3VPN: Introduction

The carrier supporting carrier feature enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the *backbone carrier*. The service provider that uses the segment of the backbone network is called the *customer carrier*.

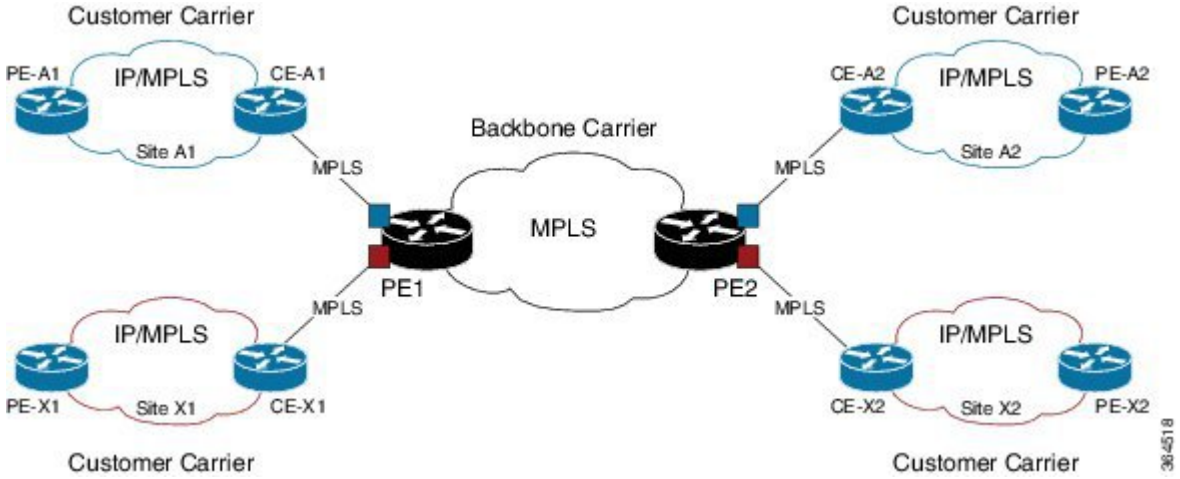
A backbone carrier offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services. The customer carrier can be either:

- An Internet service provider (ISP)
- A BGP/MPLS VPN service provider

In either case, MPLS is run in the backbone network and between the backbone and customer carrier (the PE-CE link).

Figure 6: MPLS Carrier Supporting Carrier L3VPN

This figure illustrates an MPLS CSC L3VPN.



The figure shows two customers, A and X, connecting their remote sites through the backbone carrier. The PE device of the backbone network connects with both customers through MPLS but under different VRFs according to interface-VRF mapping. The MPLS label distribution protocol for PE-CE connectivity can be either BGP or LDP, and requires them to run in a customer VRF context on the PE device.

Benefits of MPLS LDP CSC

The MPLS LDP CSC provides the following benefits to service providers who are backbone carriers and to customer carriers.

Benefits to the Backbone Carrier

- The backbone carrier can accommodate many customer carriers and give them access to its backbone. The backbone carrier does not need to create and maintain separate backbones for its customer carriers. Using one backbone network to support multiple customer carriers simplifies the backbone carrier's VPN operations. The backbone carrier uses a consistent method for managing and maintaining the backbone network. This is also cheaper and more efficient than maintaining separate backbones.
- The MPLS LDP CSC feature is scalable. CSC can change the VPN to meet changing bandwidth and connectivity needs. The feature can accommodate unplanned growth and changes. The CSC feature

enables tens of thousands of VPNs to be configured over the same network, and it allows a service provider to offer both VPN and internet services.

- The MPLS LDP CSC feature is a flexible solution. The backbone carrier can accommodate many types of customer carriers. The backbone carrier can accept customer carriers who are ISPs or VPN service providers or both. The backbone carrier can accommodate customer carriers that require security and various bandwidths.

Benefits to the Customer Carriers

- The MPLS LDP CSC feature removes from the customer carrier the burden of configuring, operating, and maintaining its own backbone. The customer carrier uses the backbone network of a backbone carrier, but the backbone carrier is responsible for network maintenance and operation.
- Customer carriers who use the VPN services provided by the backbone carrier receive the same level of security that Frame Relay or ATM-based VPNs provide. Customer carriers can also use IPSec in their VPNs for a higher level of security; it is completely transparent to the backbone carrier.
- Customer carriers can use any link layer technology (SONET, Digital Subscriber Line, Frame Relay, and so on) to connect the CE routers to the PE routers and the PE routers to the P routers. The MPLS LDP CSC feature is link layer independent. The CE routers and PE routers use IP or MPLS to communicate, and the backbone carrier uses MPLS.
- The customer carrier can use any addressing scheme and still be supported by a backbone carrier. The customer address space and routing information are independent of the address space and routing information of other customer carriers or the backbone provider.

Multiple VRF Support

To support multiple VRFs, IOS XR LDP configuration model is extended to allow VRF submode and per-VRF configuration and feature or interface enabling.

IOS XR LDP process is not distributed nor it is multi-instance, hence the single LDP process services all the configured VRFs. In large scale VRF deployment, it is recommended to enable VRF under LDP with appropriate policies and label filtering.

RSI

To obtain VRF and routing tables' related information, LDP interacts with the router space infrastructure (RSI) server. For every LDP enabled non-default VRF, LDP registers with RSI to get notifications upon VRF default (IPv4/IPv6) tables getting created or deleted, and populate the LDP VRF database accordingly.

VRF Table ID Database

A new database is added in the LDP process to keep track of all VRFs enabled under LDP. This database holds both active as well as forward-reference VRF records. In addition to serving as an LDP context, each active record of this database also holds VRF's default (IPv4/IPv6 unicast) table IDs.

VRF-Interface Mapping

To enable LDP on an interface for a given address family under a VRF context , it is required to list interface and its address family explicitly under a LDP VRF submode. LDP does not enforce or check correctness of the interface and VRF mapping at the time of configuration, and hence configuration may be accepted by LDP. The interface with incorrect VRF mapping is not made operational by LDP and remains down from the LDP point of view.

This means that an interface remains LDP operationally down for which either:

- LDP has not received any address update, or
- LDP has received update with different table-id (VRF) than configured under LDP.

Also, a user must not configure the same LDP interface under more than one VRF.

Context Isolation

Each active VRF under LDP points to a separate context under which LDP runs. This means that various variables, database, tables, FSM are kept separate in their respective VRF contexts and do not interfere or interact with each other. This allows the LDP to provide per-VRF isolation and support CSC with customers with overlapping addresses or routing information.

Default Context

The default (global) context is enabled at the time of the LDP process startup and remains enabled always. It is not possible to disable IPv4 for the default context. Also, it is required to explicitly enable IPv4 for non-default context. Therefore you can effectively disable IPv4 for non-default context by not configuring it. This means that, it is possible to enable or disable the non-default context under LDP, whereas the same is not possible for a default context.

Restrictions and Recommendations

The following restrictions and recommendations apply to the MPLS LDP CSC feature:

- Only IPv4 address family is supported for a default or a non-default VRF.
- No T-LDP support in a VRF context.
- An address family under VRF and VRF interface must be configured for non-default VRFs.
- Following scenarios are not supported :
  - Different VRFs between a given PE-CE device pair (VRFs configured on different links and interfaces)
  - LDP/BGP CSC co-existence on a given VRF between a given PE-CE device pair:
    - Single link
    - Parallel links: LDP CSC on one link and BGP CSC on the other
- LDP router-id must be configured per-VRF. If not configured for non-default VRF, LDP computes router-id from available loopback interfaces under the VRF.
- It is recommended to configure a routable discovery transport address under a VRF IPv4 address-family submode for deterministic transport endpoint and connection.
- When LDP CSC is configured and in use:
  - BGP label allocation policy for VRF prefixes must be per-prefix
  - Selective VRF Download (SVD) feature must be disabled

IPv6 Support in MPLS LDP

Internet Protocol version 6 (IPv6) support in MPLS LDP (Label Distribution Protocol) feature makes the LDP control plane to run on IPv6 in order to setup LSPs for IPv6 prefixes. This support enables most of the LDP functions supported on IPv4 to be extended to IPv6. In this context, support for native MPLS LDP over IPv6 is provided in order to seamlessly continue providing existing services while enabling new ones.

LDP associates a forwarding equivalence class (FEC) with each label switched path (LSP) it creates. The FEC associated with an LSP specifies which packets are mapped to that LSP. LDP establishes sessions with peers and exchanges FEC label bindings with them to enable creation of LSPs to carry MPLS traffic destined to IP prefixes.

LDP base specification, RFC 5036 defines procedures and messages for exchanging bindings for IPv4 and IPv6 addresses and routing prefixes. LDP IPv6 specification (draft-ietf-mpls-ldp-ipv6) updates LDP base specifications for IPv6 support, and further clarifies and focuses on the procedures for supporting LDP IPv6 control plane and binding advertisement.

The procedures of address bindings, label bindings, and forwarding setup are same for IPv4 and IPv6 address families in LDP. The only difference is that, a different address format is used according to the IP address family. While a single-stack IP address family (IPv4-only or IPv6-only) enabled interfaces between a set of routers is the most typical deployment, scenarios for LSR interconnections using both IPv4 and IPv6 interfaces are also supported.

IPv6 support in MPLS LDP implements draft-ietf-mpls-ldp-ipv6 version12 issued by the Internet Engineering Task Force (IETF).

LDP IPv6 Functionality

LDP functionality can be broadly divided into two categories:

- Control Plane

  Control plane includes functions such as: neighbor discovery (hello adjacencies), transport connection/endpoint (TCP connection), session and peering, and bindings exchange.

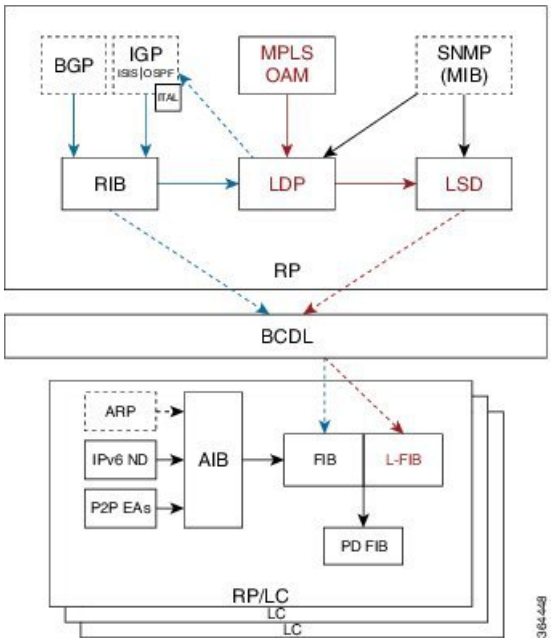
- LSP Setup

  LSP setup includes functions such as: acquire FEC information through RIB, assign and advertise local label bindings for FEC, advertise local (interface) IP address bindings and setup forwarding rewrites.

For the control plane, the underlying address family can be either IPv4-only, IPv6-only or both. Whereas for the LSP setup, an LSP is setup for IPv4 or IPv6 FEC prefix.

Figure 7: LDP IPv6 Architecture

This figure illustrates the main components that collaborate to achieve the required functionality for the LDP IPv6 feature.

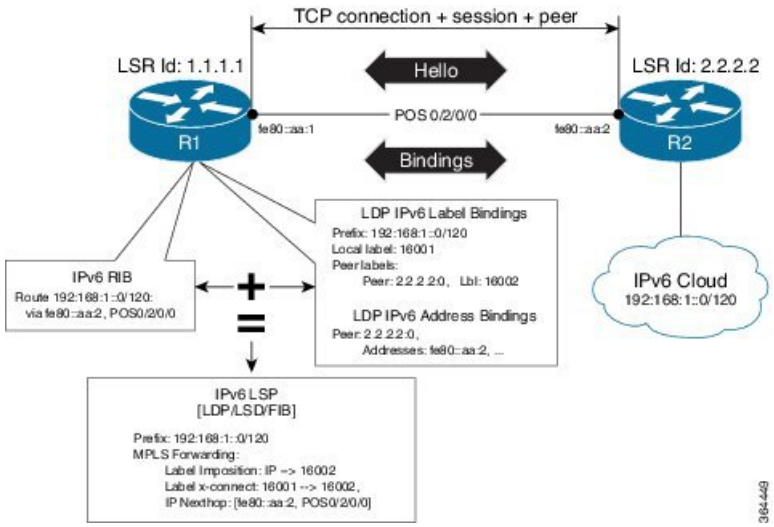


The functions of LDP in the MPLS LDP IPv6 setup are as follows:

- Receive routing updates from routing information base (RIB) for global IPv6 prefixes
- Assign local labels for IPv6 prefixes
- Receive IPv6 address or state notifications for local IPv6 enabled interfaces from IP Address Repository Manager (IP-ARM/IM) and LAS for IPv6 link-local unicast addresses
- Advertise/Accept IPv6 label bindings and address bindings to/from peers
- Setup MPLS forwarding to create IPv6 LSPs
- Provide IPv6 LSP information to MPLS OAM as and when requested
- Service MIB requests for IPv6 control plane queries and generate MIB traps
- Provide LDPv6 convergence status for a link to IGP for LDP-IGP Sync feature for IPv6
- Support IPv6 address family for all existing LDP features that intersect with prefixes and/or addresses

Figure 8: LDP IPv6 Control Plane and LSP Setup

This figure illustrates the high level functionality of LDP in terms of control plane and LSP setup in an IPv6 environment.



Topological Scenarios

A typical deployment scenario consists of single-stack IP address-family (IPv4-only or IPv6-only) enabled interfaces between a set of routers.

Three topology scenarios in which the LSRs are connected through one or more dual-stack LDP enabled interfaces, or one or more single-stack LDP enabled interfaces are defined as follows:

Note **R2** is the main router.

1. One dual-stack interface/same neighbor:

```
R1_ _ _ _ _ _ _ _R2
     IPv4+IPv6
```

2. Two single-stack interfaces/same neighbor:

```
     1. (IPv4)
R1_ _ _ _ _ _ _ _ _R2
  _ _ _ _ _ _ _ _ _
     2. (IPv6)
```

3. Two single-stack interfaces/different neighbors with different address families:

```
     1. (IPv4)          2. (IPv6)
R1_ _ _ _ _ _ _ _ R2_ _ _ _ _ _ _ _ R3
```

Case Study

A description of the control plane and LSP setup scenarios for the previously shown three configurations are as follows:

Case 1:

Neighbor Discovery: Both IPv4 and IPv6 Hellos sent on the interface to R1.

Transport Connection: IPv4 endpoints or IPv6 endpoints (as per user preference).

Label binding exchange: Both IPv4 and IPv6 prefixes.

Address binding exchange: Both IPv4 and IPv6 addresses.

LSPs: Both IPv4 and IPv6 over the same nexthop interface to R1.

Case 2:

Neighbor Discovery: IPv4 Hellos on interface-1 to R1 and IPv6 Hellos on interface-2 to R1.

Transport Connection: IPv4 endpoints or IPv6 endpoints (as per user preference).

Label binding exchange: Both IPv4 and IPv6 prefixes.

Address binding exchange: Both IPv4 and IPv6 addresses.

LSPs: IPv4 over nexthop interface-1 to R1 and IPv6 over nexthop interface-2 to R1.

Case 3:

Neighbor Discovery: IPv4 Hellos on interface-1 to R1 and IPv6 Hellos on interface-2 to R3.

Transport Connection: IPv4 endpoints with R1 and IPv6 endpoints with R3.

Label binding exchange: Both IPv4 and IPv6 prefixes to R1 and R3.



Note Even if all the three LSRs are dual-stack, traffic from R1 to R3 will not be completely labeled.

- If there is IPv6 traffic, it is unlabeled from R1 to R2. Labels are imposed only at R2 (although in this specific case implicit null imposition) to R3.
- If there is IPv4 traffic, it is labeled from R1 to R2. But the traffic will go unlabeled between R2 and R3 given that no IPv4 adjacency exists between R2 and R3.

Address binding exchange: Both IPv4 and IPv6 addresses to R1 and R3.

LSPs: IPv4 over nexthop interface-1 to R1 and IPv6 over nexthop interface-2 to R3.

Restrictions

IPv6 support in MPLS LDP has the following restrictions and constraints:

- IPv6 address family is supported only under default VRF
- Implicit enabling of IPv6 address family is not allowed. It needs explicit enabling.
- It is recommended to configure a routable IPv6 **discovery transport address** when only LDP IPv6 is configured without explicitly specifying a router-id

Features Supported in LDP IPv6

The following features are supported in LDP IPv6:

- Single-stack (native IPv6) and dual-stack (IPv4+IPv6) topologies
- New operating modes in LDP:
  - Native LDP IPv6
  - LDP IPv6 over IPv4 and LDP IPv4 over IPv6 connection endpoints

    LDP Hellos carry optional transport address type length value (TLV) to notify a peer about TCP or transport connection endpoint. An LSR can include either IPv4 or IPv6 transport address TLV in an IPv4 or IPv6 Hello message. There is no difference in the TLV format of transport address for IPv4 and IPv6.

    Only one transport connection is established between two discovered peers, whether there be single address family Hello adjacencies or multi-address family (both IPv4 and IPv6) Hello adjacencies.

    In a dual-stack setup, when LDP has the option to establish transport connection either using IPv4 endpoints or IPv6 endpoints, IPv6 connection is preferred over IPv4 connection. If LDP is locally enabled for both IPv4 and IPv6 address families, every new session is treated as potential dual-stack connection. Under such circumstances, IPv6 preference is kept in place for maximum fifteen seconds for the session to establish, after which the LDP tries to establish a connection with the peer using IPv4. A user can override this default behavior by specifying the preference for a set of dual-stack peers to use IPv4 transport for the connection. Furthermore, a user may also specify maximum wait time to wait to establish the preferred transport connection. If the preferred transport establishment times out, LDP tries to establish connection with other non-preferred transport address families. This applies to both the cases when an LSR acts as active side or passive side for the TCP connection.

    To override default IPv6 transport preference for dual-stack cases, use the **mpls ldp neighbor dual-stack transport-connection prefer ipv4 for-peers** command. To specify the maximum time the preferred address family connection must wait to establish a connection before resorting to a non-preferred address family, use the **mpls ldp neighbor dual-stack transport-connection max-wait** command.

    Once a transport connection is established, it is not torn down depending on preferences. If the address family related to established transport connection is disabled under LDP, the corresponding transport connection is reset to reestablish the connection.

    For a single-stack setup, there is no contention; the transport connection uses the given address family.

- LDP Control Plane is IPv6 aware
- LDP IPv6 LSP forwarding setup

  LDP interacts with LSD in order to setup IPv6 LSP forwarding. The steps involved in this interaction are:

  - Label allocation for an IPv6 prefix is learnt from RIB.
  - Setup imposition and label switching forwarding path for given IPv6 prefix by creating IPv6 forwarding rewrites.
  - Like LDP IPv4, rewrite delete and label free operations are performed when a route disappears or is disallowed under LDP due to label policy.

- There is no new requirement related to MPLS enabling or disabling. LDP also MPLS-enables in LSD (if not already) any LDP enabled interface, which is in the *UP* state for IP4 and/or IPv6 and has IPv4 and/or IPv6 addresses assigned.
- In case of dual-stack LDP, a single Resource-Complete is sent by LDP to LSD once RIB-Converged notification is received for both IPv4 and IPv6 redistribute tables.

- Distribution of IPv4 and IPv6 bindings over a single LDP session established over IPv4 or IPv6
- LDP Downstream on Demand
- LDP session protection

  LDP session protection is a feature to protect an IPv6 LDP session. In case of dual-stack hello adjacencies with a peer, there is only a single targeted hello adjacency to protect the session. Session protection forms targeted adjacency of address family same as the transport connection. For IPv6, the target of the session protection is the remote transport connection endpoint. For IPv4, the target of the session protection is remote LSR ID.

- LDP IGPv6 sync on IPv6 interface

  This feature lets IGP support LDP IGP Sync feature for IPv6 address family. This means that Intermediate System-to-Intermediate System (IS-IS) allows IGP under an interface's IPv6 address family, whereas OSPFv3 implements it just like existing support in OSPF for IPv4. When the IGP Sync feature is enabled, LDP convergence status on an interface is considered by the IGP under the context of a given address family. This behavior applies to IGP Sync for both non-TE as well as TE tunnel interfaces.

- LDP Typed Wildcard for IPv6 prefix FEC

  This feature adds support for Typed Wildcard for IPv6 Prefix FEC. The support includes:

  - Being able to send or receive IPv6 Prefix Typed Wildcard FEC element in label messages.
  - Respond to Typed Wildcard Label Requests received from peer by replaying its label database for IPv6 prefixes.
  - Make use of Typed Wildcard Label Requests towards peers to request replay of peer label database for IPv6 prefixes. For example, on local inbound policy changes.

- Label allocation, advertisement and accept policies for IPv6 prefixes
- Local label assignment and advertisement for IPv6 default-route (::/0)
- Session MD5 authentication for IPv6 transport
- IPv6 Explicit-Null label

  IPv6 explicit null label feature support includes:

  - Advertisement and receipt of IPv6 explicit-null label to and from peers.
  - IPv6 explicit-null outgoing label in forwarding setup.
  - Explicit-null advertisement policy for a set of IPv6 prefixes and/or set of peers.
  - Explicit-null configuration change. Change in explicit-null configuration is handled by first transferring a wildcard withdraw with null label to peer(s), followed by advertising the appropriate null (implicit or explicit) label to the peer(s) again. This works without any issue as long as a single IP address family is enabled. In case of a dual-stack LSR peer, a change of configuration related to

explicit-null advertisement for a given address family may cause unnecessary mix-up in the other address family.

- LDP IPv6 LFA FRR

  Local LFA FRR for IPv6 is supported. However, it is required that the primary and backup paths are of the same address family type, that is, an IPv4 primary path must not have an IPv6 backup path.

- NSF for LDP IPv6 traffic

  Non-stop forwarding (NSF) support is either provided through LDP NSR or graceful restart mechanisms.

- IGP/LDP NSR for IPv6
- IGP/LDP Graceful Restart for IPv6
- LDP ICCP IPv6 neighbor node

  LDP Inter-Chassis Communication Protocol (ICCP) is supported with IPv6 neighbor node. ICCP is used as a mechanism for multi-chassis LACP.

- SSO/ISSU for LDP IPv6
- MPLS OAM: New FECs

  LSPV supports two new FECs.

  - LDP IPv6 Prefix FEC Encoding/Decoding

    Label Switched Path Verification (LSPV) encodes/decodes the LDP IPv6 Prefix FEC. Prefix is in the network byte order and the trailing bits are to be set to zero when prefix length is shorter than 128 bits.

  - Generic IPv6 Prefix FEC Encoding/Decoding

    LSPV encodes/decodes the generic IPv6 Prefix FEC. Prefix is in the network byte order and the trailing bits are to be set to zero when prefix length is shorter than 128 bits.

    Generic IPv6 FEC is used in addition to the LDP IPv6 FEC. This serves the following primary purposes:

    - Allows user to perform LSP ping and traceroute to verify data plane without involving control plane of the FEC in echo request and response.
    - If support for a new FEC is preferred in the future, the generic FEC can be used until corresponding control plane is explicitly supported by LSPV.

- IPv6 LSR MIB

  MPLS OAM LDP MIBS is extended to support IPv6. All LSR MIB objects that reference an InSegment prefix and OutSegment next hop address are modified to support IPv6.

- LSP ping support for LDP IPv6
- LSP trace-route support for LDP IPv6
- LSP tree-trace support for LDP IPv6

The following features are not supported in LDP IPv6:

- LDPv6 over TEv4 (traffic engineering)
- L2VPN/PW (over IPv6 LSPs)
- L3VPN (over IPv6 LSPs)
- LDP auto-config for IPv6 IGP/Interfaces
- LDP ICCP with IPv6 neighbor node
- Multicast extension to LDP (mLDP) for IPv6 FEC with label binding through IPv4 and IPv6 transport
- Native IPv4 and IPv6 L3VPN over LDP IPv6 core
- L2VPN signaling with LDP when the nexthop address is IPv6
- IPv6 LDP CSC

Implicit IPv4 Disable

The LDP configuration model was changed with the introduction of explicit address family enabling under LDP (VRF) global and LDP (VRF) interfaces. However, in order to support backward compatibility, the old configuration model was still supported for default VRF. There was, however, no option to disable the implicitly enabled IPv4 address family under default VRF's global or interface level.

A new configuration **mpls ldp default-vrf implicit-ipv4 disable** is now available to the user to disable the implicitly enabled IPv4 address family for the default VRF. The new configuration provides a step towards migration to new configuration model for the default VRF that mandates enabling address family explicitly. This means that if the new option is configured, the user has to explicitly enable IPv4 address family for default VRF global and interface levels. It is recommended to migrate to this explicitly enabled IPv4 configuration model.

For detailed configuration steps, see Disabling Implicit IPv4, on page 98

IPv6 Label Bindings

LDP stores label bindings associated with FEC prefix in its Label Information Base (LIB) [TIB in Cisco LDP]. An entry in LIB corresponds to a prefix and holds the following bindings:

- Local binding: Local label assigned for this prefix (which is learnt through local RIB).
- Remote bindings: Array of peer labels (prefix-label bindings received in label mapping message from peer(s)).

An entry in LIB can exist due to local binding presence, or due to remote binding(s) presence, or due to both local and remote bindings presence. The forwarding setup, however, mandates that local binding be present for a prefix.

Extensions have been implemented to support IPv6 prefixes for LIB in LDP. For per-address family convergence or preference reasons, separate or new LIB is implemented to keep and maintain IPv6 prefixes. In case of dual-stack LDP, LIBv4 is preferred over LIBv6 wherever possible. For example, during background *housekeeping* function, LIBv4 is processed before LIBv6.

IPv6 Address Bindings

LDP needs to maintain IPv6 address database for local and peer interface addresses. The IPv4 address module for local/peer addresses is extended to keep IPv4/IPv6 addresses in their respective databases, much like LIB

database. In case of a dual-stack LDP, IPv4 local address database function is preferred over IPv6 local address database function where ever possible.

Default Transport Address

LDP computes default local transport address for IPv6 from its IPv6 interface or address database by picking the lowest operational loopback interface with global unicast IPv6 address. This means that any change in this loopback state or address, flaps or changes the default transport address for IPv6 and may cause session flaps using such an address as transport endpoint. For example, if a session is currently active on Loopback2 as during it's inception it was the lowest loopback with an IPv6 address, and a lower loopback, Loopback0, is configured with an IPv6 address, the session does not flap. However, if it does flap, the next time the session is attempted, Loopback0 is used.

The session flaps when configuring discovery transport address explicitly.

Use the **discovery transport-address** command under the LDP address family submode to specify the global transport address for IPv4 or IPv6.

It is recommended to configure global transport-address for IPv6 address family to avoid a potentially unstable default transport address.

LDP Control Plane: Bindings Advertisement

LDP base specification allows exchange of IPv4/IPv6 bindings (address/label) on an established session. When both IPv4 and IPv6 address families are enabled under LDP, LDP distributes address/label bindings for both address families to its established peer according to local policies. Following are a few significant points pertaining to bindings support for IPv6:

- LDP allocates/advertises local label bindings for link-local IPv6 address prefixes. If received, such FEC bindings are ignored.
- LDP sends only the Prefix FEC of the single address family type in a FEC TLV and not include both. If such a FEC binding is received, the entire message is ignored.
- LDP sends only the addresses belonging to same address family in a single address list TLV (in address or address withdraw message).

If an address family is not enabled on receiving LSR, LDP discards any bindings received from peer(s) for the address family. This means that when address family is enabled, LDP needs to reset existing sessions with the peers in order to re-learn the discarded bindings. The implementation is optimized to reset only those sessions which were previously known to be dual-stack and had sent bindings for both address families.

LSP Mapping

LDP uses IPv6 adjacency information instead of IP address to map an IPv6 link-local nexthop to an LDP peer.

In addition to other usual checks before using a label from nexthop LDP peer, LDP uses the nexthop label for a prefix of a given address family, if there are one or more LDP hello adjacencies of the same address family type established with the peer.

Label Policies

LDP allows a user to configure label policies for allocation, acceptance, receipt, and advertisement of labels for the given prefixes.

Following are the significant points pertaining to the IPv6 support for label policies:

- Label policies and their configurations are allowed under address family IPv6.
- Any policy that specifies prefix or a set of prefixes through an ACL, supports both IPv4 and IPv6 variants for address(s) or ACLs.
- Any policy that specifies peer address or set of peer addresses through an ACL, supports both IPv4 and IPv6 variant for peer address(s) or ACL.
- Any policy that specifies the peer's LSR ID in a peer ACL continues to take IPv4 ACL based policy irrespective of the feature configuration.

IS-IS

Intermediate System-to-Intermediate System (IS-IS) is an Interior Gateway Protocol (IGP) that advertises link-state information throughout the network to create a picture of the network topology. IPv6 IS-IS extends the address families supported by IS-IS to include IPv6, in addition to IPv4.

Previously, IS-IS supported registration of only LDP IPv4 sync status change. This has now been enhanced to support registration of notifications of LDP IPv6 sync status change. IS-IS determines the link-metrics to be advertised based on the LDP-IGP sync status on the IPv4 and IPv6 address families.

IS-IS supports non-stop forwarding (NSF) by preserving the LDPv6-IGP sync status across high availability (HA) events of IS-IS process restarts and failover.

IS-IS also supports LDPv6-IGP sync for LFA-FRR by checking the sync status of the backup interface (if it is configured with LDP IPv6 sync).

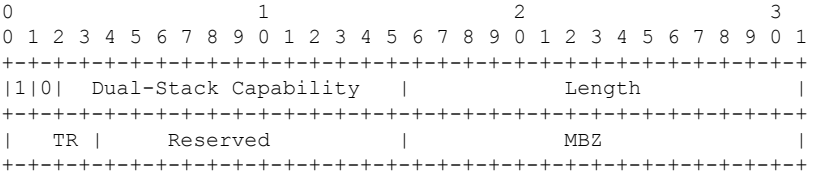
Dual-Stack Capability TLV

Clear rules are specified in RFC 5036 to determine transport connection roles in setting up a TCP connection for single-stack LDP. But RFC 5036 is not clear about dual-stack LDP, in which an LSR may assume different roles for different address families, causing issues in establishing LDP sessions.

To ensure a deterministic transport connection role for the dual-stack LDP, the dual-stack LSR conveys its transport connection preference in every LDP Hello message. This preference is encoded in a new TLV (Type Length Value) called the Dual-Stack Capability TLV. Dual-stack LSR always checks for the presence of the dual-stack capability TLV in the received LDP Hello messages and takes appropriate action for establishing or maintaining sessions.

RFC 7552 specifies more details about updates to LDP for IPv6.

Dual-Stack Capability TLV Format



Dual-Stack Capability TLV Fields

Field	Description
U and F bits	1 and 0 (as specified by RFC 5036)
Dual-Stack Capability	TLV code point (0x0701)
TR: Transport Connection Preference	TR: Transport Connection Preference: • 0100: LDPoIPv4 connection • 0110: LDPoIPv6 connection (default)
Reserved	This field is reserved. It must be set to zero on transmission and ignored on receipt
MBZ	Must be zero

Compliance Check

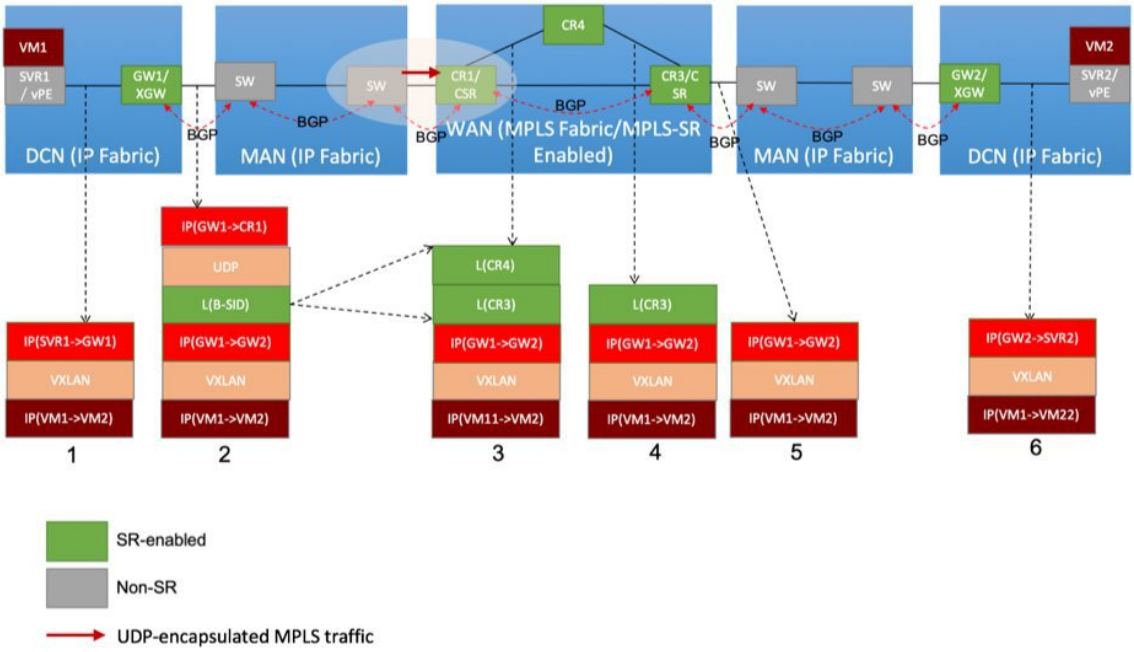
The compliance check prevents sessions being formed with prior RFC 7552 implementation of LDP IPv6.

If the dual-stack capability TLV is not present in the received Hellos and the compliance check is configured, the local and remote preferences must match to establish a session. If the preferences do not match, the LDP Hellos are dropped and the session is not established. Compliance check has therefore been disabled by default.

Use the command **neighbor dual-stack tlv-compliance** in MPLS LDP configuration to enable the compliance check.

UDP Decapsulation of MPLS-Over-UDP Traffic

You can encapsulate MPLS traffic in a UDP header (as per RFC 7510). UDP-encapsulated MPLS traffic allows better load balancing of MPLS traffic over ECMP (and LAGs) by acting as an entropy field. MPLS traffic can pass through two adjacent LSRs in an LSP, even when separated by an IP network. A metropolitan-area network (MAN) or LAN deploys this configuration, and not a WAN.



The image depicts the MAN border router **sw** sending UDP-encapsulated MPLS traffic to the WAN edge Cisco ASR 9000 Series router **CR1/CSR**. The destination IP address field contains the (peering) loopback IP address of the WAN edge router. The destination UDP port field is 6635, allocated for UDP tunnels that transport MPLS traffic. The WAN edge router removes the UDP header. Based on the MPLS label, it forwards the MPLS traffic toward the destination.

To enable the UDP decapsulation function on the ASR 9000 Series router, configure the **hw-module l3 feature mpls-over-udp-decap enable** command in global configuration mode. If you don't enable this function, the ASR 9000 Series router drops the UDP-encapsulated MPLS traffic it receives. Configuration:

```
Router# configure
Router(config)# hw-module l3 feature mpls-over-udp-decap enable
Router(config)# commit
```

Route Convergence with NHID Option for LDP in MPLS Networks

Table 3: Feature History Table

Feature Name	Release Information	Feature Description
Route Convergence with Next-Hop ID Option for LDP in MPLS Networks	Release 24.3.1	This release improves route convergence during routing changes and reduces downtime due to asynchronous Forwarding Information Base (FIB) updates by introducing Next-Hop ID (NHID) support for LDP via UDP sockets in MPLS networks. By synchronizing FIB updates across line cards and RPs, NHID ensures swift packet forwarding decisions without the need to reprogram all entries.

NHID for LDP Sessions in MPLS Networks

When there are more routes and links in a network, it can take longer for the Forwarding Information Base (FIB) to update and program new paths into the hardware. Asynchronous route updates on line cards and the Route Processor (RP) can further impact control plane connections resulting in traffic loss. This happens because the software FIB on the RP updates faster than the hardware, leading to mismatches in forwarding paths. If the time difference between these updates is too long, it can disrupt control plane connections, especially for LDP discovery hello messages used to maintain LDP sessions.

NHID is a feature that

- uses a predefined UDP socket option with NHID capability for LDP-related UDP traffic,
- improves network convergence during asynchronous FIB route updates by uniquely identifying the next hop in a routing path to expedite traffic forwarding decisions,
- minimizes traffic loss during FIB route convergence events,
- integrates with LDP to enhance the network's ability to handle increased routing scales and the demands of numerous parallel links, and
- benefits any unicast UDP control packets, such as discovery hello messages, sent to keep LDP sessions alive.

Usage Guidelines for NHID Option for UDP Sockets in MPLS

- This feature is enabled by default and you can neither disable it or configure it.
- The feature is applicable for both IPv4 and IPv6.

Verify NHID Options for UDP Sockets in MPLS

To verify the NHID option for UDP sockets is supported for LDP control packets, you can check the LDP operational parameters and identify specific UDP sockets with port 646, and then verify if the NHID option is enabled for those sockets.

Procedure

Step 1 Verify the NHID option for UDP sockets is supported for LDP control packets.

Example:

```
Router#show mpls ldp parameters
LDP Parameters:
  Role: Active
  Protocol Version: 1
  Router ID: 37.0.0.1
  Null Label:
    IPv4: Implicit
  Session:
    Hold time: 180 sec
    Keepalive interval: 60 sec
    Backoff: Initial:15 sec, Maximum:120 sec
    Global MD5 password: Disabled
  Discovery:
    Link Hellos:     Holdtime:15 sec, Interval:5 sec
    Targeted Hellos: Holdtime:45 sec, Interval:15 sec
                     Accepting:
                       IPv4: all;
    Quick-start: Enabled (by default)
    Transport address:
      IPv4: 37.0.0.1
  Graceful Restart:
    Enabled
    Reconnect Timeout:120 sec, Forwarding State Holdtime:180 sec
  NSR: Enabled, Not Sync-ed
  Timeouts:
    Housekeeping periodic timer: 10 sec
    Local binding: 300 sec
    Forwarding state in LSD: 360 sec
  Delay in AF Binding Withdrawl from peer: 180 sec
  Max:
    5000 interfaces (4000 attached, 1000 TE tunnel), 2000 peers
  OOR state
    Memory: Normal
  IGP sync delay:
    Interface up: 60 sec
  MPLS NHID Support: Yes
```

Step 2 Identify the UDP sockets with port 646 for LDP control packets from a list of all the UDP sockets.

Example:

```
Router#show udp brief
   PCB     VRF-ID     Recv-Q Send-Q  Local Address          Foreign Address
0x7fe448003420 0x00000000      0      0  :::0                   :::0
0x7fe448001c50 0x60000000      0      0  0.0.0.0:68             0.0.0.0:0
0x7fe448000f90 0x00000000      0      0  0.0.0.0:68             0.0.0.0:0
0x7fe448002c70 0x60000000      0      0  0.0.0.0:646            0.0.0.0:0
```

```
0x7fe448002400 0x00000000      0      0  0.0.0.0:646            0.0.0.0:0
```

Step 3 Verify the NHID option is enabled for a specific UDP socket with port 646.

Example:

```
Router#show udp detail pcb 0x7fe448002c70
Fri Oct  6 15:46:40.359 UTC

================================================
PCB is 0x7fe448002c70 SO 0x7fe448001f50, Family: 2, VRF: 0x60000000
Local host: 0.0.0.0:646 (Local App PID: 2698)
Foreign host: 0.0.0.0:0
Current send queue size: 0
Current receive queue size: 0
PCB flags: RECVDSTADDR, RECVIF
PCB Transport flags: MPLS_NHID_LBL
Traffic Class: 192
```

How to Implement MPLS LDP

A typical MPLS LDP deployment requires coordination among several global neighbor routers. Various configuration tasks are required to implement MPLS LDP :

Configuring LDP Discovery Parameters

Perform this task to configure LDP discovery parameters (which may be crucial for LDP operations).

Note The LDP discovery mechanism is used to discover or locate neighbor nodes.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **router-id** *ip-address lsr-id*
4. **discovery** { **hello** | **targeted-hello** } **holdtime** *seconds*
5. **discovery** { **hello** | **targeted-hello** } **interval** *seconds*
6. **commit**
7. (Optional) **show mpls ldp** [**vrf** *vrf-name*] **parameters**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	[**vrf** *vrf-name*] **router-id** *ip-address lsr-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1`	(Optional) Specifies a non-default VRF. Specifies the router ID of the local node. • In Cisco IOS XR software, the router ID is specified as an interface IP address. By default, LDP uses the global router ID (configured by the global router ID process).

Step 4	**discovery** { **hello** | **targeted-hello** } **holdtime** *seconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# discovery hello holdtime 30`
	`RP/0/RSP0/CPU0:router(config-ldp)# discovery targeted-hello holdtime 180`
		Specifies the time that a discovered neighbor is kept without receipt of any subsequent hello messages. The default value for the *seconds* argument is 15 seconds for link hello and 90 seconds for targeted hello messages.

Step 5	**discovery** { **hello** | **targeted-hello** } **interval** *seconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# discovery hello interval 15`
	`RP/0/RSP0/CPU0:router(config-ldp)# discovery targeted-hello interval 20`
		Selects the period of time between the transmission of consecutive hello messages. The default value for the *seconds* argument is 5 seconds for link hello messages and 10 seconds for targeted hello messages.

Step 6	**commit**	

Step 7	(Optional) **show mpls ldp** [**vrf** *vrf-name*] **parameters**
	Example:
	`RP/0/RSP0/CPU0:router # show mpls ldp parameters`
	`RP/0/RSP0/CPU0:router # show mpls ldp vrf red parameters`
		Displays all the current MPLS LDP parameters.
		Displays the LDP parameters for the specified VRF.

Related Topics

LDP Control Plane, on page 7

Configure Label Distribution Protocol Targeted Neighbor

LDP session between LSRs that are not directly connected is known as targeted LDP session. For LDP neighbors which are not directly connected, you must manually configure the LDP neighborship on both the routers.

Configuration Example

This example shows how to configure LDP for non-directly connected routers.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# mpls ldp
RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.0.2.1
RP/0/RSP0/CPU0:router(config-ldp)# neighbor 198.51.100.1:0 password encrypted 13061E010803
RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv4
RP/0/RSP0/CPU0:router(config-ldp-af)# discovery targeted-hello accept
RP/0/RSP0/CPU0:router(config-ldp-af)# neighbor 198.51.100.1 targeted
RP/0/RSP0/CPU0:router(config-ldp-af)# commit
```

Running Configuration

This section shows the LDP targeted neighbor running configuration.

```
mpls ldp
router-id 192.0.2.1
neighbor 198.51.100.1:0 password encrypted 13061E010803
address-family ipv4
  discovery targeted-hello accept
  neighbor 198.51.100.1 targeted
!
```

Verification

Verify LDP targeted neighbor configuration.

```
RP/0/RSP0/CPU0:router#show mpls ldp discovery
Wed Nov 28 04:30:31.862 UTC

Local LDP Identifier: 192.0.2.1:0
Discovery Sources:
  Targeted Hellos:  <<< targeted hellos based session
    192.0.2.1 -> 198.51.100.1(active/passive), xmit/recv   <<< both transmit and receive
of targeted hellos between the neighbors
      LDP Id: 198.51.100.1:0
          Hold time: 90 sec (local:90 sec, peer:90 sec)
          Established: Nov 28 04:19:55.340 (00:10:36 ago)

RP/0/RSP0/CPU0:router#show mpls ldp neigbhor
Wed Nov 28 04:30:38.272 UTC

Peer LDP Identifier: 198.51.100.1:0
  TCP connection: 198.51.100.1:0:13183 - 192.0.2.1:646; MD5 on
  Graceful Restart: No
  Session Holdtime: 180 sec
```

```
  State: Oper; Msgs sent/rcvd: 20/20; Downstream-Unsolicited
  Up time: 00:10:30
  LDP Discovery Sources:
    IPv4: (1)
      Targeted Hello (192.0.2.1 -> 198.51.100.1, active/passive) <<< targeted LDP based
session
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (4)
     198.51.100.1        10.0.0.1       172.16.0.1       192.168.0.1
    IPv6: (0)
```

Configuring LDP Discovery Over a Link

Perform this task to configure LDP discovery over a link.

Note There is no need to enable LDP globally.

Before you begin

A stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **router-id** *ip-address lsr-id*
4. **interface** *type interface-path-id*
5. **commit**
6. (Optional) **show mpls ldp discovery**
7. (Optional) **show mpls ldp vrf** *vrf-name* **discovery**
8. (Optional) **show mpls ldp vrf all discovery summary**
9. (Optional) **show mpls ldp vrf all discovery brief**
10. (Optional) **show mpls ldp vrf all ipv4 discovery summary**
11. (Optional) **show mpls ldp discovery summary all**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:**	Enters MPLS LDP configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# mpls ldp`	
Step 3	[**vrf** *vrf-name*] **router-id** *ip-address lsr-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1`	(Optional) Specifies a non-default VRF. Specifies the router ID of the local node. • In Cisco IOS XR software, the router ID is specified as an interface name or IP address. By default, LDP uses the global router ID (configured by the global router ID process).

Step 4	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# interface tunnel-te 12001`
	`RP/0/RSP0/CPU0:router(config-ldp-if)#`
		Enters interface configuration mode for the LDP protocol. Interface type must be Tunnel-TE.

Step 5	**commit**	
Step 6	(Optional) **show mpls ldp discovery** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp discovery`	Displays the status of the LDP discovery process. This command, without an interface filter, generates a list of interfaces over which the LDP discovery process is running. The output information contains the state of the link (xmt/rcv hellos), local LDP identifier, the discovered peer's LDP identifier, and holdtime values.
Step 7	(Optional) **show mpls ldp vrf** *vrf-name* **discovery** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red discovery`	Displays the status of the LDP discovery process for the specified VRF.
Step 8	(Optional) **show mpls ldp vrf all discovery summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery summary`	Displays the summarized status of the LDP discovery process for all VRFs.
Step 9	(Optional) **show mpls ldp vrf all discovery brief** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery brief`	Displays the brief status of the LDP discovery process for all VRFs.
Step 10	(Optional) **show mpls ldp vrf all ipv4 discovery summary** **Example:**	Displays the summarized status of the LDP discovery process for all VRFs for the IPv4 address family.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router# show mpls ldp vrf all ipv4 discovery summary`	
Step 11	(Optional) **show mpls ldp discovery summary all** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp discovery summary all`	Displays the aggregate summary across all the LDP discovery processes.

Related Topics

LDP Control Plane, on page 7
Configuring LDP Link: Example, on page 102

Configuring LDP Discovery for Active Targeted Hellos

Perform this task to configure LDP discovery for active targeted hellos.

Note The active side for targeted hellos initiates the unicast hello toward a specific destination.

Before you begin

These prerequisites are required to configure LDP discovery for active targeted hellos:

- Stable router ID is required at either end of the targeted session. If you do not assign a router ID to the routers, the system will default to the global router ID. Please note that default router IDs are subject to change and may cause an unstable discovery.
- One or more MPLS Traffic Engineering tunnels are established between non-directly connected LSRs.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **router-id** *ip-address lsr-id*
4. **interface** *type interface-path-id*
5. **commit**
6. (Optional) **show mpls ldp discovery**
7. (Optional) **show mpls ldp vrf** *vrf-name* **discovery**
8. (Optional) **show mpls ldp vrf all discovery summary**
9. (Optional) **show mpls ldp vrf all discovery brief**
10. (Optional) **show mpls ldp vrf all ipv4 discovery summary**
11. (Optional) **show mpls ldp discovery summary all**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	[**vrf** *vrf-name*] **router-id** *ip-address lsr-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1`	(Optional) Specifies a non-default VRF. Specifies the router ID of the local node. In Cisco IOS XR software, the router ID is specified as an interface name or IP address or LSR ID. By default, LDP uses the global router ID (configured by global router ID process).
Step 4	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# interface tunnel-te 12001`	Enters interface configuration mode for the LDP protocol.
Step 5	**commit**	
Step 6	(Optional) **show mpls ldp discovery** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp discovery`	Displays the status of the LDP discovery process. This command, without an interface filter, generates a list of interfaces over which the LDP discovery process is running. The output information contains the state of the link (xmt/rcv hellos), local LDP identifier, the discovered peer's LDP identifier, and holdtime values.
Step 7	(Optional) **show mpls ldp vrf** *vrf-name* **discovery** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red discovery`	Displays the status of the LDP discovery process for the specified VRF.
Step 8	(Optional) **show mpls ldp vrf all discovery summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery summary`	Displays the summarized status of the LDP discovery process for all VRFs.
Step 9	(Optional) **show mpls ldp vrf all discovery brief** **Example:**	Displays the brief status of the LDP discovery process for all VRFs.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery brief`	
Step 10	(Optional) **show mpls ldp vrf all ipv4 discovery summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all ipv4 discovery summary`	Displays the summarized status of the LDP discovery process for all VRFs for the IPv4 address family.
Step 11	(Optional) **show mpls ldp discovery summary all** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp discovery summary all`	Displays the aggregate summary across all the LDP discovery processes.

Related Topics

LDP Control Plane, on page 7
Configuring LDP Discovery for Targeted Hellos: Example, on page 102

Configuring LDP Discovery for Passive Targeted Hellos

Perform this task to configure LDP discovery for passive targeted hellos.

A passive side for targeted hello is the destination router (tunnel tail), which passively waits for an incoming hello message. Because targeted hellos are unicast, the passive side waits for an incoming hello message to respond with hello toward its discovered neighbor.

Before you begin

Stable router ID is required at either end of the link to ensure that the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **router-id** *ip-address lsr-id*
4. **discovery targeted-hello accept**
5. **commit**
6. (Optional) **show mpls ldp discovery**
7. (Optional) **show mpls ldp vrf** *vrf-name* **discovery**
8. (Optional) **show mpls ldp vrf all discovery summary**
9. (Optional) **show mpls ldp vrf all discovery brief**
10. (Optional) **show mpls ldp vrf all ipv4 discovery summary**
11. (Optional) **show mpls ldp discovery summary all**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	[**vrf** *vrf-name*] **router-id** *ip-address lsr-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# router-id 192.168.70.1`	(Optional) Specifies a non-default VRF. Specifies the router ID of the local node. • In Cisco IOS XR software, the router ID is specified as an interface IP address or LSR ID. By default, LDP uses the global router ID (configured by global router ID process).
Step 4	**discovery targeted-hello accept** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# discovery targeted-hello accept`	Directs the system to accept targeted hello messages from any source and activates passive mode on the LSR for targeted hello acceptance. • This command is executed on the receiver node (with respect to a given MPLS TE tunnel). • You can control the targeted-hello acceptance using the **discovery targeted-hello accept** command.
Step 5	**commit**	
Step 6	(Optional) **show mpls ldp discovery** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp discovery`	Displays the status of the LDP discovery process. This command, without an interface filter, generates a list of interfaces over which the LDP discovery process is running. The output information contains the state of the link (xmt/rcv hellos), local LDP identifier, the discovered peer's LDP identifier, and holdtime values.
Step 7	(Optional) **show mpls ldp vrf** *vrf-name* **discovery** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red discovery`	Displays the status of the LDP discovery process for the specified VRF.
Step 8	(Optional) **show mpls ldp vrf all discovery summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery summary`	Displays the summarized status of the LDP discovery process for all VRFs.

	Command or Action	Purpose
Step 9	(Optional) **show mpls ldp vrf all discovery brief** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all discovery brief`	Displays the brief status of the LDP discovery process for all VRFs.
Step 10	(Optional) **show mpls ldp vrf all ipv4 discovery summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all ipv4 discovery summary`	Displays the summarized status of the LDP discovery process for all VRFs for the IPv4 address family.
Step 11	(Optional) **show mpls ldp discovery summary all** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp discovery summary all`	Displays the aggregate summary across all the LDP discovery processes.

Related Topics

LDP Control Plane, on page 7
Configuring LDP Discovery for Targeted Hellos: Example, on page 102

Configuring Label Advertisement Control (Outbound Filtering)

Perform this task to configure label advertisement (outbound filtering).

By default, a label switched router (LSR) advertises all incoming label prefixes to each neighboring router. You can control the exchange of label binding information using the **mpls ldp label advertise** command. Using the optional keywords, you can advertise selective prefixes to all neighbors, advertise selective prefixes to defined neighbors, or disable label advertisement to all peers for all prefixes.

Note Prefixes and peers advertised selectively are defined in the access list.

Before you begin

Before configuring label advertisement, enable LDP and configure an access list.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **address-family** { **ipv4** | **ipv6**}
4. **label local advertise** [**to** *ldp-id* **for** *prefix-acl* | **interface** *type interface-path-id*]
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.

Step 3	[**vrf** *vrf-name*] **address-family** { **ipv4** | **ipv6**}
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv4`
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`
		(Optional) Specifies a non-default VRF.
		Enables the LDP IPv4 or IPv6 address family.

Step 4	**label local advertise** [**to** *ldp-id* **for** *prefix-acl* | **interface** *type interface-path-id*]
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp-af)# label local advertise to 10.0.0.1:0 for pfx_acl1`
	`RP/0/RSP0/CPU0:router(config-ldp-af)# label local advertise interface POS 0/1/0/0`
		Configures outbound label advertisement control by specifying one of the following options:
		interface
		Specifies an interface for label advertisement.
		to ***ldp-id***
		for ***prefix-acl***
		Specifies neighbors to advertise and receive label advertisements.

Step 5	**commit**	

Related Topics

Label Advertisement Control (Outbound Filtering), on page 13
Configuring Label Advertisement (Outbound Filtering): Example, on page 103

Setting Up LDP Neighbors

Perform this task to set up LDP neighbors.

Before you begin

Stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **interface** *type interface-path-id*
4. **address-family** {**ipv4** | **ipv6** }
5. **discovery transport-address** [*ip-address* | **interface**]
6. **exit**
7. **holdtime** *seconds*
8. [**vrf** *vrf-name*] **neighbor** *ldp-id* **password** [**encrypted**] *password*
9. **backoff** *initial maximum*
10. **commit**
11. (Optional) **show mpls ldp neighbor**
12. (Optional) **show mpls ldp vrf** *vrf-name* **neighbor**
13. (Optional) **show mpls ldp vrf all neighbor brief**
14. (Optional) **clear mpls ldp neighbor**
15. (Optional) **clear mpls ldp vrf all neighbor**
16. (Optional) **clear mpls ldp vrf** *vrf-name* **neighbor**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# interface POS 0/1/0/0`	Enters interface configuration mode for the LDP protocol.

Step 4	**address-family** {**ipv4**	**ipv6** }
		Example:
		`RP/0/RSP0/CPU0:router(config-ldp-if)# address-family ipv4`
		or
		`RP/0/RSP0/CPU0:router(config-ldp-if)# address-family ipv6`
			Enables the LDP IPv4 or IPv6 address family.

	Command or Action	Purpose

Step 5	**discovery transport-address** [*ip-address* | **interface**]
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp-if-af)# discovery transport-address 192.168.1.42`
	`RP/0/RSP0/CPU0:router(config-ldp-if-af)# discovery transport-address 5:6::78`
	or
	`RP/0/RSP0/CPU0:router(config-ldp-if-af)# discovery transport-address interface`
		Provides an alternative transport address for a TCP connection.
		• Default transport address advertised by an LSR (for TCP connections) to its peer is the router ID.
		• Transport address configuration is applied for a given LDP-enabled interface.
		• If the interface version of the command is used, the configured IP address of the interface is passed to its neighbors as the transport address.

Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-if)# exit`	Exits the current configuration mode.
Step 7	**holdtime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# holdtime 30`	Changes the time for which an LDP session is maintained in the absence of LDP messages from the peer. • Outgoing keepalive interval is adjusted accordingly (to make three keepalives in a given holdtime) with a change in session holdtime value. • Session holdtime is also exchanged when the session is established. • In this example holdtime is set to 30 seconds, which causes the peer session to timeout in 30 seconds, as well as transmitting outgoing keepalive messages toward the peer every 10 seconds.
Step 8	[**vrf** *vrf-name*] **neighbor** *ldp-id* **password** [**encrypted**] *password* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# neighbor 192.168.2.44:0 password secretpasswd`	(Optional) Specifies a non-default VRF. Configures password authentication (using the TCP MD5 option) for a given neighbor.
Step 9	**backoff** *initial maximum* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# backoff 10 20`	Configures the parameters for the LDP backoff mechanism. The LDP backoff mechanism prevents two incompatibly configured LSRs from engaging in an unthrottled sequence of session setup failures. If a session setup attempt fails due to such incompatibility, each LSR delays its next attempt (backs off), increasing the delay exponentially with each successive failure until the maximum backoff delay is reached.
Step 10	**commit**	

	Command or Action	Purpose
Step 11	(Optional) **show mpls ldp neighbor** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp neighbor`	Displays the status of the LDP session with its neighbors. This command can be run with various filters as well as with the brief option.
Step 12	(Optional) **show mpls ldp vrf** *vrf-name* **neighbor** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red neighbor`	Displays the status of the LDP session with its neighbors for the specified VRF. This command can be run with the brief option.
Step 13	(Optional) **show mpls ldp vrf all neighbor brief** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all neighbor brief`	Displays the brief LDP session neighbor information for all VRFs.
Step 14	(Optional) **clear mpls ldp neighbor** **Example:** `RP/0/RSP0/CPU0:router# clear mpls ldp neighbor`	Resets an LDP session.
Step 15	(Optional) **clear mpls ldp vrf all neighbor** **Example:** `RP/0/RSP0/CPU0:router# clear mpls ldp vrf all neighbor`	Resets LDP session for all VRFs.
Step 16	(Optional) **clear mpls ldp vrf** *vrf-name* **neighbor** **Example:** `RP/0/RSP0/CPU0:router# clear mpls ldp vrf red neighbor`	Resets LDP session for the specified VRF.

Related Topics

Configuring LDP Neighbors: Example, on page 104

Setting Up LDP Forwarding

Perform this task to set up LDP forwarding.

By default, the LDP control plane implements the penultimate hop popping (PHOP) mechanism. The PHOP mechanism requires that label switched routers use the implicit-null label as a local label for the given Forwarding Equivalence Class (FEC) for which LSR is the penultimate hop. Although PHOP has certain advantages, it may be required to extend LSP up to the ultimate hop under certain circumstances (for example, to propagate MPL QoS). This is done using a special local label (explicit-null) advertised to the peers after which the peers use this label when forwarding traffic toward the ultimate hop (egress LSR).

Before you begin

Stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **address-family** {**ipv4** | **ipv6** }
4. **label local advertise explicit-null**
5. **commit**
6. (Optional) **show mpls ldp forwarding**
7. (Optional) **show mpls ldp vrf all forwarding**
8. (Optional) **show mpls ldp vrf all forwarding summary**
9. (Optional) **show mpls ldp vrf** *vrf-name* **ipv4 forwarding**
10. (Optional) **show mpls ldp forwarding summary all**
11. (Optional) **clear mpls ldp vrf** *vrf-name* **ipv4 forwarding**
12. (Optional) **clear mpls ldp** [**ipv4** | **ipv6**]**forwarding**
13. (Optional) **show mpls ldp afi-all forwarding**
14. (Optional) **show mpls ldp ipv6 forwarding**
15. (Optional) **show mpls forwarding**
16. (Optional) **ping** *ip-address*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.

Step 3	[**vrf** *vrf-name*] **address-family** {**ipv4**	**ipv6** }
		Example:
		`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv4`
		or
		`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`
			(Optional) Specifies a non-default VRF.
			Enables the LDP IPv4 or IPv6 address family.

	Command or Action	Purpose
Step 4	**label local advertise explicit-null** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af)# label local advertise explicit-null`	Causes a router to advertise an explicit null label in situations where it normally advertises an implicit null label (for example, to enable an ultimate-hop disposition instead of PHOP).
Step 5	**commit**	
Step 6	(Optional) **show mpls ldp forwarding** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp forwarding`	Displays the MPLS LDP view of installed forwarding states (rewrites). **Note** For local labels, only up to 12000 rewrites are supported. If the rewrites exceed this limit, MPLS LSD or MPLS LDP or both the processes may crash.
Step 7	(Optional) **show mpls ldp vrf all forwarding** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all forwarding`	Displays the forwarding setup information of all LDP configured VRFs.
Step 8	(Optional) **show mpls ldp vrf all forwarding summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all forwarding summary`	Displays the forwarding setup summary of all LDP configured VRFs.
Step 9	(Optional) **show mpls ldp vrf** *vrf-name* **ipv4 forwarding** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red ipv4 forwarding`	Displays the forwarding setup information for the specified VRF for IPv4.
Step 10	(Optional) **show mpls ldp forwarding summary all** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp forwarding summary all`	Displays the aggregate summary across LDP processes and all VRFs.
Step 11	(Optional) **clear mpls ldp vrf** *vrf-name* **ipv4 forwarding** **Example:** `RP/0/RSP0/CPU0:router# clear mpls ldp vrf red ipv4 forwarding`	Resets the MPLS forwarding rewrites for the specified VRF for IPv4.
Step 12	(Optional) **clear mpls ldp** [**ipv4** | **ipv6**]**forwarding** **Example:**	Resets the MPLS forwarding rewrites for either IPv4 or IPv6 addresses.

	Command or Action	Purpose

	`RP/0/RSP0/CPU0:router# clear mpls ldp ipv4 forwarding`
	or
	`RP/0/RSP0/CPU0:router# clear mpls ldp ipv6 forwarding`	

Step 13	(Optional) **show mpls ldp afi-all forwarding** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp afi-all forwarding`	Displays the forwarding setup information of all address families.
Step 14	(Optional) **show mpls ldp ipv6 forwarding** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp ipv6 forwarding`	Displays the MPLS LDP view of installed forwarding states (rewrites) for IPv6.
Step 15	(Optional) **show mpls forwarding** **Example:** `RP/0/RSP0/CPU0:router# show mpls forwarding`	Displays a global view of all MPLS installed forwarding states (rewrites) by various applications (LDP, TE, and static).
Step 16	(Optional) **ping** *ip-address* **Example:** `RP/0/RSP0/CPU0:router# ping 192.168.2.55`	Checks for connectivity to a particular IP address (going through MPLS LSP as shown in the **show mpls forwarding** command).

Related Topics

LDP Forwarding, on page 8
Configuring LDP Forwarding: Example, on page 104

Configuring Global Transport Address

Perform this task to configure global transport address for the IPv4 address family.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **address-family ipv4**
4. **discovery transport-address** *ip-address*
5. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv4`	Enables LDP IPv4 address family.
Step 4	**discovery transport-address** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af)# discovery transport-address 192.168.1.42`	Provides an alternative transport address for a TCP connection. • Default transport address advertised by an LSR (for TCP connections) to its peer is the router ID.

Step 5	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Setting Up LDP NSF Using Graceful Restart

Perform this task to set up NSF using LDP graceful restart.

LDP graceful restart is a way to enable NSF for LDP. The correct way to set up NSF using LDP graceful restart is to bring up LDP neighbors (link or targeted) with additional configuration related to graceful restart.

Before you begin

Stable router ID is required at either end of the link to ensure the link discovery (and session setup) is successful. If you do not assign a router ID to the routers, the system will default to the global router ID. Default router IDs are subject to change and may cause an unstable discovery.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **interface** *type interface-path-id*
4. **exit**
5. **graceful-restart**
6. **graceful-restart forwarding-state-holdtime** *seconds*
7. **graceful-restart reconnect-timeout** *seconds*
8. **commit**
9. (Optional) **show mpls ldp** [**vrf** *vrf-name*] **parameters**
10. (Optional) **show mpls ldp neighbor**
11. (Optional) **show mpls ldp graceful-restart**
12. (Optional) **show mpls ldp vrf all graceful-restart**
13. (Optional) **show mpls ldp vrf** *vrf-name* **graceful-restart**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.

Step 3	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# interface POS 0/1/0/0`
	`RP/0/RSP0/CPU0:router(config-ldp-if)#`
		Enters interface configuration mode for the LDP protocol.

Step 4	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-if)# exit`	Exits the current configuration mode.

	Command or Action	Purpose
Step 5	**graceful-restart** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart`	Enables the LDP graceful restart feature.
Step 6	**graceful-restart forwarding-state-holdtime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart forwarding-state-holdtime 180`	Specifies the length of time that forwarding can keep LDP-installed forwarding states and rewrites, and specifies wh en the LDP control plane restarts. • After restart of the control plane, when the forwarding state holdtime expires, any previously installed LDP forwarding state or rewrite that is not yet refreshed is deleted from the forwarding. • Recovery time sent after restart is computed as the current remaining value of the forwarding state hold timer.
Step 7	**graceful-restart reconnect-timeout** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart reconnect-timeout 169`	Specifies the length of time a neighbor waits before restarting the node to reconnect before declaring an earlier graceful restart session as down. This command is used to start a timer on the peer (upon a neighbor restart). This timer is referred to as *Neighbor Liveness* timer.
Step 8	**commit**	

Step 9	(Optional) **show mpls ldp** [**vrf** *vrf-name*] **parameters**
	Example:
	`RP/0/RSP0/CPU0:router # show mpls ldp parameters`
	`RP/0/RSP0/CPU0:router # show mpls ldp vrf red parameters`
		Displays all the current MPLS LDP parameters.
		Displays the LDP parameters for the specified VRF.

Step 10	(Optional) **show mpls ldp neighbor** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp neighbor`	Displays the status of the LDP session with its neighbors. This command can be run with various filters as well as with the brief option.
Step 11	(Optional) **show mpls ldp graceful-restart** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp graceful-restart`	Displays the status of the LDP graceful restart feature. The output of this command not only shows states of different graceful restart timers, but also a list of graceful restart neighbors, their state, and reconnect count.

	Command or Action	Purpose
Step 12	(Optional) **show mpls ldp vrf all graceful-restart** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all graceful-restart`	Displays the status of the LDP graceful restart for all VRFs.
Step 13	(Optional) **show mpls ldp vrf** *vrf-name* **graceful-restart** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red graceful-restart`	Displays the status of the LDP graceful restart for the specified VRF.

Related Topics

LDP Graceful Restart, on page 9
Phases in Graceful Restart, on page 11
Recovery with Graceful-Restart, on page 11
Configuring LDP Nonstop Forwarding with Graceful Restart: Example, on page 104

Configuring Label Acceptance Control (Inbound Filtering)

Perform this task to configure LDP inbound label filtering.

Note By default, there is no inbound label filtering performed by LDP and thus an LSR accepts (and retains) all remote label bindings from all peers.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **label accept for** *prefix-acl* **from** *ip-address*
4. [**vrf** *vrf-name*] **address-family** { **ipv4** | **ipv6**}
5. **label remote accept from** *ldp-id* **for** *prefix-acl*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:**	Enters the MPLS LDP configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# mpls ldp`	

Step 3	**label accept for** *prefix-acl* **from** *ip-address*
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# label accept for pfx_acl_1 from 192.168.1.1`
	`RP/0/RSP0/CPU0:router(config-ldp)# label accept for pfx_acl_2 from 192.168.2.2`
		Configures inbound label acceptance for prefixes specified by prefix-acl from neighbor (as specified by its IP address).

Step 4	[**vrf** *vrf-name*] **address-family** { **ipv4** | **ipv6**}
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv4`
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`
		(Optional) Specifies a non-default VRF.
		Enables the LDP IPv4 or IPv6 address family.

Step 5	**label remote accept from** *ldp-id* **for** *prefix-acl* **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af)# label remote accept from 192.168.1.1:0 for pfx_acl_1`	Configures inbound label acceptance control for prefixes specified by prefix-acl from neighbor (as specified by its LDP ID).
Step 6	**commit**	

Related Topics

Label Acceptance Control (Inbound Filtering), on page 13
Configuring Label Acceptance (Inbound Filtering): Example, on page 105

Configuring Local Label Allocation Control

Perform this task to configure label allocation control.

Note By default, local label allocation control is disabled and all non-BGP prefixes are assigned local labels.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **address-family** { **ipv4** | **ipv6**}
4. **label local allocate for** *prefix-acl*

5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters the MPLS LDP configuration mode.

Step 3	[**vrf** *vrf-name*] **address-family** { **ipv4** | **ipv6**}
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv4`
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`
		(Optional) Specifies a non-default VRF.
		Enables the LDP IPv4 or IPv6 address family.

Step 4	**label local allocate for** *prefix-acl* **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af)# label local allocate for pfx_acl_1`	Configures label allocation control for prefixes as specified by prefix-acl.
Step 5	**commit**	

Related Topics

Local Label Allocation Control, on page 13
Configuring Local Label Allocation Control: Example, on page 105

Configuring Session Protection

Perform this task to configure LDP session protection.

By default, there is no protection is done for link sessions by means of targeted hellos.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **session protection** [**for** *peer-acl*] [**duration** *seconds*]
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters the MPLS LDP configuration mode.
Step 3	**session protection** [**for** *peer-acl*] [**duration** *seconds*] **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# session protection for peer_acl_1 duration 60`	Configures LDP session protection for peers specified by peer-acl with a maximum duration, in seconds.
Step 4	**commit**	

Related Topics

Session Protection, on page 14
Configuring LDP Session Protection: Example, on page 105

Configuring LDP IGP Synchronization: OSPF

Perform this task to configure LDP IGP Synchronization under OSPF.

Note By default, there is no synchronization between LDP and IGPs.

SUMMARY STEPS

1. **configure**
2. **router ospf** *process-name*
3. (Optional) **vrf** *vrf-name*
4. Use one of the following commands:
   - **mpls ldp sync**
   - **area** *area-id* **mpls ldp sync**
   - **area** *area-id* **interface** *name* **mpls ldp sync**
5. (Optional) Use one of the following commands:
   - **mpls ldp sync**
   - **area** *area-id* **mpls ldp sync**
   - **area** *area-id* **interface** *name* **mpls ldp sync**

6. **commit**
7. (Optional) **show mpls ldp vrf** *vrf-name* **ipv4 igp sync**
8. (Optional) **show mpls ldp vrf all ipv4 igp sync**
9. (Optional) **show mpls ldp** { **ipv4** | **ipv6** }**igp sync**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router ospf** *process-name* **Example:** `RP/0/RSP0/CPU0:router(config)# router ospf 100`	Identifies the OSPF routing process and enters OSPF configuration mode.
Step 3	(Optional) **vrf** *vrf-name* **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# vrf red`	Specifies the non-default VRF.
Step 4	Use one of the following commands: • **mpls ldp sync** • **area** *area-id* **mpls ldp sync** • **area** *area-id* **interface** *name* **mpls ldp sync** **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# mpls ldp sync`	Enables LDP IGP synchronization on an interface.

Step 5	(Optional) Use one of the following commands:
	• **mpls ldp sync**
	• **area** *area-id* **mpls ldp sync**
	• **area** *area-id* **interface** *name* **mpls ldp sync**
	Example:
	`RP/0/RSP0/CPU0:router(config-ospf-vrf)# mpls ldp sync`
	`RP/0/RSP0/CPU0:router(config-ospf-vrf)# area 1 mpls ldp sync`
	`RP/0/RSP0/CPU0:router(config-ospf-vrf)# area 1 interface POS 0/2/0/0 mpls ldp sync`
		Enables LDP IGP synchronization on an interface for the specified VRF.

	Command or Action	Purpose
Step 6	**commit**	
Step 7	(Optional) **show mpls ldp vrf** *vrf-name* **ipv4 igp sync** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red ipv4 igp sync`	Displays the LDP IGP synchronization information for the specified VRF for address family IPv4.
Step 8	(Optional) **show mpls ldp vrf all ipv4 igp sync** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all ipv4 igp sync`	Displays the LDP IGP synchronization information for all VRFs for address family IPv4.

Step 9	(Optional) **show mpls ldp** { **ipv4** | **ipv6** }**igp sync**
	Example:
	`RP/0/RSP0/CPU0:router# show mpls ldp ipv4 igp sync`
	`RP/0/RSP0/CPU0:router# show mpls ldp ipv6 igp sync`
		Displays the LDP IGP synchronization information for IPv4 or IPv6 address families.

Related Topics

IGP Synchronization, on page 15
Configuring LDP IGP Synchronization—OSPF: Example, on page 106

Disabling LDP IGP Synchronization: OSPF

Perform this task to disable LDP IGP Synchronization under OSPF.

You can disable LDP IGP synchronization on a per-interface basis. This lets LDP enable all IGP interfaces except those that are explicitly disabled.

SUMMARY STEPS

1. **configure**
2. **router ospf** *process-name*
3. (Optional) **vrf** *vrf-name*
4. Use one of the following commands:
   - **area** *area-id* **mpls ldp sync disable**
   - **area** *area-id* **interface** *name* **mpls ldp sync disable**
5. (Optional) Use one of the following commands:
   - **area** *area-id* **mpls ldp sync disable**
   - **area** *area-id* **interface** *name* **mpls ldp sync disable**

6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router ospf** *process-name* **Example:** `RP/0/RSP0/CPU0:router(config)# router ospf 109`	Identifies the OSPF routing process and enters OSPF configuration mode.
Step 3	(Optional) **vrf** *vrf-name* **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# vrf red`	Specifies the non-default VRF.

Step 4	Use one of the following commands:
	• **area** *area-id* **mpls ldp sync disable**
	• **area** *area-id* **interface** *name* **mpls ldp sync disable**
	Example:
	`RP/0/RSP0/CPU0:router(config-ospf)# area 1 mpls ldp sync disable`
	`RP/0/RSP0/CPU0:router(config-ospf)# area 1 interface POS 0/2/0/0 mpls ldp sync disable`
		Disables LDP IGP synchronization on an interface.

Step 5	(Optional) Use one of the following commands:
	• **area** *area-id* **mpls ldp sync disable**
	• **area** *area-id* **interface** *name* **mpls ldp sync disable**
	Example:
	`RP/0/RSP0/CPU0:router(config-ospf-vrf)# area 1 mpls ldp sync disable`
	`RP/0/RSP0/CPU0:router(config-ospf-vrf)# area 1 interface POS 0/2/0/0 mpls ldp sync disable`
		Disables LDP IGP synchronization on an interface for the specified VRF.

Step 6	**commit**	

Configuring LDP IGP Synchronization: ISIS

Perform this task to configure LDP IGP Synchronization under ISIS.

Note By default, there is no synchronization between LDP and ISIS.

SUMMARY STEPS

1. **configure**
2. **router isis** *instance-id*
3. **interface** *type interface-path-id*
4. **address-family** {**ipv4** | **ipv6**} **unicast**
5. **mpls ldp sync**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**router isis** *instance-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# router isis 100`
	`RP/0/RSP0/CPU0:router(config-isis)#`
		Enables the Intermediate System-to-Intermediate System (IS-IS) routing protocol and defines an IS-IS instance.

Step 3	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-isis)# interface POS 0/2/0/0`
	`RP/0/RSP0/CPU0:router(config-isis-if)#`
		Configures the IS-IS protocol on an interface and enters ISIS interface configuration mode.

Step 4	**address-family** {**ipv4**	**ipv6**} **unicast**
		Example:
		`RP/0/RSP0/CPU0:router(config-isis-if)#`
		`address-family ipv4 unicast`
		`RP/0/RSP0/CPU0:router(config-isis-if-af)#`
		
		`RP/0/RSP0/CPU0:router(config-isis-if)#`
		`address-family ipv6 unicast`
		`RP/0/RSP0/CPU0:router(config-isis-if-af)#`
			Enters address family configuration mode for configuring IS-IS routing for a standard IP version 4 (IPv4) or IP version 6 (IPv6) address prefix.

	Command or Action	Purpose
Step 5	**mpls ldp sync** **Example:** `RP/0/RSP0/CPU0:router(config-isis-if-af)# mpls ldp sync`	Enables LDP IGP synchronization.
Step 6	**commit**	

Related Topics

IGP Synchronization, on page 15
Configuring LDP IGP Synchronization—ISIS: Example, on page 106

Enabling LDP Auto-Configuration for a Specified OSPF Instance

Perform this task to enable IGP auto-configuration globally for a specified OSPF process name.

You can disable auto-configuration on a per-interface basis. This lets LDP enable all IGP interfaces except those that are explicitly disabled.

Note This feature is supported for IPv4 unicast family in default VRF only.

SUMMARY STEPS

1. **configure**
2. **router ospf** *process-name*
3. **mpls ldp auto-config**
4. **area** *area-id*
5. **interface** *type interface-path-id*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**router ospf** *process-name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# router ospf 190`
	`RP/0/RSP0/CPU0:router(config-ospf)#`
		Enters a uniquely identifiable OSPF routing process. The process name is any alphanumeric string no longer than 40 characters without spaces.

	Command or Action	Purpose
Step 3	**mpls ldp auto-config** **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# mpls ldp auto-config`	Enables LDP auto-configuration.
Step 4	**area** *area-id* **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# area 8`	Configures an OSPF area and identifier. ***area-id*** Either a decimal value or an IP address.
Step 5	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ospf-ar)# interface pos 0/6/0/0`	Enables LDP auto-configuration on the specified interface. **Note** LDP configurable limit for maximum number of interfaces does not apply to IGP auto-configuration interfaces.
Step 6	**commit**	

Related Topics

IGP Auto-configuration, on page 15
Configuring LDP Auto-Configuration: Example, on page 106
Disabling LDP Auto-Configuration, on page 67

Enabling LDP Auto-Configuration in an Area for a Specified OSPF Instance

Perform this task to enable IGP auto-configuration in a defined area with a specified OSPF process name.

You can disable auto-configuration on a per-interface basis. This lets LDP enable all IGP interfaces except those that are explicitly disabled.

Note This feature is supported for IPv4 unicast family in default VRF only.

SUMMARY STEPS

1. **configure**
2. **router ospf** *process-name*
3. **area** *area-id*
4. **mpls ldp auto-config**
5. **interface** *type interface-path-id*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**router ospf** *process-name*
	Example:
	`RP/0/RSP0/CPU0:router(config)# router ospf 100`
	`RP/0/RSP0/CPU0:router(config-ospf)#`
		Enters a uniquely identifiable OSPF routing process. The process name is any alphanumeric string no longer than 40 characters without spaces.

Step 3	**area** *area-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-ospf)# area 8`
	`RP/0/RSP0/CPU0:router(config-ospf-ar)#`
		Configures an OSPF area and identifier.
		area-id
		Either a decimal value or an IP address.

Step 4	**mpls ldp auto-config** **Example:** `RP/0/RSP0/CPU0:router(config-ospf-ar)# mpls ldp auto-config`	Enables LDP auto-configuration.

Step 5	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-ospf-ar)# interface pos 0/6/0/0`
	`RP/0/RSP0/CPU0:router(config-ospf-ar-if)`
		Enables LDP auto-configuration on the specified interface. The LDP configurable limit for maximum number of interfaces does not apply to IGP auto-config interfaces.

Step 6	**commit**	

Related Topics

IGP Auto-configuration, on page 15
Configuring LDP Auto-Configuration: Example, on page 106
Disabling LDP Auto-Configuration, on page 67

Disabling LDP Auto-Configuration

Perform this task to disable IGP auto-configuration.

You can disable auto-configuration on a per-interface basis. This lets LDP enable all IGP interfaces except those that are explicitly disabled.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**

3. **interface** *type interface-path-id*
4. **igp auto-config disable**
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**mpls ldp**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls ldp`
	`RP/0/RSP0/CPU0:router(config-ldp)#`
		Enters the MPLS LDP configuration mode.

Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# interface pos 0/6/0/0`	Enters interface configuration mode and configures an interface.
Step 4	**igp auto-config disable** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-if)# igp auto-config disable`	Disables auto-configuration on the specified interface.
Step 5	**commit**	

Related Topics

IGP Auto-configuration, on page 15
Configuring LDP Auto-Configuration: Example, on page 106

Configuring LDP Nonstop Routing

Perform this task to configure LDP NSR.

Note By default, NSR is globally-enabled on all LDP sessions except AToM.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **nsr**

4. **commit**
5. (Optional) **show mpls ldp** [**vrf** *vrf-name*] **nsr statistics**
6. (Optional) **show mpls ldp vrf** *vrf-name* **nsr statistics neighbor**
7. (Optional) **show mpls ldp** [**vrf** *vrf-name*] **nsr summary**
8. (Optional) **show mpls ldp** [**vrf** *vrf-name*] **nsr pending**
9. (Optional) **show mpls ldp vrf** *vrf-name* **nsr pending neighbor**
10. (Optional) **show mpls ldp vrf all nsr summary**
11. (Optional) **show mpls ldp nsr summary all**
12. (Optional) **clear mpls ldp vrf** *vrf-name* **nsr statistics neighbor**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters the MPLS LDP configuration mode.
Step 3	**nsr** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# nsr`	Enables LDP nonstop routing.
Step 4	**commit**	

Step 5	(Optional) **show mpls ldp** [**vrf** *vrf-name*] **nsr statistics**
	Example:
	`RP/0/RSP0/CPU0:router# show mpls ldp nsr statistics`
	`RP/0/RSP0/CPU0:router# show mpls ldp vrf red nsr statistics`
		Displays MPLS LDP NSR statistics.
		Displays LDP NSR statistics for the specified VRF.

Step 6	(Optional) **show mpls ldp vrf** *vrf-name* **nsr statistics neighbor** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red nsr statistics neighbor 10.0.0.1`	Displays LDP NSR statistics for the specified VRF for a given neighbor.
Step 7	(Optional) **show mpls ldp** [**vrf** *vrf-name*] **nsr summary** **Example:**	Displays MPLS LDP NSR summarized information. Displays LDP NSR summarized information for the specified VRF.

	Command or Action	Purpose

	`RP/0/RSP0/CPU0:router# show mpls ldp nsr summary`
	
	`RP/0/RSP0/CPU0:router# show mpls ldp vrf red nsr summary`	

Step 8	(Optional) **show mpls ldp** [**vrf** *vrf-name*] **nsr pending**
	Example:
	`RP/0/RSP0/CPU0:router# show mpls ldp nsr pending`
	
	`RP/0/RSP0/CPU0:router# show mpls ldp vrf red nsr pending`
		Displays MPLS LDP NSR pending information.
		Displays LDP NSR pending information for the specified VRF.

Step 9	(Optional) **show mpls ldp vrf** *vrf-name* **nsr pending neighbor** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf red nsr pending neighbor 172.16.0.1`	Displays LDP NSR pending information for the specified VRF for a given neighbor.
Step 10	(Optional) **show mpls ldp vrf all nsr summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp vrf all nsr summary`	Displays all LDP configured VRF (including default VRF) summarized information.
Step 11	(Optional) **show mpls ldp nsr summary all** **Example:** `RP/0/RSP0/CPU0:router# show mpls ldp nsr summary all`	Displays aggregate summary across LDP processes and all VRFs.
Step 12	(Optional) **clear mpls ldp vrf** *vrf-name* **nsr statistics neighbor** **Example:** `RP/0/RSP0/CPU0:router# clear mpls ldp vrf red nsr statistics neighbor`	Resets LDP NSR statistics for the specified VRF for neighbor.

Related Topics

LDP Nonstop Routing, on page 16

Configuring LDP Downstream on Demand mode

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name* **session**] **downstream-on-demand**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	[**vrf** *vrf-name* **session**] **downstream-on-demand** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# vrf red session downstream-on-demand with ABC`	(Optional) Enters downstream on demand label advertisement mode under the specified non-default VRF. Enters downstream on demand label advertisement mode. The ACL contains the list of peer IDs that are configured for downstream-on-demand mode. When the ACL is changed or configured, the list of established neighbor is traversed.
Step 4	**commit**	

Related Topics

Downstream on Demand, on page 18

Setting Up Implicit-Null-Override Label

Perform this task to configure implicit-null label for non-egress prefixes.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. [**vrf** *vrf-name*] **address-family** {**ipv4** | **ipv6** }
4. **label**
5. **local implicit-null-override for** *access-list*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.

Step 3	[**vrf** *vrf-name*] **address-family** {**ipv4** | **ipv6** }
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv4`
	or
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`
		(Optional) Specifies a non-default VRF.
		Enables the LDP IPv4 or IPv6 address family.

Step 4	**label** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af)# label`	Configures the allocation, advertisement ,and acceptance of labels.
Step 5	**local implicit-null-override for** *access-list* **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af-lbl)# local implicit-null-override for 70`	Configures implicit-null local label for non-egress prefixes. **Note** This feature works with any prefix including static, IGP, and BGP, when specified in the ACL.
Step 6	**commit**	

Redistributing MPLS LDP Routes into BGP

Perform this task to redistribute Border Gateway Protocol (BGP) autonomous system into an MPLS LDP.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **redistribute bgp**
4. **end** or **commit**
5. **show run mpls ldp**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**redistribute bgp** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# redistribute bgp advertise-to acl_1`	Allows the redistribution of BGP routes into an MPLS LDP processes. **Note** Autonomous system numbers (ASNs) are globally unique identifiers used to identify autonomous systems (ASs) and enable ASs to exchange exterior routing information between neighboring ASs. A unique ASN is allocated to each AS for use in BGP routing. ASNs are encoded as 2-byte numbers and 4-byte numbers in BGP.
Step 4	**end** or **commit**	• When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:` • Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. • Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. • Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

	Command or Action	Purpose
Step 5	**show run mpls ldp** **Example:** `RP/0/RSP0/CPU0:router# show run mpls ldp`	Displays information about the redistributed route information.

Enabling MLDP

Perform this task to enable Multicast Label Distribution Protocol (MLDP) in MPLS LDP.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **mldp**
4. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters the MPLS LDP configuration mode.

Step 3	**mldp**
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# mldp`
	`RP/0/RSP0/CPU0:router(config-ldp-mldp)#`
		Enables MLDP.

Step 4	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

	Command or Action	Purpose
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. • Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Enabling MLDP Make-Before-Break

Perform this task to enable the make-before-break (MBB) feature in MPLS MLDP.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **mldp**
4. **address-family ipv4**
5. **make-before-break** [**delay** *seconds*]
6. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**mldp** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# mldp`	Enables MLDP.

	Command or Action	Purpose
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp)# address-family ipv4`	Enables MLDP for IPv4 address family.
Step 5	**make-before-break** [**delay** *seconds*] **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp-af)# make-before-break delay 10`	Enables the make-before-break feature. (Optional) Configures the MBB forwarding delay in seconds. Range is 0 to 600.

Step 6	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Enabling MLDP MoFRR

Perform this task to enable multicast only fast reroute (MoFRR) support in MPLS MLDP.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **mldp**
4. **address-family ipv4**
5. **mofrr**
6. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**mldp** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# mldp`	Enables MLDP.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp)# address-family ipv4`	Enables MLDP for IPv4 address family.
Step 5	**mofrr** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp-af)# mofrr`	Enables MoFRR support.

Step 6	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

	Command or Action	Purpose
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Enabling MLDP Recursive FEC

Perform this task to enable recursive forwarding equivalence class (FEC) support in MPLS MLDP.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **mldp**
4. **address-family ipv4**
5. **recursive-fec**
6. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**mldp** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# mldp`	Enables MLDP.
Step 4	**address-family ipv4** **Example:**	Enables MLDP for IPv4 address family.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-ldp-mldp)# address-family ipv4`	
Step 5	**recursive-fec** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp-af)# recursive-fec`	Enables recursive FEC support.

Step 6	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Enabling MLDP Static Multipoint to Multipoint LSP

Perform this task to enable static multipoint to multipoint (MP2MP) LSP support in MPLS MLDP.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **mldp**
4. **address-family ipv4**
5. **static mp2mp** *ip-address*
6. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**mldp** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# mldp`	Enables MLDP.
Step 4	**address-family ipv4** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp)# address-family ipv4`	Enables MLDP for IPv4 address family.
Step 5	**static mp2mp** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp-af)# static mp2mp 10.10.10.10 1`	Enables static MP2MP LSP support and specifies MP2MP LSP root IP address followed by the number of LSPs in the range 1 to 1000.

Step 6	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

	Command or Action	Purpose
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Enabling MLDP Static Point to Multipoint LSP

Perform this task to enable static point to multipoint (P2MP) LSP support in MPLS MLDP.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **mldp**
4. **address-family ipv4**
5. **static p2mp** *ip-address*
6. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**mldp** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# mldp`	Enables MLDP.
Step 4	**address-family ipv4** **Example:**	Enables MLDP for IPv4 address family.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-ldp-mldp)# address-family ipv4`	
Step 5	**static p2mp** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-ldp-mldp-af)# static p2mp 10.0.0.1 1`	Enables static P2MP LSP support and specifies P2MP LSP root IP address followed by the number of LSPs in the range 1 to 1000.

Step 6	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-mldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Disabling MLDP

Perform this task to disable MLDP on Label Distribution Protocol (LDP) enabled interfaces.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **interface** *type interface-path-id*
4. **address-family** {**ipv4** | **ipv6** }
5. **igp mldp disable**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# interface POS 0/1/0/0`	Enters interface configuration mode for the LDP protocol.

Step 4	**address-family** {**ipv4** | **ipv6** }
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp-if)# address-family ipv4`
	or
	`RP/0/RSP0/CPU0:router(config-ldp-if)# address-family ipv6`
		Enables the LDP IPv4 or IPv6 address family.

Step 5	**igp mldp disable** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-if-af)# igp mldp disable`	Disables MLDP.
Step 6	**commit**	

Controlling State Advertisements In An mLDP-Only Setup

This function explains controlling of state advertisements of non-negotiated Label Distribution Protocol (LDP) applications. This implementation is in conformance with RFC 7473 (Controlling State Advertisements of Non-negotiated LDP Applications).

The main purpose of documenting this function is to use it in a Multipoint LDP (mLDP)-only environment, wherein participating routers don't need to exchange any unicast binding information.

Non-Negotiated LDP Applications

The LDP capabilities framework enables LDP applications' capabilities exchange and negotiation, thereby enabling LSRs to send necessary LDP state. However, for the applications that existed prior to the definition of the framework (called *non-negotiated* LDP applications), there is no capability negotiation done. When an LDP session comes up, an LDP speaker may unnecessarily advertise its local state (without waiting for any capabilities exchange and negotiation). In other words, even when the peer session is established for Multipoint LDP (mLDP), the LSR advertises the state for these early LDP applications.

One example is *IPv4/IPv6 Prefix LSPs Setup* (used to set up Label Switched Paths [LSPs] for IP prefixes). Another example is *L2VPN P2P FEC 128 and FEC 129 PWs Signaling* (an LDP application that signals point-to-point [P2P] Pseudowires [PWs] for Layer 2 Virtual Private Networks [L2VPNs]).

In an mLDP-only setup, you can disable these non-negotiated LDP applications and avoid unnecessary LDP state advertisement. An LDP speaker that only runs mLDP announces to its peer(s) its disinterest (or non-support) in non-negotiated LDP applications. That is, it announces to its peers its disinterest to set up IP Prefix LSPs or to signal L2VPN P2P PW, at the time of session establishment.

Upon receipt of such a capability, the receiving LDP speaker, if supporting the capability, disables the advertisement of the state related to the application towards the sender of the capability. This new capability can also be sent later in a Capability message, either to disable a previously enabled application's state advertisement, or to enable a previously disabled application's state advertisement.

As a result, the flow of LDP state information in an mLDP-only setup is faster. When routers come up after a network event, the network convergence time is fast too.

IP Address Bindings In An mLDP Setup

An LSR typically uses peer IP address(es) to map an IP routing next hop to an LDP peer in order to implement its control plane procedures. mLDP uses a peer's IP address(es) to determine its upstream LSR to reach the root node, and to select the forwarding interface towards its downstream LSR. Hence, in an mLDP-only network, while it is desirable to disable advertisement of label bindings for IP (unicast) prefixes, disabling advertisement of IP address bindings will break mLDP functionality.

Uninteresting State - For the *Prefix-LSP* LDP application, *uninteresting* state refers to any state related to IP Prefix FEC, such as FEC label bindings and LDP Status. IP address bindings are not considered as an *uninteresting* state.

For the P2P-PW application LDP application, *uninteresting* state refers to any state related to P2P PW FEC 128 or FEC 129, such as FEC label bindings, MAC address withdrawal, and LDP PW status.

Control State Advertisement

To control advertisement of *uninteresting* state of non-negotiated LDP applications, the capability parameter TLV *State Advertisement Control Capability* is used. This TLV is only present in the Initialization and Capability messages, and the TLV can hold one or more State Advertisement Control (SAC) Elements.

As an example, consider two LSRs, S (LDP speaker) and P (LDP peer), that support all non-negotiated applications. S is participating (or set to participate) in an mLDP-only setup. Pointers for this scenario:

- By default, the LSRs will advertise state for all LDP applications to their peers, as soon as an LDP session is established.
- The **capabilities sac mldp-only** function is enabled on S.
- P receives an update from S via a Capability message that specifies to disable all four non-negotiated applications states.

- P's outbound policy towards S blocks and disables state for the unneeded applications.
- S only receives mLDP advertisements from specific mLDP-participating peers.

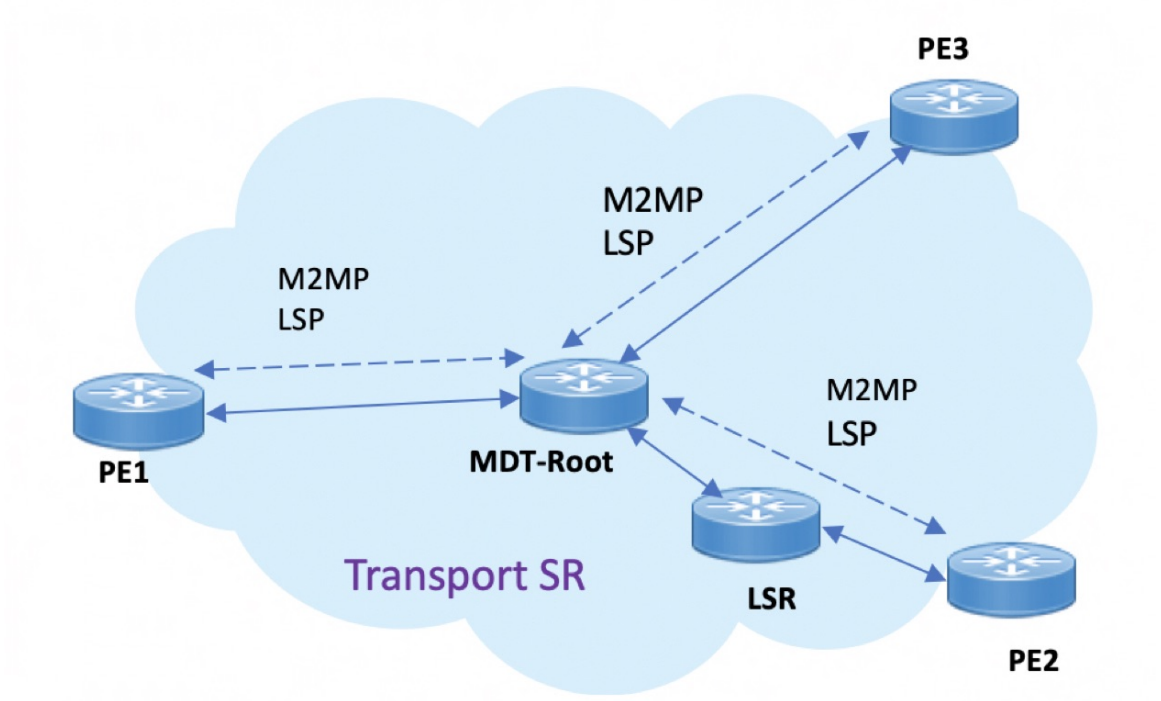
Use Cases For Controlling MLDP State Advertisements

Two use cases are explained, **mLDP-Based MVPN** and **Disable Prefix-LSPs On An L2VPN/PW tLDP Session**.

mLDP-Based MVPN

A sample topology and relevant configurations are noted below.

Figure 9: mLDP-Based MVPN Over Segment Routing



- The topology represents an MVPN profile 1 where an mLDP-based MVPN service is deployed over a Segment Routing core setup
- mLDP is required to signal MP2MP LSPs, whereas SR handles the transport.
- SAC capabilities are used to signal *mLDP-only* capability, which blocks unrequired unicast IPv4, IPv6, FEC128, and FEC129 related label binding advertisements.
- The **mldp-only** option is enabled on PE routers and P routers to remove unwanted advertisements.

Configuration

PE1 Configuration

Configure mLDP SAC capability on PE1.

```
PE1(config)# mpls ldp
PE1(config-ldp)# capabilities sac mldp-only
PE1(config-ldp)# commit
```

PE2 Configuration

Configure mLDP SAC capability on PE2.

```
PE2(config)# mpls ldp
PE2(config-ldp)# capabilities sac mldp-only
PE2(config-ldp)# commit
```

Verification

LDP peers (PE1 and PE2) are configured with **mldp-only** option, disabling all other SAC capabilities.

```
PE1# show running-config mpls ldp

mpls ldp
   capabilities sac mldp-only
   mldp
        address-family ipv4
        !

PE2# show running-config mpls ldp

mpls ldp
   capabilities sac mldp-only
   mldp
        address-family ipv4
        !
```

On PE1, verify PE2's SAC capabilities:

```
PE1# show mpls ldp neighbor 209.165.201.20 capabilities detail

Peer LDP Identifier: 209.165.201.20:0
  Capabilities:
    Sent:
      0x508  (MP: Point-to-Multipoint (P2MP))
      0x509  (MP: Multipoint-to-Multipoint (MP2MP))
      0x50b  (Typed Wildcard FEC)
      0x50d  (State Advertisement Control)
        [ {IPv4-disable}{IPv6-disable}{FEC128-disable}{FEC129-disable} ](length 4)
    Received:
      0x508  (MP: Point-to-Multipoint (P2MP))
      0x509  (MP: Multipoint-to-Multipoint (MP2MP))
      0x50b  (Typed Wildcard FEC)
      0x50d  (State Advertisement Control)
        [ {IPv4-disable}{IPv6-disable}{FEC128-disable}{FEC129-disable} ](length 4)
```

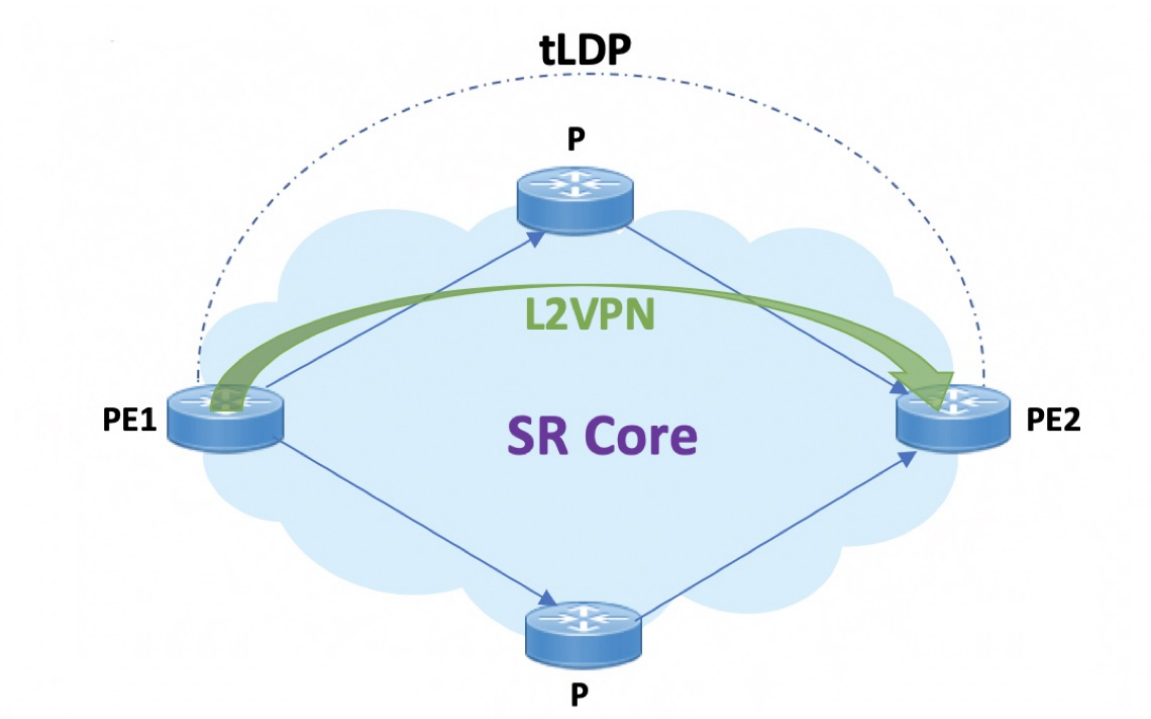
Capabilities Sent shows that **mldp-only** option disables all other advertisements.

Capabilities Received shows that **mldp-only** is enabled on peer PE2 too.

Disable Prefix-LSPs On An L2VPN/PW tLDP Session

A sample topology and relevant configurations are noted below.

Figure 10: L2VPN Xconnect Service Over Segment Routing



- The topology represents an L2VPN Xconnect service over a Segment Routing core setup.
- By default, Xconnect uses tLDP to signal service labels to remote PEs.
- By default, tLDP not only signals the service label, but also known (IPv4 and IPv6) label bindings to the tLDP peer, which is not required.
- The LDP SAC capabilities is an optional configuration enabled under LDP, and users can block IPv4 and IPv6 label bindings by applying configurations on PE1 and PE2.

Configuration

PE1 Configuration

Disable IPv4 prefix LSP binding advertisements on PE1:

```
PE1(config)# mpls ldp capabilities sac ipv4-disable
PE1(config)# commit
```

Disable IPv6-prefix LSP binding advertisements on PE1:

```
PE1(config)# mpls ldp capabilities sac ipv4-disable ipv6-disable
PE1(config)# commit
```

Note Whenever you disable a non-negotiated LDP application state on a router, you must include previously disabled non-negotiated LDP applications too, in the same command line. If not, the latest configuration overwrites the existing ones. You can see that ipv4-disable is added again, though it was already disabled.

PE2 Configuration

Enable SAC capability awareness on PE2, and make PE2 stop sending IPv4 prefix LSP binding advertisements to PE1:

```
PE2(config)#mpls ldp capabilities sac
PE2(config)#commit
```

Verification

On PE1, verify PE2's SAC capabilities:

```
PE1# show mpls ldp neighbor 198.51.100.1 detail

Peer LDP Identifier: 198.51.100.1:0
  TCP connection: 198.51.100.1:29132 - 192.0.2.1:646
  Graceful Restart: No
  Session Holdtime: 180 sec
  State: Oper; Msgs sent/rcvd: 14/14; Downstream-Unsolicited
  Up time: 00:03:30
  LDP Discovery Sources:
    IPv4: (1)
      Targeted Hello (192.0.2.1 -> 198.51.100.1, active)
    IPv6: (0)
  Addresses bound to this peer:
    IPv4: (3)
      203.0.113.1     209.165.201.1    10.0.0.1   198.51.100.1
      172.16.0.1
    IPv6: (0)
  Peer holdtime: 180 sec; KA interval: 60 sec; Peer state: Estab
  NSR: Disabled
  Clients: AToM
  Capabilities:
    Sent:
      0x508  (MP: Point-to-Multipoint (P2MP))
      0x509  (MP: Multipoint-to-Multipoint (MP2MP))
      0x50b  (Typed Wildcard FEC)
      0x50d  (State Advertisement Control)
        [ {IPv4-disable}  ] (length 1)
    Received:
      0x508  (MP: Point-to-Multipoint (P2MP))
      0x509  (MP: Multipoint-to-Multipoint (MP2MP))
      0x50b  (Typed Wildcard FEC)
      0x50d  (State Advertisement Control)
```

Capabilities Sent SAC capability **ipv4-disable** is sent, and local IPv4 label bindings are not generated.

Capabilities Received The peer (PE2) understands SAC capability and won't send its local IPv4 label bindings to local PE.

On PE1, verify SAC capabilities:

```
PE1# show mpls ldp capabilities detail

  Type     Description                                Owner
  ------   ----------------------------------------   ------------
  0x50b    Typed Wildcard FEC                         LDP
     Capability data: None

  0x3eff   Cisco IOS-XR                               LDP
     Capability data:
       Length: 12
       Desc  : [ host=PE1; platform=ASR9000; release=07.01.01 ]
```

```
0x508    MP: Point-to-Multipoint (P2MP)             mLDP
   Capability data: None

0x509    MP: Multipoint-to-Multipoint (MP2MP)       mLDP
   Capability data: None

0x50d    State Advertisement Control                LDP
   Capability data:
     Length: 1
     Desc  : [ {IPv4-disable}  ]

0x703    P2MP PW                                    L2VPN-AToM
   Capability data: None
```

On PE1, verify that local and remote FEC bindings are removed.

```
PE1# show mpls ldp neighbor 198.51.100.1
Wed March 3 13:42:13.359 EDTs
```

LDP IPv6 Configuration

The LDP configuration model is extended to introduce IPv6 as an option under the address family submodes that reside under LDP global and interface configurations. Address family IPv6 is available as a submode under LDP global, LDP VRF global and interface configurations. LDP IPv6 is supported only under default VRF.

Enabling LDP IPv6 Native

Perform this task to enable LDP IPv6 native under LDP.

The user must enable IPv6 address family under LDP submodes.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **address-family ipv6**
4. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**mpls ldp** **Example:**	Enters MPLS LDP configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# mpls ldp`	

Step 3	**address-family ipv6**
	Example:
	`RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`
	`RP/0/RSP0/CPU0:router(config-ldp-af)#`
		Enables native LDP IPv6 address family.

Step 4	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Enabling LDP IPv6 Control Plane

Perform this task to enable LDP IPv6 control plane on an LDP interface.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **interface** *type interface-path-id*
4. **address-family ipv6**
5. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# interface pos 0/6/0/0`	Enters interface configuration mode for the LDP protocol.
Step 4	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-if)# address-family ipv6`	Enables LDP IPv6 control plane.

Step 5	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-if-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-if-af)# commit`
		Note This configuration will be rejected if (mpls-ldp-af) for the given address family is not already enabled.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

	Command or Action	Purpose
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring IPv6-only LSR

Perform this task to configure IPv6-only LSR.

IPv4 is implicitly enabled under default VRF and any LDP interface under default VRF. In order to operate as an IPv6-only LSR, the user must also explicitly disable IPv4 address family.

SUMMARY STEPS

1. **configure**
2. **interface loopback** *number*
3. **ipv6 address** *prefix*
4. **exit**
5. **interface** *type interface-path-id*
6. **ipv6 address** *prefix*
7. **exit**
8. **router isis** *process-id*
9. **net** *network-entity-title*
10. **interface loopback** *number*
11. **address-family ipv6 unicast**
12. **exit**
13. **exit**
14. **interface** *type interface-path-id*
15. **address-family ipv6 unicast**
16. **exit**
17. **exit**
18. **mpls ldp**
19. **default-vrf implicit-ipv4 disable**
20. **router-id** *lsr id*
21. **address-family ipv6**
22. **exit**
23. **interface** *type interface-path-id*
24. **address-family ipv6**
25. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**interface loopback** *number* **Example:** `RP/0/RSP0/CPU0:router(config)# interface Loopback 0`	Enters interface configuration mode.
Step 3	**ipv6 address** *prefix* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv6 address 6:6:6::6/128`	Configures IPv6 address on interface.
Step 4	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.
Step 5	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface GigabitEthernet 0/0/0/0`	Enters interface configuration mode for the LDP protocol.
Step 6	**ipv6 address** *prefix* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv6 address 16:1::6/120`	Configures IPv6 address on interface.
Step 7	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if)# exit`	Exits interface configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 8	**router isis** *process-id* **Example:** `RP/0/RSP0/CPU0:router(config)# router isis 100`	Enables IS-IS routing for the specified routing process.
Step 9	**net** *network-entity-title* **Example:** `RP/0/RSP0/CPU0:router(config-isis)# net 49.0000.0000.0000.0006.00`	Configures the NET on the router. The NET identifies the router for IS-IS.
Step 10	**interface loopback** *number* **Example:** `RP/0/RSP0/CPU0:router(config-isis)# interface Loopback 0`	Enters interface configuration mode.
Step 11	**address-family ipv6 unicast** **Example:** `RP/0/RSP0/CPU0:router(config-isis-if)# address-family ipv6 unicast`	Enters the IS-IS interface IPv6 address family configuration submode. Specifies unicast topology.
Step 12	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-isis-if-af)# exit`	Exits address family configuration submode and enters interface configuration mode.
Step 13	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-isis-if)# exit`	Exits interface configuration mode.
Step 14	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-isis)# interface GigabitEthernet 0/0/0/0`	Enters interface configuration mode for the LDP protocol.
Step 15	**address-family ipv6 unicast** **Example:**	Enters the IS-IS interface IPv6 address family configuration submode. Specifies unicast topology.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-isis-if)# address-family ipv6 unicast`	
Step 16	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-isis-if-af)# exit`	Exits address family configuration submode and enters interface configuration mode.
Step 17	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-isis-if)# exit`	Exits interface configuration mode.
Step 18	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config-isis)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 19	**default-vrf implicit-ipv4 disable** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# default-vrf implicit-ipv4 disable`	Disables the implicitly enabled IPv4 address family for default VRF.
Step 20	**router-id** *lsr id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# router-id 5.5.5.5`	Configures router ID.
Step 21	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`	Enables native LDP IPv6 address family.
Step 22	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af)# exit`	Exits the current configuration mode.

	Command or Action	Purpose
Step 23	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# interface GigabitEthernet 0/0/0/0`	Enters interface configuration mode for the LDP protocol.
Step 24	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-if)# address-family ipv6`	Enables LDP IPv6 control plane.

Step 25	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-if-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-if-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		  • Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		  • Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		  • Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Example

Configuring Global Transport Address for IPV6

Perform this task to configure global transport address for IPv6 address family.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **address-family ipv6**

4. **discovery transport-address** *ip-address*
5. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**address-family ipv6** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# address-family ipv6`	Enables native LDP IPv6 address family.
Step 4	**discovery transport-address** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-ldp-af)# discovery transport-address 5:6::78`	Configures the global transport address for the specified IPv6 address.

Step 5	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-af)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp-af)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.

	Command or Action	Purpose
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Disabling Implicit IPv4

Perform this task to disable the implicitly enabled IPv4 address family for default VRF.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **default-vrf implicit-ipv4 disable**
4. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**default-vrf implicit-ipv4 disable** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# default-vrf implicit-ipv4 disable`	Disables the implicitly enabled IPv4 address family for default VRF.
Step 4	**end** or **commit** **Example:**	• When you issue the **end** command, the system prompts you to commit changes: `Uncommitted changes found, commit them before`

	Command or Action	Purpose

	`RP/0/RP/0/RSP0/CPU0:router (config-ldp)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp)# commit`
		`exiting(yes/no/cancel)?`
		`[cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring IPv4 as Transport Preference

Perform this task to configure IPv4 as the preferred transport (overriding the default setting of IPv6 as preferred transport) to establish connection for a set of dual-stack peers.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **neighbor dual-stack transport-connection prefer ipv4 for-peers** *peer lsr-id*
4. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.

	Command or Action	Purpose
Step 3	**neighbor dual-stack transport-connection prefer ipv4 for-peers** *peer lsr-id* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# neighbor dual-stack transport-connection prefer ipv4 for-peers 5.5.5.5`	Configures IPv4 as the preferred transport connection for the specified peer.

Step 4	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Transport Preference Maximum Wait Time

Perform this task to configure the maximum time (in seconds) the preferred address family connection must wait to establish transport connection before resorting to non-preferred address family.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **neighbor dual-stack transport-connection max-wait** *seconds*
4. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**neighbor dual-stack transport-connection max-wait** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# neighbor dual-stack transport-connection max-wait 5`	Configures the maximum wait time.

Step 4	**end** or **commit**
	Example:
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp)# end`
	or
	`RP/0/RP/0/RSP0/CPU0:router (config-ldp)# commit`
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		• Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		• Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		• Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuration Examples for Implementing MPLS LDP

These configuration examples are provided to implement LDP:

Configuring LDP with Graceful Restart: Example

The example shows how to enable LDP with graceful restart on the POS interface 0/2/0/0.

```
mpls ldp
 graceful-restart
 interface pos0/2/0/0
!
```

Configuring LDP Discovery: Example

The example shows how to configure LDP discovery parameters.

```
mpls ldp
 router-id 192.168.70.1
 discovery hello holdtime 15
 discovery hello interval 5
!

show mpls ldp parameters
show mpls ldp discovery
```

Configuring LDP Link: Example

The example shows how to configure LDP link parameters.

```
mpls ldp
 interface pos 0/1/0/0
 !
!

show mpls ldp discovery
```

Related Topics

Configuring LDP Discovery Over a Link, on page 40
LDP Control Plane, on page 7

Configuring LDP Discovery for Targeted Hellos: Example

The examples show how to configure LDP Discovery to accept targeted hello messages.

Active (tunnel head)

```
mpls ldp
 router-id 192.168.70.1
 interface tunnel-te 12001
 !
!
```

Passive (tunnel tail)

```
mpls ldp
 router-id 192.168.70.2
 discovery targeted-hello accept
!
```

Related Topics

Configuring LDP Discovery for Active Targeted Hellos, on page 42
Configuring LDP Discovery for Passive Targeted Hellos, on page 44
LDP Control Plane, on page 7

Configuring Label Advertisement (Outbound Filtering): Example

The example shows how to configure LDP label advertisement control.

```
 mpls ldp
    address-family ipv4
      label local advertise
         disable
         for pfx_acl_1 to peer_acl_1
         for pfx_acl_2 to peer_acl_2
         for pfx_acl_3
         interface POS 0/1/0/0
         interface POS 0/2/0/0
      !
   !

ipv4 access-list pfx_acl_1
    10 permit ipv4 host 10.0.0.4 any
!
ipv4 access-list pfx_acl_2
    10 permit ipv4 host 10.20.0.4 any
!
ipv4 access-list peer_acl_1
    10 permit ipv4 host 10.0.0.1 any
    20 permit ipv4 host 10.1.1.2 any
!
ipv4 access-list peer_acl_2
    10 permit ipv4 host 172.16.0.1 any
!
!

show mpls ldp binding
```

Related Topics

Configuring Label Advertisement Control (Outbound Filtering), on page 46

Label Advertisement Control (Outbound Filtering), on page 13

Configuring LDP Neighbors: Example

The example shows how to disable label advertisement.

```
mpls ldp
   address-family ipv4
     label local advertise
       disable
     !
   !
!
```

Related Topics

Setting Up LDP Neighbors, on page 47

Configuring LDP Forwarding: Example

The example shows how to configure LDP forwarding.

```
mpls ldp
 address-family ipv4
 label local advertise explicit-null
!

show mpls ldp forwarding
show mpls forwarding
```

Related Topics

Setting Up LDP Forwarding, on page 50
LDP Forwarding, on page 8

Configuring LDP Nonstop Forwarding with Graceful Restart: Example

The example shows how to configure LDP nonstop forwarding with graceful restart.

```
mpls ldp
log
graceful-restart
!
 graceful-restart
 graceful-restart forwarding state-holdtime 180
 graceful-restart reconnect-timeout 15
 interface pos0/1/0/0
!

show mpls ldp graceful-restart
show mpls ldp neighbor gr
show mpls ldp forwarding
show mpls forwarding
```

Related Topics

Setting Up LDP NSF Using Graceful Restart, on page 54
LDP Graceful Restart, on page 9
Phases in Graceful Restart, on page 11
Recovery with Graceful-Restart, on page 11

Configuring Label Acceptance (Inbound Filtering): Example

The example shows how to configure inbound label filtering.

```
mpls ldp
 label
accept
 for pfx_acl_2 from 192.168.2.2
!
 !
!
```

```
mpls ldp
 address-family ipv4
  label remote accept from 192.168.1.1:0 for pfx_acl_2
  !
 !
!
```

Related Topics

Configuring Label Acceptance Control (Inbound Filtering), on page 57
Label Acceptance Control (Inbound Filtering), on page 13

Configuring Local Label Allocation Control: Example

The example shows how to configure local label allocation control.

```
mpls ldp
 address-family ipv4
  label local allocate for pfx_acl_1
  !
 !
```

Related Topics

Configuring Local Label Allocation Control, on page 58
Local Label Allocation Control, on page 13

Configuring LDP Session Protection: Example

The example shows how to configure session protection.

```
mpls ldp
 session protection duration 60 for peer_acl_1
```

```
!
```

Related Topics

Configuring Session Protection, on page 59
Session Protection, on page 14

Configuring LDP IGP Synchronization—OSPF: Example

The example shows how to configure LDP IGP synchronization for OSPF.

```
router ospf 100
mpls ldp sync
!
mpls ldp
 igp sync delay 30
!
```

Related Topics

Configuring LDP IGP Synchronization: OSPF, on page 60
IGP Synchronization, on page 15

Configuring LDP IGP Synchronization—ISIS: Example

The example shows how to configure LDP IGP synchronization.

```
router isis 100
 interface POS 0/2/0/0
address-family ipv4 unicast
mpls ldp sync
!
 !
!
mpls ldp
 igp sync delay 30
!
```

Related Topics

Configuring LDP IGP Synchronization: ISIS, on page 64
IGP Synchronization, on page 15

Configuring LDP Auto-Configuration: Example

The example shows how to configure the IGP auto-configuration feature globally for a specific OSPF interface ID.

```
router ospf 100
 mpls ldp auto-config
 area 0
  interface pos 1/1/1/1
```

The example shows how to configure the IGP auto-configuration feature on a given area for a given OSPF interface ID.

```
router ospf 100
 area 0
  mpls ldp auto-config
  interface pos 1/1/1/1
```

Related Topics

Enabling LDP Auto-Configuration for a Specified OSPF Instance, on page 65
Enabling LDP Auto-Configuration in an Area for a Specified OSPF Instance, on page 66
Disabling LDP Auto-Configuration, on page 67
IGP Auto-configuration, on page 15

Configure IP LDP Fast Reroute Loop Free Alternate: Examples

This example shows how to configure LFA FRR with default tie-break configuration:

```
router isis TEST
 net 49.0001.0000.0000.0001.00
 address-family ipv4 unicast
  metric-style wide

 interface GigabitEthernet0/6/0/13
  point-to-point
  address-family ipv4 unicast
   fast-reroute per-prefix
   # primary path GigabitEthernet0/6/0/13 will exclude the interface
   # GigabitEthernet0/6/0/33 in LFA backup path computation.
   fast-reroute per-prefix exclude interface GigabitEthernet0/6/0/33
!
 interface GigabitEthernet0/6/0/23
  point-to-point
  address-family ipv4 unicast
!
 interface GigabitEthernet0/6/0/24
  point-to-point
  address-family ipv4 unicast
!
 interface GigabitEthernet0/6/0/33
  point-to-point
  address-family ipv4 unicast
!
```

This example shows how to configure TE tunnel as LFA backup:

```
router isis TEST
 net 49.0001.0000.0000.0001.00
 address-family ipv4 unicast
  metric-style wide
```

```
 interface GigabitEthernet0/6/0/13
  point-to-point
  address-family ipv4 unicast
   fast-reroute per-prefix
   # primary path GigabitEthernet0/6/0/13 will exclude the interface
   # GigabitEthernet0/6/0/33 in LFA backup path computation. TE tunnel 1001
   # is using the link GigabitEthernet0/6/0/33.
   fast-reroute per-prefix exclude interface GigabitEthernet0/6/0/33
   fast-reroute per-prefix lfa-candidate interface tunnel-te1001
!
 interface GigabitEthernet0/6/0/33
  point-to-point
  address-family ipv4 unicast
!
```

This example shows how to configure LFA FRR with configurable tie-break configuration:

```
router isis TEST
 net 49.0001.0000.0000.0001.00
 address-family ipv4 unicast
  metric-style wide
  fast-reroute per-prefix tiebreaker ?
  downstream            Prefer backup path via downstream node
  lc-disjoint           Prefer line card disjoint backup path
  lowest-backup-metric  Prefer backup path with lowest total metric
  node-protecting       Prefer node protecting backup path
  primary-path          Prefer backup path from ECMP set
  secondary-path        Prefer non-ECMP backup path

  fast-reroute per-prefix tiebreaker lc-disjoint index ?
  <1-255>  Index
  fast-reroute per-prefix tiebreaker lc-disjoint index 10

Sample configuration:

router isis TEST
 net 49.0001.0000.0000.0001.00
 address-family ipv4 unicast
  metric-style wide
  fast-reroute per-prefix tiebreaker downstream index 60
  fast-reroute per-prefix tiebreaker lc-disjoint index 10
  fast-reroute per-prefix tiebreaker lowest-backup-metric index 40
  fast-reroute per-prefix tiebreaker node-protecting index 30
  fast-reroute per-prefix tiebreaker primary-path index 20
  fast-reroute per-prefix tiebreaker secondary-path index 50
!
interface GigabitEthernet0/6/0/13
  point-to-point
  address-family ipv4 unicast
   fast-reroute per-prefix
!
 interface GigabitEthernet0/1/0/13
  point-to-point
  address-family ipv4 unicast
   fast-reroute per-prefix
!
 interface GigabitEthernet0/3/0/0.1
  point-to-point
  address-family ipv4 unicast
!
 interface GigabitEthernet0/3/0/0.2
  point-to-point
  address-family ipv4 unicast
```

Related Topics

IP LDP Fast Reroute Loop Free Alternate, on page 16

Verify IP LDP Fast Reroute Loop Free Alternate: Example

The following examples show how to verify the IP LDP FRR LFA feature on the router.

The following example shows how to verify ISIS FRR output:

```
RP/0/RSP0/CPU0:router#show isis fast-reroute summary

IS-IS 1 IPv4 Unicast FRR summary

                         Critical   High       Medium     Low        Total
                         Priority   Priority   Priority   Priority
Prefixes reachable in L1
  All paths protected     0          0          4          1008       1012
  Some paths protected    0          0          0          0          0
  Unprotected             0          0          0          0          0
  Protection coverage     0.00%      0.00%      100.00%    100.00%    100.00%
Prefixes reachable in L2
  All paths protected     0          0          1          0          1
  Some paths protected    0          0          0          0          0
  Unprotected             0          0          0          0          0
  Protection coverage     0.00%      0.00%      100.00%    0.00%      100.00%
```

The following example shows how to verify the IGP route 10.21.1.1/24 in ISIS Fast Reroute output:

```
RP/0/RSP0/CPU0:router#show isis fast-reroute 10.21.1.1/24

L1 10.21.1.1/24 [40/115]
     via 12.0.0.2, GigabitEthernet0/6/0/13, NORTH
       FRR backup via 14.0.2.2, GigabitEthernet0/6/0/0.3, SOUTH

RP/0/RSP0/CPU0:router#show isis fast-reroute 10.21.1.1/24 detail

L1 10.21.1.1/24 [40/115] low priority
     via 12.0.0.2, GigabitEthernet0/6/0/13, NORTH
       FRR backup via 14.0.2.2, GigabitEthernet0/6/0/0.3, SOUTH
       P: No, TM: 130, LC: No, NP: Yes, D: Yes
     src sr1.00-00, 173.1.1.2
   L2 adv [40] native, propagated
```

The following example shows how to verify the IGP route 10.21.1.1/24 in RIB output:

```
RP/0/RSP0/CPU0:router#show route 10.21.1.1/24

Routing entry for 10.21.1.0/24
  Known via "isis 1", distance 115, metric 40, type level-1
  Installed Nov 27 10:22:20.311 for 1d08h
  Routing Descriptor Blocks
    12.0.0.2, from 173.1.1.2, via GigabitEthernet0/6/0/13, Protected
      Route metric is 40
    14.0.2.2, from 173.1.1.2, via GigabitEthernet0/6/0/0.3, Backup
      Route metric is 0
```

```
  No advertising protos.
```

The following example shows how to verify the IGP route 10.21.1.1/24 in FIB output:

```
RP/0/RSP0/CPU0:router#show cef 10.21.1.1/24
10.21.1.0/24, version 0, internal 0x40040001 (ptr 0x9d9e1a68) [1], 0x0              \
(0x9ce0ec40), 0x4500 (0x9e2c69e4)
 Updated Nov 27 10:22:29.825
 remote adjacency to GigabitEthernet0/6/0/13
 Prefix Len 24, traffic index 0, precedence routine (0)
   via 12.0.0.2, GigabitEthernet0/6/0/13, 0 dependencies, weight 0, class 0,         \
protected [flags 0x400]
    path-idx 0, bkup-idx 1 [0x9e5b71b4 0x0]
    next hop 12.0.0.2
     local label 16080      labels imposed {16082}
   via 14.0.2.2, GigabitEthernet0/6/0/0.3, 3 dependencies, weight 0, class 0,        \
backup [flags 0x300]
    path-idx 1
    next hop 14.0.2.2
    remote adjacency
     local label 16080      labels imposed {16079}

RP/0/RSP0/CPU0:router#show cef 10.21.1.1/24 detail
10.21.1.0/24, version 0, internal 0x40040001 (ptr 0x9d9e1a68) [1], 0x0              \
(0x9ce0ec40), 0x4500 (0x9e2c69e4)
 Updated Nov 27 10:22:29.825
 remote adjacency to GigabitEthernet0/6/0/13
 Prefix Len 24, traffic index 0, precedence routine (0)
  gateway array (0x9cc622f0) reference count 1158, flags 0x28000d00, source lsd      \
(2),
                [387 type 5 flags 0x101001 (0x9df32398) ext 0x0 (0x0)]
  LW-LDI[type=5, refc=3, ptr=0x9ce0ec40, sh-ldi=0x9df32398]
   via 12.0.0.2, GigabitEthernet0/6/0/13, 0 dependencies, weight 0, class 0,         \
protected [flags 0x400]
    path-idx 0, bkup-idx 1 [0x9e5b71b4 0x0]
    next hop 12.0.0.2
     local label 16080      labels imposed {16082}
   via 14.0.2.2, GigabitEthernet0/6/0/0.3, 3 dependencies, weight 0, class 0,        \
backup [flags 0x300]
    path-idx 1
    next hop 14.0.2.2
    remote adjacency
     local label 16080      labels imposed {16079}


    Load distribution: 0 (refcount 387)

    Hash  OK  Interface                 Address
    0     Y   GigabitEthernet0/6/0/13   remote
```

The following example shows how to verify the IGP route 10.21.1.1/24 in MPLS LDP output:

```
RP/0/RSP0/CPU0:router#show mpls ldp forwarding 10.21.1.1/24

Prefix           Label   Label      Outgoing     Next Hop            GR Stale
                 In      Out        Interface
---------------- ------- ---------- ------------ ------------------- -- -----
10.21.1.0/24     16080   16082      Gi0/6/0/13   12.0.0.2            Y  N
```

```
                          16079      Gi0/6/0/0.3  14.0.2.2 (!)        Y  N


RP/0/RSP0/CPU0:router#show mpls ldp forwarding 10.21.1.1/24 detail

Prefix           Label   Label      Outgoing     Next Hop            GR Stale
                 In      Out        Interface
---------------- ------- ---------- ------------ ------------------- -- -----
10.21.1.0/24     16080   16082      Gi0/6/0/13   12.0.0.2            Y  N
                         [ Protected; path-id 1 backup-path-id 33;
                           peer 20.20.20.20:0 ]
                         16079      Gi0/6/0/0.3  14.0.2.2 (!)        Y  N
                         [ Backup; path-id 33; peer 40.40.40.40:0 ]
  Routing update   : Nov 27 10:22:19.560 (1d08h ago)
  Forwarding update: Nov 27 10:22:29.060 (1d08h ago)
```

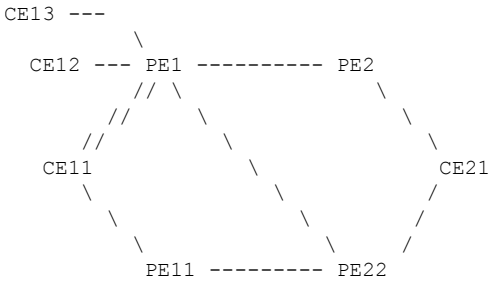
Related Topics

IP LDP Fast Reroute Loop Free Alternate, on page 16

MPLS LDP CSC for Multiple VRFs Configuration: Examples

This figure shows a L3VPN LDP CSC topology that uses either BGP or LDP between PE and CE routers to distribute routes and MPLS labels.

L3VPN CSC VPN: LDP / BGP



VRF red: CE11, CE21

VRF blue: CE12, CE13 (local only switching)

Multi-home CEs: CE11, CE21

LDP CSC: PE1/PE11 with CE1x

BGP CSC: PE2/PE22 with CE2x

CSC-CE11 Configuration

```
hostname ce11

interface Loopback0
 ipv4 address 198.51.100.254 255.255.255.255
!
interface POS0/2/0/0
 ipv4 address 192.168.1.11 255.255.255.0
```

```
!
interface POS0/2/0/1
 ipv4 address 192.168.2.11 255.255.255.0
!
interface POS0/2/0/2
 ipv4 address 192.168.3.11 255.255.255.0
!
router ospf 100
 log adjacency changes
 router-id 198.51.100.254
 area 0
  interface Loopback0
  !
  interface POS0/2/0/0
  !
  interface POS0/2/0/1
  !
  interface POS0/2/0/2
  !
 !
!
mpls ldp
 log
  adjacency
  neighbor
 !
 router-id 198.51.100.254
 address-family ipv4
 !
 interface POS0/2/0/0
  address-family ipv4
  !
 !
 interface POS0/2/0/1
  address-family ipv4
  !
 !
 interface POS0/2/0/2
  address-family ipv4
  !
 !
!
no interface POS0/2/0/0 shut
no interface POS0/2/0/1 shut
no interface POS0/2/0/2 shut
end
```

CSC-CE12 Configuration

```
hostname ce12

interface Loopback0
 ipv4 address 198.51.100.252 255.255.255.255
!
interface POS0/2/0/0
 ipv4 address 192.169.1.12 255.255.255.0
!
router ospf 100
 log adjacency changes
 router-id 198.51.100.252
 area 0
  interface Loopback0
```

```
  !
  interface POS0/2/0/0
  !
 !
!
mpls ldp
 log
  adjacency
  neighbor
 !
 router-id 198.51.100.252
 address-family ipv4
 !
 interface POS0/2/0/0
  address-family ipv4
  !
 !
!
no interface POS0/2/0/0 shut
end
```

CSC-CE13 Configuration

```
hostname ce13

interface Loopback0
 ipv4 address 198.51.100.254 255.255.255.255
!
interface POS0/2/0/0
 ipv4 address 192.170.1.12 255.255.255.0
!
router ospf 100
 log adjacency changes
 router-id 198.51.100.254
 area 0
  interface Loopback0
  !
  interface POS0/2/0/0
  !
 !
!
mpls ldp
 log
  adjacency
  neighbor
 !
 router-id 198.51.100.254
 address-family ipv4
 !
 interface POS0/2/0/0
  address-family ipv4
  !
 !
!
no interface POS0/2/0/0 shut
end
```

CSC-CE21 Configuration

```
hostname ce21

interface Loopback0
 ipv4 address 10.20.20.21 255.255.255.255
!
interface POS0/2/0/0
 ipv4 address 192.168.1.21 255.255.255.0
!
interface POS0/2/0/1
 ipv4 address 192.169.1.21 255.255.255.0
!
route-policy pass-all
  pass
end-policy
!
router static
 address-family ipv4 unicast
  192.168.1.2/32 POS0/2/0/0
  192.169.1.2/32 POS0/2/0/1
 !
 address-family ipv6 unicast
  1:1:1::1/128 POS0/2/0/0
 !
!
router bgp 2
 bgp router-id 10.20.20.21
 address-family ipv4 unicast
  redistribute connected
  allocate-label all
 !
 neighbor 192.168.1.2
  remote-as 100
  address-family ipv4 labeled-unicast
   route-policy pass-all in
   route-policy pass-all out
  !
 !
 neighbor 192.169.1.22
  remote-as 100
  address-family ipv4 labeled-unicast
   route-policy pass-all in
   route-policy pass-all out
  !
 !
!
no interface POS0/2/0/0 shut
no interface POS0/2/0/1 shut
end
```

CSC-PE1 Configuration

```
hostname pe1

vrf red
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
  !
 !
```

```
!
vrf blue
 address-family ipv4 unicast
 !
!
interface Loopback0
 ipv4 address 10.0.0.1 255.255.255.255
 ipv6 address 1:1:1::1/128
!
interface Loopback1
 vrf red
 ipv4 address 10.0.0.1 255.255.255.255
!
interface Loopback2
 vrf blue
 ipv4 address 10.0.0.1 255.255.255.255
!
interface Loopback11
 ipv4 address 10.0.0.2 255.255.255.255
 ipv6 address 1:1:1::2/128
!
interface Loopback112
 vrf blue
 ipv4 address 10.0.0.112 255.255.255.255
!
interface POS0/2/0/0
 vrf red
 ipv4 address 192.168.1.1 255.255.255.0
!
interface POS0/2/0/1
 vrf red
 ipv4 address 192.168.2.1 255.255.255.0
!
interface POS0/2/0/2
 vrf blue
 ipv4 address 192.169.1.1 255.255.255.0
!
interface POS0/2/0/3
 vrf blue
 ipv4 address 192.170.1.1 255.255.255.0
!
interface POS0/2/0/4
 ipv4 address 12.10.0.1 255.255.255.0
 ipv6 address 12:1::1/120
!
interface POS0/2/0/5
 ipv4 address 122.1.0.1 255.255.255.0
!
router static
 address-family ipv6 unicast
  2:2:2::2/128 POS0/2/0/4
 !
!
router ospf 100
 log adjacency changes
 router-id 10.0.0.1
 area 0
  interface Loopback0
  !
  interface POS0/2/0/4
  !
  interface POS0/2/0/5
  !
 !
```

```
 vrf red
  router-id 10.0.0.1
  redistribute bgp 100
  area 0
   interface Loopback1
   !
   interface POS0/2/0/0
   !
   interface POS0/2/0/1
   !
  !
 !
 vrf blue
  router-id 10.0.0.1
  area 0
   interface Loopback2
   !
   interface POS0/2/0/2
   !
   interface POS0/2/0/3
   !
  !
 !
!
router bgp 100
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 neighbor 172.16.0.1
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 neighbor 172.16.0.12
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 vrf red
  rd 1:1
  address-family ipv4 unicast
   maximum-paths eibgp 8
   redistribute ospf 100
  !
 !
!
mpls ldp
 log
  adjacency
  neighbor
 !
 nsr
 router-id 10.0.0.1
 address-family ipv4
  label
   local
    advertise
     explicit-null
    !
   !
  !
```

```
 !
 interface POS0/2/0/4
  address-family ipv4
  !
 !
 interface POS0/2/0/5
  address-family ipv4
  !
 !
 vrf red
  address-family ipv4
  !
  interface POS0/2/0/0
   address-family ipv4
   !
  !
  interface POS0/2/0/1
   address-family ipv4
   !
  !
 !
 vrf blue
  router-id 10.0.0.2
  address-family ipv4
   discovery transport-address 10.0.0.1
   label
    local
     allocate for host-routes
    !
   !
  !
  interface POS0/2/0/2
   address-family ipv4
   !
  !
  interface POS0/2/0/3
   address-family ipv4
   !
  !
 !
!
no interface POS0/2/0/0 shut
no interface POS0/2/0/1 shut
no interface POS0/2/0/2 shut
no interface POS0/2/0/3 shut
no interface POS0/2/0/4 shut
no interface POS0/2/0/5 shut
end
```

CSC-PE2 Configuration

```
hostname pe2

vrf red
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
  !
 !
```

```
!
interface Loopback0
 ipv4 address 172.16.0.1 255.255.255.255
 ipv6 address 2:2:2::2/128
!
interface Loopback1
 vrf red
 ipv4 address 172.16.0.1 255.255.255.255
!
interface POS0/2/0/0
 ipv4 address 12.1.0.2 255.255.255.0
 ipv6 address 12:1::2/120
!
interface POS0/2/0/1
 vrf red
 ipv4 address 192.168.1.2 255.255.255.0
!
route-policy pass-all
  pass
end-policy
!
router static
 address-family ipv6 unicast
  1:1:1::1/128 POS0/2/0/0
  1:1:1::2/128 POS0/2/0/0
 !
 vrf red
  address-family ipv4 unicast
   192.168.1.21/32 POS0/2/0/1
  !
 !
!
router ospf 100
 log adjacency changes
 router-id 172.16.0.1
 area 0
  interface Loopback0
  !
  interface POS0/2/0/0
  !
 !
!
router bgp 100
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 neighbor 10.0.0.1
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 vrf red
  rd 1:1
  address-family ipv4 unicast
   allocate-label all
  !
  neighbor 192.168.1.21
   remote-as 2
   address-family ipv4 labeled-unicast
    route-policy pass-all in
    route-policy pass-all out
   !
```

```
  !
 !
!
mpls ldp
 log
  adjacency
  neighbor
 !
 router-id 172.16.0.1
 address-family ipv4
  label
   local
    advertise
     explicit-null
    !
   !
  !
 !
 interface POS0/2/0/0
  address-family ipv4
  !
 !
!
no interface POS0/2/0/0 shut
no interface POS0/2/0/1 shut
end
```

CSC-PE11 Configuration

```
hostname pe11

vrf red
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
  !
 !
!
interface Loopback0
 ipv4 address 10.0.0.11 255.255.255.255
!
interface Loopback1
 vrf red
 ipv4 address 10.0.0.11 255.255.255.255
!
interface POS0/2/0/0
 vrf red
 ipv4 address 192.168.3.1 255.255.255.0
!
interface POS0/2/0/1
 ipv4 address 10.12.0.1 255.255.255.0
!
router ospf 100
 log adjacency changes
 router-id 10.0.0.11
 area 0
  interface Loopback0
  !
  interface POS0/2/0/1
```

```
  !
 !
 vrf red
  router-id 10.0.0.11
  redistribute bgp 100
  area 0
   interface Loopback1
   !
   interface POS0/2/0/0
   !
  !
 !
!
router bgp 100
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 neighbor 172.16.0.12
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 vrf red
  rd 1:1
  address-family ipv4 unicast
   maximum-paths eibgp 8
   redistribute ospf 100
  !
 !
!
mpls ldp
 log
  adjacency
  neighbor
 !
 router-id 10.0.0.11
 address-family ipv4
 !
 interface POS0/2/0/1
  address-family ipv4
  !
 !
 vrf red
  address-family ipv4
  !
  interface POS0/2/0/0
   address-family ipv4
   !
  !
 !
!
no interface POS0/2/0/0 shut
no interface POS0/2/0/1 shut
end
```

CSC-PE22 Configuration

```
hostname pe22

vrf red
```

```
 address-family ipv4 unicast
  import route-target
   100:1
  !
  export route-target
   100:1
  !
 !
!
interface Loopback0
 ipv4 address 172.16.0.12 255.255.255.255
!
interface Loopback1
 vrf red
 ipv4 address 172.16.0.12 255.255.255.255
!
interface POS0/2/0/0
 ipv4 address 122.1.0.22 255.255.255.0
!
interface POS0/2/0/1
 vrf red
 ipv4 address 192.169.1.22 255.255.255.0
!
interface POS0/2/0/2
 ipv4 address 10.10.1.22 255.255.255.0
!
route-policy pass-all
  pass
end-policy
!
router static
 vrf red
  address-family ipv4 unicast
   192.169.1.21/32 POS0/2/0/1
  !
 !
!
router ospf 100
 log adjacency changes
 router-id 172.16.0.12
 area 0
  interface Loopback0
  !
  interface POS0/2/0/0
  !
  interface POS0/2/0/2
  !
 !
!
router bgp 100
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 neighbor 10.0.0.1
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  !
 !
 neighbor 10.0.0.11
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
```

```
  !
 !
 vrf red
  rd 1:1
  address-family ipv4 unicast
   allocate-label all
  !
  neighbor 192.169.1.21
   remote-as 2
   address-family ipv4 labeled-unicast
    route-policy pass-all in
    route-policy pass-all out
   !
  !
 !
!
mpls ldp
 router-id 172.16.0.12
 address-family ipv4
 !
 interface POS0/2/0/0
  address-family ipv4
  !
 !
 interface POS0/2/0/2
  address-family ipv4
  !
 !
!
no interface POS0/2/0/0 shut
no interface POS0/2/0/1 shut
no interface POS0/2/0/2 shut
end
```

The following example shows the output for the **show running-config mpls ldp** command.

```
RP/0/RSP0/CPU0:router# show running-config mpls ldp

mpls ldp
 log
  adjacency
  neighbor
  nsr
  graceful-restart
  session-protection
 !
 nsr
 graceful-restart
 graceful-restart reconnect-timeout 60
 graceful-restart forwarding-state-holdtime 180
 igp sync delay on-proc-restart 300
 igp sync delay on-session-up 15
 discovery
  quick-start disable
  instance-tlv disable
  hello holdtime 30
  hello interval 10
  targeted-hello holdtime 180
  targeted-hello interval 20
 !
 session backoff 5 15
 session holdtime 300
```

```
signalling dscp 48
mldp
 logging notifications
 address-family ipv4
  static p2mp 10.0.0.1 1
  static mp2mp 10.10.20.10 1
  make-before-break delay 10
  mofrr
  recursive-fec
 !
!
router-id 10.0.0.1
neighbor
 password encrypted 01100F17580454
 172.16.0.1:0 password disable
 192.168.0.1:0 password encrypted 02050D480809
!
session downstream-on-demand with peer_acl1
session protection for peer_acl2 duration 30
address-family ipv4
 discovery targeted-hello accept from peer_acl1
 neighbor 172.16.0.1 targeted
 traffic-eng
  auto-tunnel mesh
   group all
   group 10
   group 20
  !
 !
 redistribute
  bgp
   as 100
   advertise-to peer_acl1
  !
 !
 label
  local
   default-route
   implicit-null-override for pfx_acl1
   allocate for pfx_acl
   advertise
    disable
    for pfx_acl1 to peer_acl1
    for pfx_acl2 to peer_acl2
    interface GigabitEthernet0/0/0/0
    explicit-null for pfx_acl1 to peer_acl1
   !
  !
  remote
   accept
    from 172.16.0.1:0 for pfx_acl2
    from 192.168.0.1:0 for pfx_acl3
   !
  !
 !
!
interface GigabitEthernet0/0/0/0
 igp sync delay on-session-up disable
 discovery quick-start disable
 discovery hello holdtime 30
 discovery hello interval 10
 address-family ipv4
  igp auto-config disable
  discovery transport-address interface
```

```
   mldp disable
  !
 !
 interface GigabitEthernet0/0/0/1
  igp sync delay on-session-up 10
  address-family ipv4
   discovery transport-address 10.0.0.1
  !
 !
 interface GigabitEthernet0/0/0/2
 !
!
```

LDP IPv6 Configuration: Examples

The following example shows how to enable LDP IPv6 native under LDP. The user must enable IPv6 address family under LDP submodes.

```
configure
  mpls ldp
   address-family ipv6
   !
  !
```

The following example shows how to enable LDP IPv6 control plane on an LDP interface:

```
configure
  mpls ldp
    interface pos 0/6/0/0
      address-family ipv6
    !
  !
```

The following examples shows how to configure IPv6-only LSR:

Note IPv4 is implicitly enabled under default VRF and any LDP interfaces under default VRF. In order to operate as an IPv6-only LSR, the user must also explicitly disable IPv4 address family.

Example 1:

Note In this example, there is no explicit IPv6 export address. The loopback's IPv6 address is used as the export address (6:6:6::6/128).

The router ID configured in MPLS LDP is not used in anyway for export. It is used only for LDP LSR identification.

```
configure
interface Loopback0
 ipv6 address 6:6:6::6/128
!
```

```
interface GigabitEthernet0/0/0/0
 ipv6 address 16:1::6/120
!
router isis 100
 net 49.0000.0000.0000.0006.00
 interface Loopback0
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/0/0/0
  address-family ipv6 unicast
  !
 !
mpls ldp
 default-vrf implicit-ipv4 disable
 router-id 6.6.6.6
 address-family ipv6
 !
 interface GigabitEthernet0/0/0/0
  address-family ipv6
 !
!
```

Example 2:

Note In this example, there is an explicit IPv6 export address. However, there is no IPv6 loopback.

There is no router-id configured, but the loopback IPv4 address is used.

```
configure
interface Loopback0
 ipv4 address 6.6.6.6/32
!
interface GigabitEthernet0/0/0/0
 ipv6 address 16:1::6/120
!
router isis 100
 net 49.0000.0000.0000.0006.00
 interface Loopback0
  address-family ipv6 unicast
  !
 !
 interface GigabitEthernet0/0/0/0
  address-family ipv6 unicast
  !
 !
mpls ldp
 default-vrf implicit-ipv4 disable
 address-family ipv6
  discovery transport-address 6:6:6::6
 !
 interface GigabitEthernet0/0/0/0
  address-family ipv6
 !
!
```

Entropy Label Support for Transit Routers

Entropy label (EL) in MPLS is a mechanism that improves load balancing across a network. Load balancing helps in planning the capacity of a network by distributing traffic across multiple paths based on hashing functions.



Note On ASR 9000 series routers, entropy label is supported only on transit routers. The data plane of the transit router does not have the functionality to impose entropy label on the MPLS packet if there are any equal cost paths available for a given LSP.

Traffic load balancing over Equal Cost Multipath (ECMP) or Link Aggregation Groups (LAGs) is usually based on a hashing function. To arrive at the hash calculations, the node that performs the load balancing must read header fields in the incoming packets. Currently, Label Switching Routers (LSRs) at each transit point must do a Deep Packet Inspection (DPI) along the path of a given Label Switched Path (LSP). This includes extracting the appropriate keys for load balancing. If the LSR is unable to infer the protocol, it will use the topmost MPLS labels in the label stack as keys to balance the load. This may result in unbalanced distribution of traffic.

Entropy labels enhance load balancing by eliminating the need for DPI at the transit LSRs. The transit router recognizes the incoming MPLS packets with entropy label and performs the load balancing and forwards the MPLS packet on a selected path. The input packets are assumed to have valid EL labels within the first seven labels. Else, either IP header or other MPLS labels are used for load balancing.

The ingress LSR of an LSP computes the hash based on appropriate fields from a given packet and places the result in a label called entropy label as part of the MPLS label stack. Using the entropy label in the hash keys reduces the need of a DPI inspection in the LSR. The transit LSR can use the entire label stack of the MPLS packet to perform load balancing, as the entropy label introduces the right level of order into the label stack.

Advantages of Entropy Label

The advantages of using entropy labels in MPLS networks are:

- Ingress LSRs operate at lower bandwidths than transit LSRs, and are hence the ideal choice for load balancing.
- Transit LSRs do not need to perform DPI and can effectively load balance the packets as decided by the Ingress LSRs.
- Transit LSRs are spared from the problem of misinterpreting the protocol denoted in the label stack and thereby causing inequitable distribution of traffic across equal cost paths exiting from the LSR.

Enable Entropy Label Support on Transit Routers

Entropy label (EL) supports an orderly method for routers to signal entropy label capability (ELC) in the network. When enabled, the routers wait for the ELC signal from all downstream routers before passing their ELC to the next upstream routers in the chain. This ensures that routers report their status in an order, and not in random. Random reporting might require to and fro signaling before ELC can be established in the network. If one router in the chain does not support EL, the network does not use EL for load balancing.

Procedure

Step 1 Enable Entropy label LDP signalling.

```
Router# configure
Router(config)# mpls ldp
Router(config)# entropy-label
Router(config-ldp)# router-id {type number | ip-address}
router(config-ldp)# interface type number
router(config-ldp)# commit
router(config-ldp)# end
```

The router ID is specified as an interface name or IP address. By default, LDP uses the global router ID that is configured by the global router ID process.

Step 2 Enable using entropy label value as a field in the hash calculation for load balancing during forwarding.

```
Router# configure
Router(config)# cef load-balancing fields mpls entropy-label
router(config-ldp)# commit
```

The **cef load-balancing fields mpls entropy-label** command configures the hash tuple with the following fields.

- entropy label
- router ID
- ingress interface

Note
The **cef load-balancing fields mpls entropy-label** command is supported only on Cisco ASR 9000 enhanced ethernet line cards.

Step 3 Display the running configuration that contains the load balancing information.

```
Router# show running config
```

Step 4 Determine load balancing using entropy label. These commands provide the output interface chosen as a result of hashing with MPLS entropy label:

ECMP Path Selection

The following example shows the output for ECMP path selection:

```
Router# show mpls forwarding exact-route label 24001 entropy-label 1234
ingress-interface tenGigE 0/0/0/1/0 location 0/0/CPU0

Local    Outgoing      Prefix      Outgoing        Next Hop        Bytes
Label    Label         or ID       Interface                       Switched
------ ----------- -------------- ------------ ---------------   -----------
24001    64002       194.0.0.1/32  Te0/0/0/1/0.1   25.2.11.1         N/A
    Via: Te0/0/0/1/0.1, Next Hop: 25.2.11.1
    Label Stack (Top -> Bottom): { 64002 }
    NHID: 0x4, Encap-ID: N/A, Path idx: 2, Backup path idx: 0, Weight: 0
    Hash idx: 2
    MAC/Encaps: 18/22, MTU: 1500
    Outgoing Interface: TenGigE0/0/0/1/0.1 (ifhandle 0x00000500)
```

Bundle Member Selection

The following example shows the output for Bundle member selection:

```
Router# bundle-hash bundle-ether 5001 location 0/0/CPU0
Calculate Bundle-Hash for L2 or L3 or sub-int based: 2/3/4 [3]: 3
Enter traffic type (1:IPv4-inbound, 2:MPLS-inbound, 3:IPv6-inbound, 4:IPv4-MGSCP, 5:IPv6-MGSCP): [1]:
 2
Entropy label: y/n [n]: y
Enter Entropy Label (in decimal): 1997
Enter the source interface name (Enter to skip interface details): TenGigE0/0/0/1/0
Entropy Label 1997 -- Link hashed to is TenGigE0/1/0/29, (raw hash 0xb5703292, LAG hash 2, ICL (),
LON 2, IFH 0x06001740)

Another? [y]:
```

Additional References

For additional information related to Implementing MPLS Label Distribution Protocol, refer to the following references:

Related Documents

Related Topic	Document Title
LDP Commands	*MPLS Label Distribution Protocol Commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

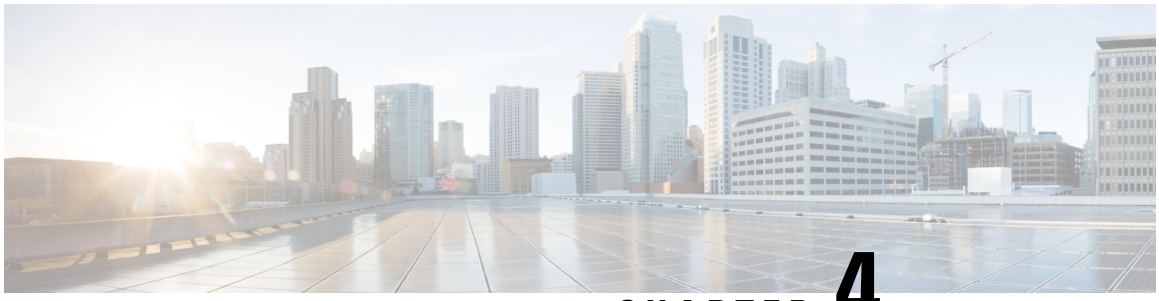
MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs **Note** Not all supported RFCs are listed.	Title
RFC 3031	*Multiprotocol Label Switching Architecture*
RFC 3036	*LDP Specification*
RFC 3037	*LDP Applicability*
RFC 3478	*Graceful Restart Mechanism for Label Distribution Protocol*
RFC 3815	*Definitions of Managed Objects for MPLS LDP*
RFC 5036	*Label Distribution and Management* *Downstream on Demand Label Advertisement*
RFC 5286	*Basic Specification for IP Fast Reroute: Loop-Free Alternates*

Technical Assistance

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



CHAPTER 4

Implementing MPLS Static Labeling

The MPLS static feature enables you to statically assign local labels to an IPv4 prefix per VRF. Also, Label Switched Paths (LSPs) can be provisioned for these static labels by specifying the next-hop information that is required to forward the packets containing static label.

If there is any discrepancy between labels assigned statically and dynamically, the router issues a warning message in the console log. By means of this warning message, the discrepancy can be identified and resolved.

Static labels are more advantageous than dynamic labels because static labels:

- Improve security because the risk of receiving unwanted labels from peers (running a compromised MPLS dynamic labeling protocol) is reduced.
- Gives users full control over defined LSPs.Gives users full control over defined LSPs.
- Utilize system resources optimally because dynamic labeling is not processed.

To perform static binding of MPLS labels, you need to:

- Enable MPLS Encapsulation on an Interface, on page 135
- Define a Range for Static MPLS Labels, on page 136
- Allocate static label:
  - Setup a Static LSP, on page 137

    or

    Allocate Static MPLS Label to an IP Prefix and Configure a LSP, on page 138
  - Allocate Static MPLS Label for a Specific VRF, on page 139
- Verify MPLS Static Bindings, on page 140
- Identify and Clear Label Discrepancy, on page 142

Restrictions

- Static labeling on IPv6 packets is not supported.
- The router does not prevent label discrepancy at the time of configuring static labels. Any generated discrepancy needs to be subsequently cleared.
- Equal-cost multi-path routing (ECMP) is not supported.

- Interfaces must be explicitly configured to handle traffic with static MPLS labels.
- The MPLS per-VRF labels cannot be shared between MPLS static and other applications.

Feature History for Implementing MPLS Static Labeling

Release	Modification
Release 5.1.1	This feature was introduced.
Release 5.2.2	Recursive Label Statistics feature was added.
Release 5.3.2	MPLS Top Label Hash for OAM Packets feature was added.

- Recursive Label Statistics, on page 132
- MPLS Top Label Hash for OAM Packets, on page 133
- Enable MPLS Encapsulation on an Interface, on page 135
- Define a Range for Static MPLS Labels, on page 136
- Setup a Static LSP, on page 137
- Allocate Static MPLS Label to an IP Prefix and Configure a LSP, on page 138
- Allocate Static MPLS Label for a Specific VRF, on page 139
- Verify MPLS Static Bindings, on page 140
- Configuring Top Label Hash, on page 141
- Identify and Clear Label Discrepancy, on page 142
- Configure Top Label Hash: Example, on page 143

Recursive Label Statistics

The MPLS static feature is enhanced to provide recursive Label Switched Path (LSP) statistics for labels created using MPLS static configuration. The recursive label statistics feature helps in identifying the unique source and destination port LSPs.

Restrictions

- LSP statistics works only for labels allocated through MPLS static configuration in a VRF, which means that it only works for recursive VPN labels.
- No packet rate support.
- During MPLS static configuration or de-configuration, label discrepancies can get generated.

Use the **clear mpls static local-label discrepancy** command to clear any discrepancy between statically allocated and dynamically allocated local labels. It is recommended to execute this command upon removal of a static configuration, so that the label prefix is reallocated to the dynamic label range which then will also free the allocated statistic point. Use the **all** keyword to clear all label discrepancies. The static label configuration takes precedence while clearing discrepancy.

MPLS Top Label Hash for OAM Packets

The MPLS top label hash feature lets label switching routers (LSRs) to be based on top label hashing for MPLS OAM packets. LSRs commonly generate a hash of the label stack or some elements of the label stack as a method of discriminating flows, and use this discriminator to distribute the flows over available equal cost multipaths (ECMPs) that exist in the network.

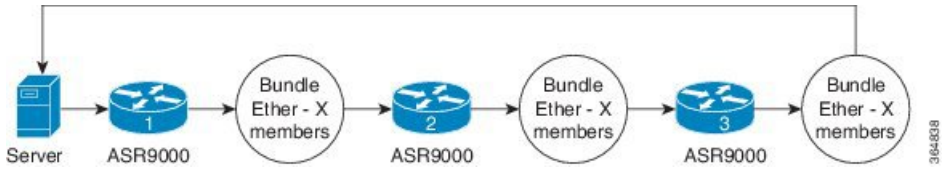
In order to determine which path (ECMP) or link aggregation group (LAG) member to choose, the system computes a hash. Certain bits out of this hash are used to identify member or path to be taken.

To configure top label hash, use the **top-label-hash** command under the MPLS static address family IPv4 unicast submode.

The benefit of the top label hash feature is that it can be used when a user wants to monitor all bundles along with members to ensure they are up and running.

Use Case Scenario

Consider the following example:



All devices have static LSPs to forward the traffic corresponding to monitoring. OAM server constructs the packets with number of labels equal to the number of hops between two ends (server to server). So, for the example shown, the packet has four labels.

Packet example:

- Packet 1: label A1, B1, C1, D1
- Packet 2: label A2, B2, C2, D2
- Packet 3: Label A3, B3, C3, D3

Top label hashing is required because you do not want to hash based on "Dx" label in every hop.

Top label hashing allows, ASR9000-1 to make decision based on "Ax" label, ASR9000-2 to make decision on "Bx" label, ASR9000-3 to make decision based on "Cx" label and so on. The user needs to define the sequence of labels to be used, such that each label uses different bundle member.

If server receives the packet back as expected, then that means end-to-end path is good and members are functioning correctly.

Forwarding Labeled Packets

This section describes how labeled packets are forwarded in MPLS networks, how forwarding labeled packets are different from forwarding IP packets, how labeled packets are load-balanced, and what a LSR does with a packet with an unknown label.

Top Label Value

When a labeled packet is received, the label value at the top of the stack is looked up. The LSR sees the 20-bit field in the top label, which carries the actual value of the label. As a result of a successful lookup, the LSR learns:

- the next hop to which the packet is to be forwarded.
- what label operation to be performed before forwarding - swap, push, or pop.

The processing is always based on the top label, without regard to the possibility that in the past some other number of another label may have been "above it", or at present that some other number of another label may be below it. An unlabeled packet can be thought of as a packet whose label stack is empty (that is, a packet whose label stack has depth zero).

IP Lookup Versus Label Lookup

When a router receives an IP packet, an IP lookup is done. This means that the packet is looked up in the Cisco Express Forwarding (CEF) table. When a router receives a labeled packet, the label forwarding information base (LFIB) of the router is looked up. The router knows by looking at the protocol field in the Layer 2 header what type of packet it receives: a labeled packet or an IP packet.

Load Balancing Labeled Packets

If multiple equal-cost paths exist for an IPv4 prefix, Cisco IOS XR Software can load-balance labeled packets. When labeled packets are load-balanced, they can have the same or different outgoing labels. The outgoing labels are the same if the two links are between a pair of routers and both links belong to the platform label space. If multiple next-hop LSRs exist, the outgoing label for each path is usually different, because the next-hop LSRs assign labels independently.

Unknown Label

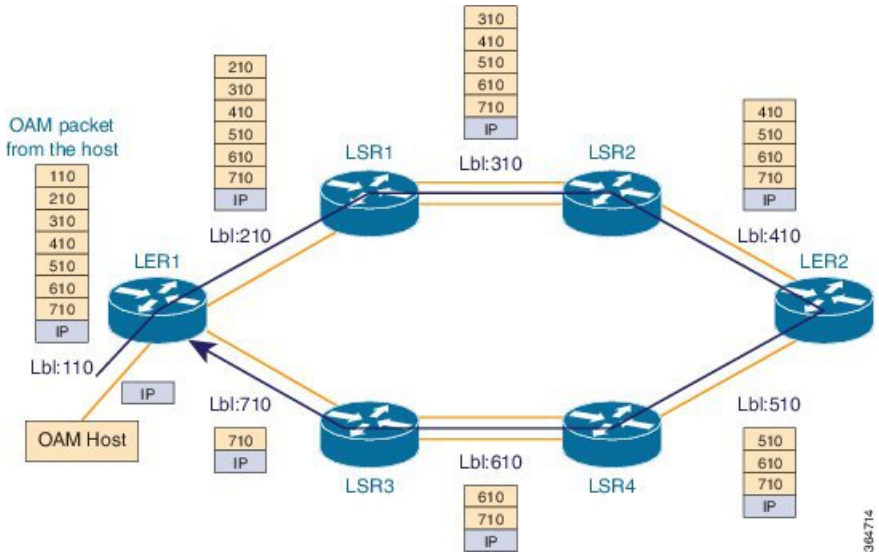
In regular operations, an LSR should receive only a labeled packet with a label at the top of the stack that is known to the LSR, because the LSR would have previously advertised that label. However, it is possible, in some cases, when something goes amiss in the MPLS network, the LSR starts receiving labeled packets with a top label that the LSR does not find in its LFIB. In such cases, the LSR drops the packet.

Functional Overview: Top Label Hash

The user configured top label hash value is pushed to the hardware abstraction layer (HAL). The FIB of the router computes the hash value based on the LSP paths and programs this hash value in the data plane. Based on the hash value, the OAM packet is then forwarded to the LAG member.

Figure 11: MPLS Top Label Hash for OAM Packets

This figure shows an OAM packet traversing different LAG members based on the top label hash value.



The OAM host sends the OAM packet with full label stack of the static LSP path. The packet is loop over bundle interface from LER1 > LSR1 > LSR2 > LER2 > LSR4 > LSR3 > LER1.

Each static LSP out-label is programmed as a 'pop' label.

Enable MPLS Encapsulation on an Interface

By default, MPLS encapsulation is disabled on all interfaces. MPLS encapsulation has to be explicitly enabled on all ingress and egress MPLS interfaces through which the static MPLS labeled traffic travels.

SUMMARY STEPS

1. **configure**
2. **mpls static**
3. **interface** *interface*
4. **commit**

DETAILED STEPS

Procedure

Step 1 **configure**

Step 2 **mpls static**

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls static
```

Enters MPLS-static configuration mode.

Step 3 **interface** *interface*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static)# interface gigabitethernet 0/0/0/3
```

Enables MPLS encapsulation on the specified interface.

Step 4 **commit**

What to do next

To verify the interfaces on which MPLS is enabled, use the **show mpls interfaces** command from the EXEC mode. For example:

```
RP/0/RSP0/CPU0:router# show  mpls interfaces
Mon May 12 06:21:30.937 DST
Interface                  LDP      Tunnel   Static   Enabled
-------------------------- -------- -------- -------- --------
GigabitEthernet0/0/0/3     No       No       Yes      Yes
```

For the interface on which MPLS static is enabled, the "Static" column displays "Yes".

Define a Range for Static MPLS Labels

The MPLS label range configuration defines the dynamic label range. Any label that falls outside this dynamic range is available for manually allocating as static labels. The router does not verify statically-configured labels against the specified label range. Therefore, to prevent label discrepancy, ensure that you do not configure static MPLS labels that fall within the dynamic label range.

Note For Cisco IOS XR software release 7.5.2 onwards, MPLS static supports 200G Ethernet.

Note The allocable range for MPLS labels is from 16 to 1048575. Label values from 0 to15 are reserved according to RFC-3032.

SUMMARY STEPS

1. **configure**
2. **mpls label range** *minimum_value maximum_value*
3. **commit**

DETAILED STEPS

Procedure

Step 1 **configure**

Step 2 **mpls label range** *minimum_value maximum_value*

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls label range 20000 30000
```

Specifies the range through which dynamic MPLS labels are allocated. All labels falling outside this range (16 to 19999 and 30001 to 1048575) can be manually allocated as static labels.

Step 3 **commit**

Setup a Static LSP

In this task, a static MPLS LSP is setup for a specific ingress label.

SUMMARY STEPS

1. **configure**
2. **mpls static**
3. **address-family ipv4 unicast**
4. **local-label** *label-value* **allocate**
5. **forward path** *path_id* **nexthop** *nexthop_address interface_type interface_id* **out-label** *outgoing_label*
6. **commit**

DETAILED STEPS

Procedure

Step 1 **configure**

Step 2 **mpls static**

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls static
```

Enters MPLS-static configuration mode.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static)# address-family ipv4 unicast
```

Applies the static configuration to an IPv4 address family in the default VRF.

Step 4 **local-label** *label-value* **allocate**

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static-af)# local-label 30500 allocate
```

Specifies the incoming label value as 30500.

Step 5 **forward path** *path_id* **nexthop** *nexthop_address interface_type interface_id* **out-label** *outgoing_label*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static-af-lbl)# forward path 1 nexthop 10.2.2.2 gigabitEthernet
0/0/0/1 out-label 30501
```

For packets that are received with the label, 30500, the MPLS protocol swaps labels and applies the label, 30501. After applying the new label, it forwards the packets to the next hop, 10.2.2.2, through the GigabitEthernet interface, 0/0/0/1.

Step 6 **commit**

Allocate Static MPLS Label to an IP Prefix and Configure a LSP

Static MPLS label bindings for IP prefixes are used by MPLS applications such as Label Distribution Protocol (LDP) or Border Gateway Protocol (BGP) for MPLS switching. It is possible to define a static LSP for the static label.

SUMMARY STEPS

1. **configure**
2. **mpls static**
3. **address-family ipv4 unicast**
4. **local-label** *label-value* **allocate per-prefix** *IPv4_prefix_entry*
5. **forward path** *path_id* **nexthop** *nexthop_address* **out-label** *outgoing_label*
6. **commit**

DETAILED STEPS

Procedure

Step 1 **configure**

Step 2 **mpls static**

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls static
```

Enters MPLS-static configuration mode.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static)# address-family ipv4 unicast
```

Applies the static configuration to an IPv4 address family in the default VRF.

Step 4 **local-label** *label-value* **allocate per-prefix** *IPv4_prefix_entry*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static-af)# local-label 30500 allocate per-prefix 100.1.1.0/24
```

The MPLS protocol requests label 30500 to be statically bound as a local label for the prefix 100.1.1.0/24.

Step 5 **forward path** *path_id* **nexthop** *nexthop_address* **out-label** *outgoing_label*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static-af-lbl)# forward path 1 nexthop 10.2.2.2 out-label 30501
```

For packets that are received with the label, 30500, the MPLS protocol swaps labels and applies the label, 30501. After applying the new label, it forwards the packets to the next hop, 10.2.2.2.

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static-af-lbl)# forward path 1 nexthop gigabitEthernet 0/0/0/4
out-label pop
```

For packets that are received with the label, 30500, the MPLS protocol removes the existing label. After removing the label, it forwards the packets to the next hop through the egress interface, GigabitEthernet 0/0/0/4.

Step 6 **commit**

Allocate Static MPLS Label for a Specific VRF

In this task, a static MPLS label is allocated to an IP prefix for a specific VRF.

Note When a static MPLS label is allocated to an IP prefix for a specific VRF, it is not possible to define a static LSP for that static label.

SUMMARY STEPS

1. **configure**
2. **mpls static**
3. **vrf** *vrf_name* **address-family ipv4 unicast**
4. • **local-label** *label-value* **allocate per-prefix** *IPv4_prefix_entry*
   • **local-label** *label-value* **allocate per-vrf** forward **path** *path-id* **pop-and-lookup**
5. **commit**

DETAILED STEPS

Procedure

Step 1 **configure**

Step 2 **mpls static**

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls static
```

Enters MPLS-static configuration mode.

Step 3 **vrf** *vrf_name* **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static)# vrf vrf1 address-family ipv4 unicast
```

Applies the static configuration to an IPv4 address family in the VRF named *vrf1*.

Step 4
- **local-label** *label-value* **allocate per-prefix** *IPv4_prefix_entry*
- **local-label** *label-value* **allocate per-vrf** forward **path** *path-id* **pop-and-lookup**

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static-vrf-af)# local-label 30500 allocate per-prefix 100.1.1.0/24
```

The MPLS protocol requests label 30500 to be statically bound as a local label for the prefix 100.1.1.0/24 in the VRF named *vrf1*.

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-static-vrf-af)# local-label 30500 allocate per-vrf forward path 1
 pop-and-lookup
```

The MPLS protocol requests single label 30500 to be statically bound as a local label for all the prefixes in the VRF named *vrf1*. When the router receives packets with VRF label 30500, it removes the label and then performs IP-based lookup to forward the packets.

Step 5 **commit**

Verify MPLS Static Bindings

These are the show commands that can be used to verify MPLS static bindings and LSPs.

SUMMARY STEPS

1. **show mpls static local-label** *label_value*
2. **show mpls label range**
3. **show mpls lsd forwarding**

DETAILED STEPS

Procedure

Step 1 **show mpls static local-label** *label_value*

Example:

```
RP/0/RSP0/CPU0:router#show mpls static local-label 200
Tue Apr 22 18:21:55.764 UTC
Label   VRF             Type         Prefix           RW Configured   Status
------- --------------- ------------ ---------------- --------------- --------
200     default         Per-Prefix   10.10.10.10/32   Yes             Created
```

Verifies that the status is "Created" for the specified label value.

Step 2 **show mpls label range**

Example:

```
RP/0/RSP0/CPU0:router#show mpls label range
Mon Apr 28 19:56:00.596 IST
Range for dynamic labels: Min/Max: 16000/1048575
```

Checks the dynamic range and ensures that the specified local-label value is outside this range.

Step 3 **show mpls lsd forwarding**

Example:

```
RP/0/RSP0/CPU0:router#show mpls lsd forwarding
Tue Apr 29 15:59:52.011 UTC
In_Label, (ID), Path_Info: <Type>
89, (IPv4, 'default':4U, 10.6.2.55/32), 1 Paths
   1/1: IPv4, 'default':4U, Gi0/0/0/21, nh=0.0.0.0, lbl=89, tun_id=0, flags=0x0 ()
110, (IPv4, 'default':4U, 172.16.0.1/32), 1 Paths
   1/1: IPv4, 'default':4U, Gi0/1/0/0, nh=10.12.1.2, lbl=Pop, tun_id=0, flags=0x0 ()
120, (IPv4, 'default':4U, 192.168.0.1/32), 1 Paths
   1/1: IPv4, 'default':4U, Gi0/1/0/0, nh=10.12.1.2, lbl=0, tun_id=0, flags=0x0 ()
130, (IPv4, 'default':4U, 209.165.201.1/32), 1 Paths
   1/1: IPv4, 'default':4U, Gi0/1/0/0, nh=10.12.1.2, lbl=200, tun_id=0, flags=0x0 ()
```

Verifies that the MPLS static configuration has taken effect, and the label forwarding is taking place.

Configuring Top Label Hash

Perform this task to configure MPLS top label hash entries.

SUMMARY STEPS

1. **configure**
2. **mpls static**
3. **address-family ipv4 unicast**
4. **top-label-hash**
5. **local-label** *label-value* **allocate**
6. **forward path** *path-count* **nexthop** *interface-type interface-id* **out-label pop**
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.

	Command or Action	Purpose
Step 2	**mpls static** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls static`	Enters MPLS-static configuration mode.
Step 3	**address-family ipv4 unicast** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-static)# address-family ipv4 unicast`	Applies the static configuration to an IPv4 address family.
Step 4	**top-label-hash** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-static-af)# top-label-hash`	Enables top label hash.
Step 5	**local-label** *label-value* **allocate** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-static-af-tlhash)# local-label 25000 allocate`	Specifies the incoming label value. In this example, the label value is 25000.
Step 6	**forward path** *path-count* **nexthop** *interface-type interface-id* **out-label pop** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-static-af-tlhash-lbl)# forward path 1 nexthop bundle-ether 1 out-label pop`	The received label is incremented by one and the label is swapped for the incremented label by the MPLS protocol. For example: For packets that are received with the label 25000, the MPLS protocol swaps labels and applies the label, 25001. After applying the new label, it forwards the packets to the next hop, through the specified interface (Bundle-Ether interface in this case). Sets the output label to 'pop' off the top of the label stack.
Step 7	**commit**	

Identify and Clear Label Discrepancy

During configuring or de-configuring static labels or a label range, a label discrepancy can get generated when:

- A static label is configured for an IP prefix (per VRF) that already has a binding with a dynamic label.
- A static label is configured for an IP prefix, when the same label value is dynamically allocated to another IP prefix.

Complete these steps to identify and clear the discrepancies.

Procedure

Step 1 To identify a label discrepancy, execute one of these:

- **show mpls static local-label discrepancy**
- **show log**

Example:

```
RP/0/RSP0/CPU0:router#show mpls static local-label discrepancy
Tue Apr 22 18:36:31.614 UTC
Label   VRF             Type         Prefix           RW Configured   Status
------- --------------- ------------ ---------------- --------------- --------
16003   default         Per-Prefix   10.0.0.1/32       No              Discrepancy
```

Example:

```
RP/0/RSP0/CPU0:router#show log
Thu Apr 24 14:18:57.655 UTC
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Console logging: level warnings, 199 messages logged
    Monitor logging: level debugging, 0 messages logged
    Trap logging: level informational, 0 messages logged
    Buffer logging: level debugging, 2 messages logged

Log Buffer (307200 bytes):

RP/0/RSP0/CPU0:Apr 24 14:18:53.743 : mpls_static[1043]:
%ROUTING-MPLS_STATIC-7-ERR_STATIC_LABEL_DISCREPANCY :
The system detected 1 label discrepancies (static label could not be allocated due to conflict with
 other applications).
Please use 'clear mpls static local-label discrepancy' to fix this issue.
RP/0/RSP0/CPU0:Apr 24 14:18:53.937 : config[65762]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed
 by user 'cisco'.
Use 'show configuration commit changes 1000000020' to view the changes.
```

Step 2 **clear mpls static local-label discrepancy all**

Example:

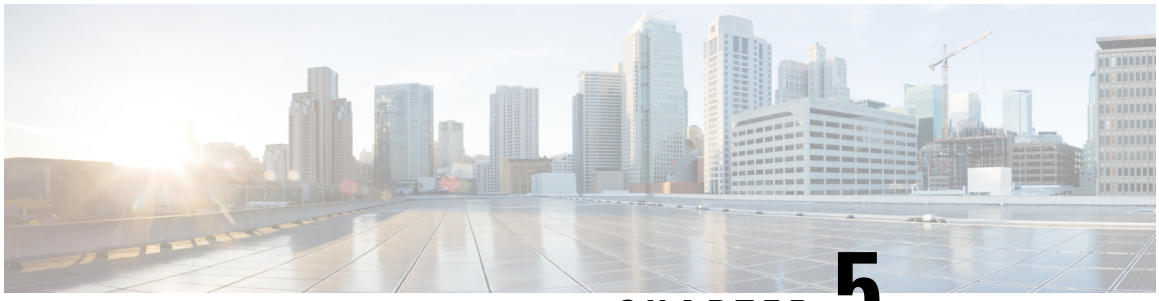
```
RP/0/RSP0/CPU0:router# clear mpls static local-label discrepancy all
```

Clears label discrepancy by allocating a new label to those IP prefixes that are allocated dynamic label. The static label configuration takes precedence while clearing discrepancy. Traffic can be affected while clearing discrepancy.

Configure Top Label Hash: Example

This example shows how to configure MPLS top label hash entries:

```
configure
 mpls static
   crossconnect 25000 bundle-ether 1 pop
   address-family ipv4 unicast
    top-label-hash
      local-label 25000 allocate forward path 1 nexthop bundle-ether 1 out-label pop
    !
   !
```



CHAPTER 5

Implementing RSVP for MPLS-TE

This module describes how to implement Resource Reservation Protocol (RSVP) for MPLS Traffic Engineering (MPLS-TE) on Cisco ASR 9000 Series Aggregation Services Routers.

The Multiprotocol Label Switching (MPLS) is a standards-based solution, driven by the Internet Engineering Task Force (IETF), devised to convert the Internet and IP backbones from best-effort networks into business-class transport media.

Resource Reservation Protocol (RSVP) is a signaling protocol that enables systems to request resource reservations from the network. RSVP processes protocol messages from other systems, processes resource requests from local clients, and generates protocol messages. As a result, resources are reserved for data flows on behalf of local and remote clients. RSVP creates, maintains, and deletes these resource reservations.

RSVP provides a secure method to control quality-of-service (QoS) access to a network.

MPLS Traffic Engineering (MPLS-TE) uses RSVP to signal label switched paths (LSPs).

Feature History for Implementing RSVP for MPLS-TE

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.0	The RSVP MIB feature was added.

- Prerequisites for Implementing RSVP for MPLS-TE , on page 145
- Usage Guidelines and Limitations, on page 146
- Information About Implementing RSVP for MPLS-TE , on page 146
- Information About Implementing RSVP Authentication, on page 152
- How to Implement RSVP, on page 157
- How to Implement RSVP Authentication, on page 169
- Configuration Examples for RSVP, on page 180
- Configuration Examples for RSVP Authentication, on page 184
- Additional References, on page 187

Prerequisites for Implementing RSVP for MPLS-TE

These prerequisites are required to implement RSVP for MPLS-TE :

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- Either a composite mini-image plus an MPLS package, or a full image, must be installed.

Usage Guidelines and Limitations

Consider these usage guidelines and limitations before implementing RSVP for MPLS-TE:

- To switch between an RSVP-TE or SR-TE configuration and an MPLS-TE configuration and vice versa, it is necessary to remove the configuration of the first process, say, RSVP-TE or SR-TE, in a separate commit operation and add the configuration of the next process, say, MPLS-TE, in another commit operation. This prevents any commit failures caused due to the delay in unconfiguring the first process before the next process configuration is applied.

Information About Implementing RSVP for MPLS-TE

To implement MPLS RSVP, you must understand the these concepts:

Related Topics

How to Implement RSVP Authentication, on page 169

Overview of RSVP for MPLS-TE

RSVP is a network control protocol that enables Internet applications to signal LSPs for MPLS-TE . The RSVP implementation is compliant with the IETF RFC 2205, and RFC 3209.

RSVP is automatically enabled on interfaces on which MPLS-TE is configured. For MPLS-TE LSPs with nonzero bandwidth, the RSVP bandwidth has to be configured on the interfaces. There is no need to configure RSVP, if all MPLS-TE LSPs have zero bandwidth .

RSVP Refresh Reduction, defined in RFC 2961, includes support for reliable messages and summary refresh messages. Reliable messages are retransmitted rapidly if the message is lost. Because each summary refresh message contains information to refresh multiple states, this greatly reduces the amount of messaging needed to refresh states. For refresh reduction to be used between two routers, it must be enabled on both routers. Refresh Reduction is enabled by default.

Message rate limiting for RSVP allows you to set a maximum threshold on the rate at which RSVP messages are sent on an interface. Message rate limiting is disabled by default.

The process that implements RSVP is restartable. A software upgrade, process placement or process failure of RSVP or any of its collaborators, has been designed to ensure Nonstop Forwarding (NSF) of the data plane.

RSVP supports graceful restart, which is compliant with RFC 3473. It follows the procedures that apply when the node reestablishes communication with the neighbor’s control plane within a configured restart time.

It is important to note that RSVP is not a routing protocol. RSVP works in conjunction with routing protocols and installs the equivalent of dynamic access lists along the routes that routing protocols calculate. Because of this, implementing RSVP in an existing network does not require migration to a new routing protocol.

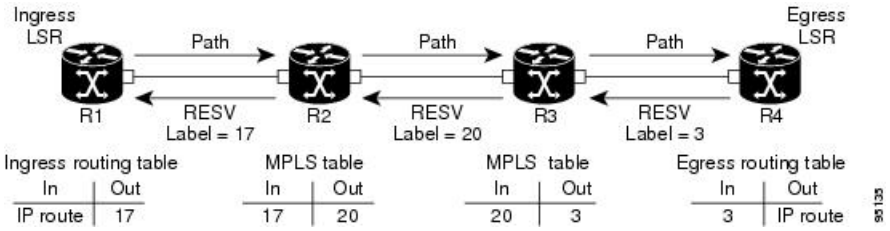
Related Topics

Configuring RSVP Packet Dropping, on page 160
Set DSCP for RSVP Packets: Example, on page 184
Verifying RSVP Configuration, on page 165

LSP Setup

LSP setup is initiated when the LSP head node sends path messages to the tail node (see the RSVP Operation figure).

Figure 12: RSVP Operation



The Path messages reserve resources along the path to each node, creating Path soft states on each node. When the tail node receives a path message, it sends a reservation (RESV) message with a label back to the previous node. When the reservation message arrives at the previous node, it causes the reserved resources to be locked and forwarding entries are programmed with the MPLS label sent from the tail-end node. A new MPLS label is allocated and sent to the next node upstream.

When the reservation message reaches the head node, the label is programmed and the MPLS data starts to flow along the path.

High Availability

RSVP is designed to ensure nonstop forwarding under the following constraints:

- Ability to tolerate the failure of one RP of a 1:1 redundant pair.
- Hitless software upgrade.

The RSVP high availability (HA) design follows the constraints of the underlying architecture where processes can fail without affecting the operation of other processes. A process failure of RSVP or any of its collaborators does not cause any traffic loss or cause established LSPs to go down. When RSVP restarts, it recovers its signaling states from its neighbors. No special configuration or manual intervention are required. You may configure RSVP graceful restart, which offers a standard mechanism to recover RSVP state information from neighbors after a failure.

Graceful Restart

RSVP graceful restart provides a control plane mechanism to ensure high availability (HA), which allows detection and recovery from failure conditions while preserving nonstop forwarding services on the systems running Cisco IOS XR software.

RSVP graceful restart provides a mechanism that minimizes the negative effects on MPLS traffic caused by these types of faults:

- Disruption of communication channels between two nodes when the communication channels are separate from the data channels. This is called *control channel failure*.
- Control plane of a node fails but the node preserves its data forwarding states. This is called *node failure*.

The procedure for RSVP graceful restart is described in the "Fault Handling" section of RFC 3473, *Generalized MPLS Signaling, RSVP-TE Extensions*. One of the main advantages of using RSVP graceful restart is recovery of the control plane while preserving nonstop forwarding and existing labels.

Note RSVP graceful restart feature is not supported when TE is running over multiple IGP instances which have different TE router-ids. This causes the TE tunnels to constantly flap.

Graceful Restart: Standard and Interface-Based

When you configure RSVP graceful restart, Cisco IOS XR software sends and expects node-id address based Hello messages (that is, Hello Request and Hello Ack messages). The RSVP graceful restart Hello session is not established if the neighbor router does not respond with a node-id based Hello Ack message.

You can also configure graceful restart to respond (send Hello Ack messages) to interface-address based Hello messages sent from a neighbor router in order to establish a graceful restart Hello session on the neighbor router. If the neighbor router does not respond with node-id based Hello Ack message, however, the RSVP graceful restart Hello session is not established.

Cisco IOS XR software provides two commands to configure graceful restart:

- **signalling hello graceful-restart**
- **signalling hello graceful-restart interface-based**

Note By default, graceful restart is disabled. To enable interface-based graceful restart, you must first enable standard graceful restart. You cannot enable interface-based graceful restart independently.

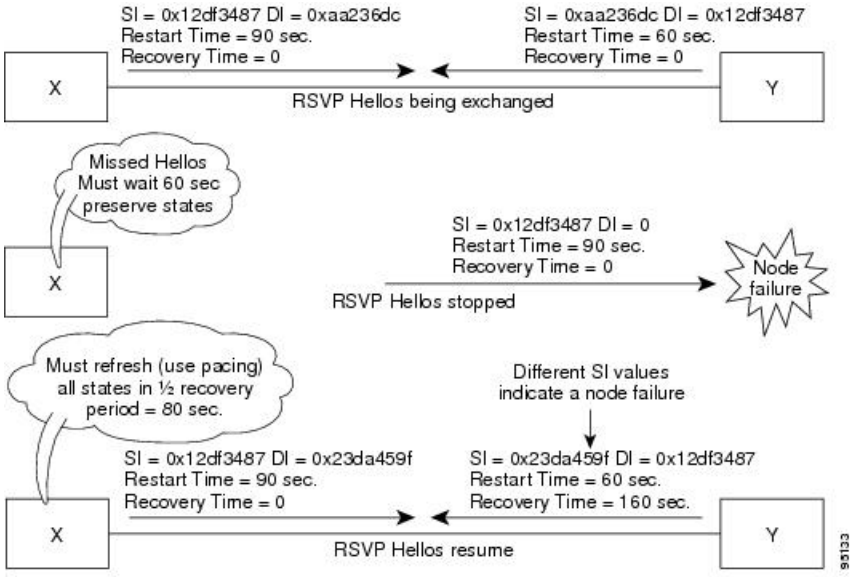
Related Topics

Enabling Graceful Restart, on page 158
Enable Graceful Restart: Example, on page 183
Enable Interface-Based Graceful Restart: Example, on page 183

Graceful Restart: Figure

Figure 13: Node Failure with RSVP

This figure illustrates how RSVP graceful restart handles a node failure condition.



RSVP graceful restart requires the use of RSVP hello messages. Hello messages are used between RSVP neighbors. Each neighbor can autonomously issue a hello message containing a hello request object. A receiver that supports the hello extension replies with a hello message containing a hello acknowledgment (ACK) object. This means that a hello message contains either a hello Request or a hello ACK object. These two objects have the same format.

The restart cap object indicates a node's restart capabilities. It is carried in hello messages if the sending node supports state recovery. The restart cap object has the following two fields:

Restart Time

Time after a loss in Hello messages within which RSVP hello session can be reestablished. It is possible for a user to manually configure the Restart Time.

Recovery Time

Time that the sender waits for the recipient to re-synchronize states after the re-establishment of hello messages. This value is computed and advertised based on number of states that existed before the fault occurred.

For graceful restart, the hello messages are sent with an IP Time to Live (TTL) of 64. This is because the destination of the hello messages can be multiple hops away. If graceful restart is enabled, hello messages (containing the restart cap object) are send to an RSVP neighbor when RSVP states are shared with that neighbor.

Restart cap objects are sent to an RSVP neighbor when RSVP states are shared with that neighbor. If the neighbor replies with hello messages containing the restart cap object, the neighbor is considered to be graceful restart capable. If the neighbor does not reply with hello messages or replies with hello messages that do not contain the restart cap object, RSVP backs off sending hellos to that neighbor. If graceful restart is disabled, no hello messages (Requests or ACKs) are sent. If a hello Request message is received from an unknown neighbor, no hello ACK is sent back.

ACL-based Prefix Filtering

RSVP provides for the configuration of extended access lists (ACLs) to forward, drop, or perform normal processing on RSVP router-alert (RA) packets. Prefix filtering is designed for use at core access routers in order that RA packets (identified by a source/destination address) can be seamlessly forwarded across the core from one access point to another (or, conversely to be dropped at this node). RSVP applies prefix filtering rules only to RA packets because RA packets contain source and destination addresses of the RSVP flow.



Note RA packets forwarded due to prefix filtering must not be sent as RSVP bundle messages, because bundle messages are hop-by-hop and do not contain RA. Forwarding a Bundle message does not work, because the node receiving the messages is expected to apply prefix filtering rules only to RA packets.

For each incoming RSVP RA packet, RSVP inspects the IP header and attempts to match the source/destination IP addresses with a prefix configured in an extended ACL. The results are as follows:

- If an ACL does not exist, the packet is processed like a normal RSVP packet.
- If the ACL match yields an explicit permit (and if the packet is not locally destined), the packet is forwarded. The IP TTL is decremented on all forwarded packets.
- If the ACL match yields an explicit deny, the packet is dropped.

If there is no explicit permit or explicit deny, the ACL infrastructure returns an implicit (default) deny. RSVP can be configured to drop the packet. By default, RSVP processes the packet if the ACL match yields an implicit (default) deny.

Related Topics

Configuring ACLs for Prefix Filtering, on page 159
Configure ACL-based Prefix Filtering: Example, on page 183

RSVP MIB

RFC 2206, RSVP Management Information Base Using SMIv2 defines all the SNMP MIB objects that are relevant to RSVP. By implementing the RSVP MIB, you can perform these functions:

- Specifies two traps (NetFlow and LostFlow) which are triggered when a new flow is created or deleted.
- Lets you use SNMP to access objects belonging to RSVP.

Related Topics

Enabling RSVP Traps, on page 168
Enable RSVP Traps: Example, on page 184

Bandwidth Reservation Percentage

The Bandwidth Reservation Percentage allows the RSVP interface bandwidth to be specified as percentages of the link's physical bandwidth.

MPLS-TE LSP OOR

MPLS-TE LSP OOR

The MPLS-TE LSP OOR function adds capability for the RSVP-TE control plane to track the LSP scale of transit routers, so that it can take a specific set of (pre-configured) actions when threshold limits are crossed, and inform other routers in the network. MPLS-TE keeps track of the number of transit LSPs set up through the router. The limits do not apply to ingress and egress LSP routers since they are driven by explicit configuration. In other words, the configuration determines how many egress or ingress LSPs a router has. For midpoint routers, the number is a function of the topology, the links metrics, and links' bandwidth.

State Transition Triggers - The LSP OOR state transition is triggered by checking the total transit LSP count and the unprotected count. If either count crosses the threshold, the state transition is triggered. If both counts cross the limit, the more critical state is chosen. Each limit will have a value for the *Yellow* threshold and a value for the *Red* threshold. When these thresholds are crossed, the configured MPLS-TE LSP OOR actions take effect. Similarly, the transition to *Green* state occurs when the LSP numbers drop.

LSP OOR State Dampening - The reason for LSP OOR State Dampening is that the number of accepted LSPs would be at the threshold and once an LSP is deleted, the state goes back from Red to Yellow, and a new LSP is setup and the state goes back to Red.

The solution is to introduce dampening when there is a state transition from Red to Yellow or from Yellow to Green. Whenever the transit number of LSPs crosses down a threshold, a timer is started for 10 seconds. After the timer expires, the new state is computed and moved to it. The timer is stopped if the transit number threshold is crossed (up) again. The transition from a state to a more severe state is not dampened.

Low and High Priority LSPs - When the LSP OOR is in yellow or red state, new high priority LSPs will not preempt low priority LSPs. Preemption can still occur but only for bandwidth reasons. In other words, if the router is in Red state where one of the actions is to reject any new LSP, the new high-priority LSPs are rejected even if there is an established low-priority LSP. The low-priority LSP is not removed to make room for the high-priority one.

Configuration Limit - Setting the configured limit to a value that is smaller than the current number of LSPs will trigger state transition but will not cause existing LSPs to be deleted or preempted. Setting the configured limit to a value that is larger than the current number of LSPs takes the node out of LSP OOR state. When an LSP cannot be admitted due to LSP OOR, the LSRs send Path Error messages to the LERs.

Event Logging - This is generated when the system transitions across OOR states, such as a resource change into an *yellow* or *red* state. Reporting level for *Red* is critical (1), and for yellow is warning (4). The following example shows that the count has crossed the threshold of 5000.

```
RP/0/RP1/CPU0:May 15 17:05:48 PDT: te_control[1034]: %ROUTING-MPLS_TE-4-LSP_OOR :

Transit LSP resources changed to Yellow.
Total transit: configured threshold 5000; actual count 5001;
Unprotected transit: configured threshold 4294967295; actual count 0
```

When the resource comes out of OOR, it will report as *green*.

Configuration Example

```
mpls traffic-eng
 lsp-oor
  green
   action accept reopt-lsp
   action flood available-bw 20
   recovery-duration
   action admit lsp-min-bw   X   -- > (in kbps, a lower limit than yellow and red state)
```

```
yellow
 transit-all threshold 75000
 action accept reopt-lsp
 action flood available-bw 0
 action admit lsp-min-bw  Y

red
 transit-all threshold 90000
 action flood available-bw 0
 action admit lsp-min-bw Z
```

The LSP OOR threshold values are set to yellow as 75000 and red as 90000. When these thresholds are crossed, corresponding actions are applied to all the TE interfaces.

Note The default values of the above thresholds are infinite.

When the LSP OOR *yellow* state is reached, the **accept reopt-lsp** action, **flood available-bw 0** action and **admit lsp-min-bw** actions are activated. This allows headend routers to reoptimize existing LSPs through, but doesn't allow new LSPs to get established. Also, MPLS-TE advertises zero bandwidth out of all interfaces, making this transit router less preferable for new LSPs. To handle a sudden burst of new LSPs that get signaled, the **action admit lsp-min-bw** function ensures only a small number of high bandwidth LSPs get provisioned through the affected router. When the red threshold state is crossed, the **flood available-bw 0** and **admit lsp-min-bw** actions prevent any additional or reoptimized transit LSPs from getting set up through the affected router.

Information About Implementing RSVP Authentication

Before implementing RSVP authentication, you must configure a keychain first. The name of the keychain must be the same as the one used in the keychain configuration. For more information about configuring keychains, see *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Note RSVP authentication supports only keyed-hash message authentication code (HMAC) type algorithms.

To implement RSVP authentication on Cisco IOS XR software, you must understand the following concepts:

RSVP Authentication Functions

You can carry out these tasks with RSVP authentication:

- Set up a secure relationship with a neighbor by using secret keys that are known only to you and the neighbor.
- Configure RSVP authentication in global, interface, or neighbor configuration modes.
- Authenticate incoming messages by checking if there is a valid security relationship that is associated based on key identifier, incoming interface, sender address, and destination address.
- Add an integrity object with message digest to the outgoing message.

- Use sequence numbers in an integrity object to detect replay attacks.

RSVP Authentication Design

Network administrators need the ability to establish a security domain to control the set of systems that initiates RSVP requests.

The RSVP authentication feature permits neighbors in an RSVP network to use a secure hash to sign all RSVP signaling messages digitally, thus allowing the receiver of an RSVP message to verify the sender of the message without relying solely on the sender's IP address.

The signature is accomplished on a per-RSVP-hop basis with an RSVP integrity object in the RSVP message as defined in RFC 2747. This method provides protection against forgery or message modification. However, the receiver must know the security key used by the sender to validate the digital signature in the received RSVP message.

Network administrators manually configure a common key for each RSVP neighbor on the shared network.

The following reasons explain how to choose between global, interface, or neighbor configuration modes:

- Global configuration mode is optimal when a router belongs to a single security domain (for example, part of a set of provider core routers). A single common key set is expected to be used to authenticate all RSVP messages.
- Interface, or neighbor configuration mode, is optimal when a router belongs to more than one security domain. For example, a provider router is adjacent to the provider edge (PE), or a PE is adjacent to an edge device. Different keys can be used but not shared.

Global configuration mode configures the defaults for interface and neighbor interface modes. These modes, unless explicitly configured, inherit the parameters from global configuration mode, as follows:

- Window-size is set to 1.
- Lifetime is set to 1800.
- **key-source key-chain** command is set to none or disabled.

Related Topics

Configuring a Lifetime for an Interface for RSVP Authentication, on page 173
RSVP Authentication by Using All the Modes: Example, on page 186

Global, Interface, and Neighbor Authentication Modes

You can configure global defaults for all authentication parameters including key, window size, and lifetime. These defaults are inherited when you configure authentication for each neighbor or interface. However, you can also configure these parameters individually on a neighbor or interface basis, in which case the global values (configured or default) are no longer inherited.



Note RSVP uses the following rules when choosing which authentication parameter to use when that parameter is configured at multiple levels (interface, neighbor, or global). RSVP goes from the most specific to least specific; that is, neighbor, interface, and global.

Global keys simplify the configuration and eliminate the chances of a key mismatch when receiving messages from multiple neighbors and multiple interfaces. However, global keys do not provide the best security.

Interface keys are used to secure specific interfaces between two RSVP neighbors. Because many of the RSVP messages are IP routed, there are many scenarios in which using interface keys are not recommended. If all keys on the interfaces are not the same, there is a risk of a key mismatch for the following reasons:

- When the RSVP graceful restart is enabled, RSVP hello messages are sent with a source IP address of the local router ID and a destination IP address of the neighbor router ID. Because multiple routes can exist between the two neighbors, the RSVP hello message can traverse to different interfaces.
- When the RSVP fast reroute (FRR) is active, the RSVP Path and Resv messages can traverse multiple interfaces.
- When Generalized Multiprotocol Label Switching (GMPLS) optical tunnels are configured, RSVP messages are exchanged with router IDs as the source and destination IP addresses. Since multiple control channels can exist between the two neighbors, the RSVP messages can traverse different interfaces.

Neighbor-based keys are particularly useful in a network in which some neighbors support RSVP authentication procedures and others do not. When the neighbor-based keys are configured for a particular neighbor, you are advised to configure all the neighbor's addresses and router IDs for RSVP authentication.

Related Topics

Configuring a Lifetime for RSVP Authentication in Global Configuration Mode, on page 170
RSVP Authentication Global Configuration Mode: Example, on page 185
Specifying the RSVP Authentication Keychain in Interface Mode, on page 172
RSVP Authentication by Using All the Modes: Example, on page 186

Security Association

A security association (SA) is defined as a collection of information that is required to maintain secure communications with a peer to counter replay attacks, spoofing, and packet corruption.

This table lists the main parameters that define a security association.

Table 4: Security Association Main Parameters

Parameter	Description
src	IP address of the sender.
dst	IP address of the final destination.
interface	Interface of the SA.
direction	Send or receive type of the SA.
Lifetime	Expiration timer value that is used to collect unused security association data.
Sequence Number	Last sequence number that was either sent or accepted (dependent of the direction type).
key-source	Source of keys for the configurable parameter.
keyID	Key number (returned form the key-source) that was last used.

Parameter	Description
digest	Algorithm last used (returned from the key-source).
Window Size	Specifies the tolerance for the configurable parameter. The parameter is applicable when the direction parameter is the receive type.
Window	Specifies the last *window size* value sequence number that is received or accepted. The parameter is applicable when the direction parameter is the receive type.

An SA is created dynamically when sending and receiving messages that require authentication. The neighbor, source, and destination addresses are obtained either from the IP header or from an RSVP object, such as a HOP object, and whether the message is incoming or outgoing.

When the SA is created, an expiration timer is created. When the SA authenticates a message, it is marked as recently used. The lifetime timer periodically checks if the SA is being used. If so, the flag is cleared and is cleaned up for the next period unless it is marked again.

This table shows how to locate the source and destination address keys for an SA that is based on the message type.

Table 5: Source and Destination Address Locations for Different Message Types

Message Type	Source Address Location	Destination Address Location
Path	HOP object	SESSION object
PathTear	HOP object	SESSION object
PathError	HOP object	IP header
Resv	HOP object	IP header
ResvTear	HOP object	IP header
ResvError	HOP object	IP header
ResvConfirm	IP header	CONFIRM object
Ack	IP header	IP header
Srefresh	IP header	IP header
Hello	IP header	IP header
Bundle	—	—

Related Topics

Specifying the Keychain for RSVP Neighbor Authentication, on page 175
RSVP Neighbor Authentication: Example, on page 186
Configuring a Lifetime for RSVP Neighbor Authentication, on page 176
RSVP Authentication Global Configuration Mode: Example, on page 185

Key-source Key-chain

The key-source key-chain is used to specify which keys to use.

You configure a list of keys with specific IDs and have different lifetimes so that keys are changed at predetermined intervals automatically, without any disruption of service. Rollover enhances network security by minimizing the problems that could result if an untrusted source obtained, deduced, or guessed the current key.

RSVP handles rollover by using the following key ID types:

- On TX, use the youngest eligible key ID.
- On RX, use the key ID that is received in an integrity object.

For more information about implementing keychain management, see *System Security Configuration Guide for Cisco ASR 9000 Series Routers*.

Related Topics

Enabling RSVP Authentication Using the Keychain in Global Configuration Mode, on page 169
RSVP Authentication Global Configuration Mode: Example, on page 185
Specifying the Keychain for RSVP Neighbor Authentication, on page 175
RSVP Neighbor Authentication: Example, on page 186

Guidelines for Window-Size and Out-of-Sequence Messages

These guidelines are required for window-size and out-of-sequence messages:

- Default window-size is set to 1. If a single message is received out-of-sequence, RSVP rejects it and displays a message.
- When RSVP messages are sent in burst mode (for example, tunnel optimization), some messages can become out-of-sequence for a short amount of time.
- Window size can be increased by using the **window-size** command. When the window size is increased, replay attacks can be detected with duplicate sequence numbers.

Related Topics

Configuring the Window Size for RSVP Authentication in Global Configuration Mode, on page 171
Configuring the Window Size for an Interface for RSVP Authentication, on page 174
Configuring the Window Size for RSVP Neighbor Authentication, on page 177
RSVP Authentication by Using All the Modes: Example, on page 186
RSVP Authentication for an Interface: Example, on page 185

Caveats for Out-of-Sequence

These caveats are listed for out-of-sequence:

- When RSVP messages traverse multiple interface types with different maximum transmission unit (MTU) values, some messages can become out-of-sequence if they are fragmented.
- Packets with some IP options may be reordered.

- Change in QoS configurations may lead to a transient reorder of packets.
- QoS policies can cause a reorder of packets in a steady state.

Because all out-of-sequence messages are dropped, the sender must retransmit them. Because RSVP state timeouts are generally long, out-of-sequence messages during a transient state do not lead to a state timeout.

How to Implement RSVP

RSVP requires coordination among several routers, establishing exchange of RSVP messages to set up LSPs. Depending on the client application, RSVP requires some basic configuration, as described in these topics:

Configuring Traffic Engineering Tunnel Bandwidth

To configure traffic engineering tunnel bandwidth, you must first set up TE tunnels and configure the reserved bandwidth per interface (there is no need to configure bandwidth for the data channel or the control channel).

Cisco IOS XR software supports two MPLS DS-TE modes: Prestandard and IETF.

Note For prestandard DS-TE you do not need to configure bandwidth for the data channel or the control channel. There is no other specific RSVP configuration required for this application. When no RSVP bandwidth is specified for a particular interface, you can specify zero bandwidth in the LSP setup if it is configured under RSVP interface configuration mode or MPLS-TE configuration mode.

Related Topics

Configuring a Prestandard DS-TE Tunnel, on page 282
Configuring an IETF DS-TE Tunnel Using RDM, on page 283
Configuring an IETF DS-TE Tunnel Using MAM, on page 285

Confirming DiffServ-TE Bandwidth

Perform this task to confirm DiffServ-TE bandwidth.

In RSVP global and subpools, reservable bandwidths are configured per interface to accommodate TE tunnels on the node. Available bandwidth from all configured bandwidth pools is advertised using IGP. RSVP signals the TE tunnel with appropriate bandwidth pool requirements.

SUMMARY STEPS

1. **configure**
2. **rsvp**
3. **interface** *type interface-path-id*
4. **bandwidth** *total-bandwidth max-flow* **sub-pool** *sub-pool-bw*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp** **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp`	Enters RSVP configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp)# interface pos 0/2/0/0`	Enters interface configuration mode for the RSVP protocol.
Step 4	**bandwidth** *total-bandwidth max-flow* **sub-pool** *sub-pool-bw* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if)# bandwidth 1000 100 sub-pool 150`	Sets the reservable bandwidth, the maximum RSVP bandwidth available for a flow and the sub-pool bandwidth on this interface.
Step 5	**commit**	

Related Topics

Differentiated Services Traffic Engineering, on page 208
Bandwidth Configuration (MAM): Example, on page 181
Bandwidth Configuration (RDM): Example, on page 181

Enabling Graceful Restart

Perform this task to enable graceful restart for implementations using both node-id and interface-based hellos.

RSVP graceful restart provides a control plane mechanism to ensure high availability, which allows detection and recovery from failure conditions while preserving nonstop forwarding services.

SUMMARY STEPS

1. **configure**
2. **rsvp**
3. **signalling graceful-restart**
4. **signalling graceful-restart interface-based**
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp** **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp`	Enters the RSVP configuration mode.
Step 3	**signalling graceful-restart** **Example:** `RP/0/RSP0/CPU0:router(config-rsvp)# signalling graceful-restart`	Enables the graceful restart process on the node.
Step 4	**signalling graceful-restart interface-based** **Example:** `RP/0/RSP0/CPU0:router(config-rsvp)# signalling graceful-restart interface-based`	Enables interface-based graceful restart process on the node.
Step 5	**commit**	

Related Topics

Graceful Restart: Standard and Interface-Based, on page 148
Enable Graceful Restart: Example, on page 183
Enable Interface-Based Graceful Restart: Example, on page 183

Configuring ACL-based Prefix Filtering

Two procedures are provided to show how RSVP Prefix Filtering is associated:

- Configuring ACLs for Prefix Filtering, on page 159
- Configuring RSVP Packet Dropping, on page 160

Configuring ACLs for Prefix Filtering

Perform this task to configure an extended access list ACL that identifies the source and destination prefixes used for packet filtering.

Note The extended ACL needs to be configured separately using extended ACL configuration commands.

SUMMARY STEPS

1. **configure**
2. **rsvp**
3. **signalling prefix-filtering access-list**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp** **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp`	Enters the RSVP configuration mode.
Step 3	**signalling prefix-filtering access-list** **Example:** `RP/0/RSP0/CPU0:router(config-rsvp)# signalling prefix-filtering access-list banks`	Enter an extended access list name as a string.
Step 4	**commit**	

Related Topics

ACL-based Prefix Filtering, on page 150
Configure ACL-based Prefix Filtering: Example, on page 183

Configuring RSVP Packet Dropping

Perform this task to configure RSVP to drop RA packets when the ACL match returns an implicit (default) deny.

The default behavior performs normal RSVP processing on RA packets when the ACL match returns an implicit (default) deny.

SUMMARY STEPS

1. **configure**
2. **rsvp**
3. **signalling prefix-filtering default-deny-action**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp** **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp`	Enters the RSVP configuration mode.
Step 3	**signalling prefix-filtering default-deny-action** **Example:** `RP/0/RSP0/CPU0:router(config-rsvp)# signalling prefix-filtering default-deny-action`	Drops RA messages.
Step 4	**commit**	

Related Topics

Overview of RSVP for MPLS-TE, on page 146
Set DSCP for RSVP Packets: Example, on page 184

Configuring Refresh Reduction

Table 6: Feature History Table

Feature Name	Release Information	Feature Description
Set Global RSVP Message Retransmission Interval	Release 24.1.1	During Fast Reroute (FRR), an RSVP router sends multiple messages to neighbors. If a neighbor fails to acknowledge the messages due to an overload of RSVP message processing or a high frequency of failures, RSVP retransmits the messages, which can result in network congestion. You can now set a longer RSVP message retransmission interval to provide sufficient processing time for neighbors, reduce signaling overhead, and prevent network congestion. You can set this interval for all directly connected neighbors at once or remote neighbors connected through backup tunnels. Previously, you could only enable this option per interface. The feature introduces these changes: **CLI**: **signalling refresh reduction reliable retransmit-time (RSVP configuration)** **YANG Data Model**: `Cisco-IOS-XR-ip-rsvp-cfg.yang` (see GitHub, YANG Data Models Navigator)

RSVP Refresh Reduction improves the reliability of Resource Reservation Protocol (RSVP) signaling to enhance network performance and message delivery and it is enabled by default. Refresh reduction is used with a neighbor only if the neighbor supports it. You can also disable refresh reduction on an interface if you want.

This feature ensures reliable delivery of RSVP messages when network traffic is disrupted. To ensure that its message is delivered to its neighbor, RSVP requests the neighbor to send an acknowledgment message by a given time duration. If it doesn't receive the acknowledgment, it resends the message and doubles its current wait time. After 5 attempts, RSVP stops retransmitting the message to the neighbor.

Set Global RSVP Message Retransmission Interval

During FRR, RSVP reroutes tunnels with failed links. With the default RSVP message retransmission interval in use, when a large number of LSPs are rerouted simultaneously, an RSVP router sends a large number of messages to its neighbor – whether connected directly or through a backup tunnel – and this may overwhelm its processing load. While the neighbor is still processing messages, the RSVP router retransmits the earlier messages, further overwhelming it and causing network congestion.

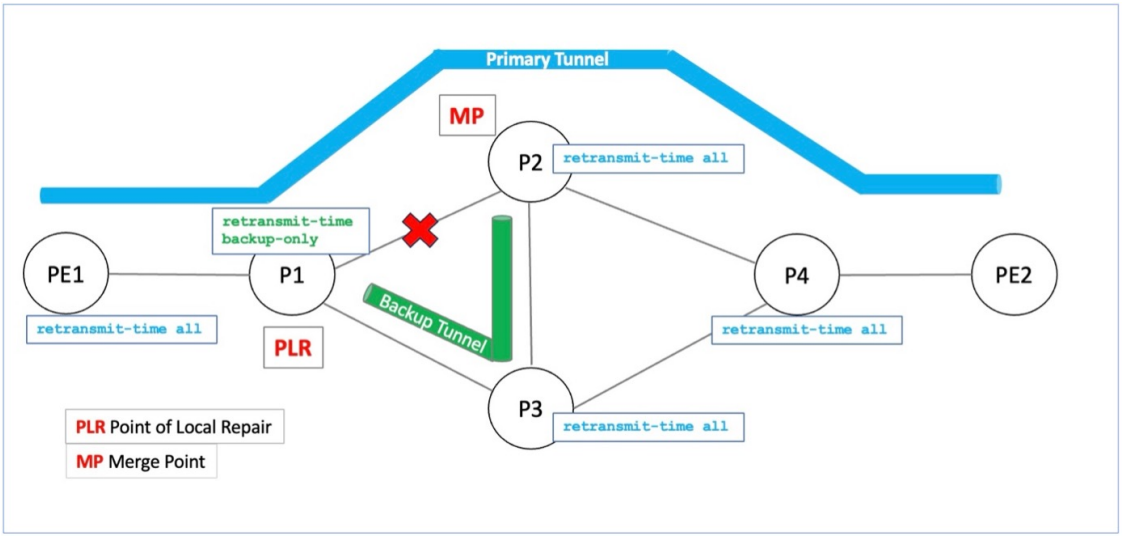
This feature allows you to configure a global timer with a longer retransmission interval so that retransmissions are relatively relaxed and provide more time for the neighbor to acknowledge messages.

To set the retransmission interval for messages sent over the backup tunnel during FRR, use the **backup-only** configuration which applies the RSVP-global configuration on backup tunnels. Another advantage of this configuration is that the interval is automatically applied to auto-backup tunnels, which are created dynamically.

Alternatively, to set the retransmission interval for all RSVP messages sent with reliable messaging (Path, Resv, PathTear, ResvTear, etc), use the **all** configuration which applies the RSVP-global configuration on all interfaces

Configuration Example for Set Global RSVP Message Retransmission Interval

Consider the following network topology.



Pointers:

- MPLS-TE, RSVP and Refresh-Reduction are enabled on all routers.
- The primary tunnel's path is PE1-P1-P2-P4-PE2.

  PE1 is the headend router, P1-to-P4 are Provider routers, and PE2 is the tail-end router.
- P1 is a potential Point of Local Repair (PLR) and headend of the backup tunnel with the path P1-P3-P2.

  ***PLR**: A router that creates a backup tunnel to handle link failures in the primary tunnel.*
- P2 is the Merge Point that merges the backup tunnel with the primary tunnel.

When P1 detects a link failure between P1-P2, it initiates FRR and reroutes the traffic through the backup tunnel.

In the following sections, the **backup-only** configuration is enabled on P1, and the **all** configuration is enabled on PE1, P2, P3 and P4.

PE1 Configuration

A retransmission interval of 4000 milliseconds is set for all RSVP-enabled PE1 interfaces:

```
PE1(config)# rsvp
PE1(config-rsvp)# signalling refresh reduction reliable retransmit-time all 4000
PE1(config-rsvp)# interface hundredGigE 0/0/0/0
PE1(config-rsvp-if)# bandwidth 200000
PE1(config-rsvp-if)# signalling refresh interval 180
PE1(config-rsvp-if)# signalling refresh reduction bundle-max-size 1400
PE1(config-rsvp-if)# commit
```

Similarly, enable configurations on P2, P3 and P4.

Verification

```
PE1# show rsvp interface detail

INTERFACE: HundredGigE0/0/0/0
..
           Retransmit: 4000ms. (Global)
```

RSVP message retransmission count:

```
PE1# show rsvp counters messages
HundredGigE0/0/0/0   Recv      Xmit
                      ..        ..
    Retransmit              8
    ..
```

RSVP message retransmission to its neighbors:

```
Router# show rsvp neighbors detail

Global Neighbor: 10.1.1.12
  Interface Neighbor: 10.2.2.10
  ..      Retransmitted messages: 34
```

Running Configuration

```
rsvp
  interface HundredGigE0/0/0/0
    bandwidth 200000
    signalling refresh interval 180
    signalling refresh reduction bundle-max-size 1400
    !
  signalling refresh reduction reliable retransmit-time all 4000
```

P1 Configuration

A retransmission interval of 5000 milliseconds is set for P1's backup tunnel interface.

Note This configuration is also applicable for auto-backup tunnels.

```
P1(config)# rsvp
P1(config-rsvp)# signalling refresh reduction reliable retransmit-time backup-only 5000
P1(config-rsvp)# interface hundredGigE 0/0/0/0
P1(config-rsvp-if)# bandwidth 200000
P1(config-rsvp-if)# signalling refresh interval 180
P1(config-rsvp-if)# signalling refresh reduction bundle-max-size 1400
P1(config-rsvp-if)# commit
```

Verification

```
P1# show rsvp interface detail

INTERFACE: HundredGigE0/0/0/0
```

```
..
                          Retransmit: 5000ms. (Global)
```

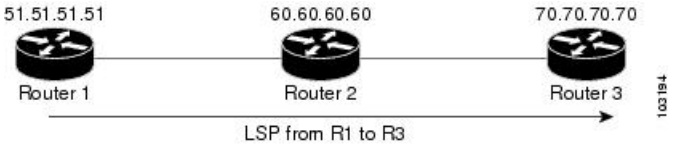
Running Configuration

```
rsvp
  interface HundredGigE0/0/0/0
    bandwidth 200000
    signalling refresh interval 180
    signalling refresh reduction bundle-max-size 1400
    !
  signalling refresh reduction reliable retransmit-time backup-only 500
```

Verifying RSVP Configuration

Figure 14: Sample Topology

This figure illustrates the topology.



Perform the following steps to verify RSVP configuration.

SUMMARY STEPS

1. **show rsvp session**
2. **show rsvp counters messages summary**
3. **show rsvp counters events**
4. **show rsvp interface** *type interface-path-id* [**detail**]
5. **show rsvp graceful-restart**
6. **show rsvp graceful-restart** [**neighbors** *ip-address* | **detail**]
7. **show rsvp interface**
8. **show rsvp neighbor**

DETAILED STEPS

Procedure

Step 1 **show rsvp session**

Verifies that all routers on the path of the LSP are configured with at least one Path State Block (PSB) and one Reservation State Block (RSB) per session.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp session

Type Destination Add DPort Proto/ExtTunID PSBs RSBs Reqs
 ---- --------------- ----- --------------- ----- ----- ----- LSP4
```

```
 172.16.70.70 6 10.51.51.51 1 1 0
```

In the example , the output represents an LSP from ingress (head) router 10.51.51.51 to egress (tail) router 172.16.70.70. The tunnel ID (also called the *destination port*) is 6.

Example:

```
If no states can be found for a session that should be up, verify the
      application (for example, MPLS-TE ) to see if
      everything is in order. If a session has one PSB but no RSB, this indicates
      that either the Path message is not making it to the egress (tail) router or
      the reservation message is not making it back to the router R1 in question.
```

Go to the downstream router R2 and display the session information:

Example:

```
If R2 has no PSB, either the path message is not making it to the
      router or the path message is being rejected (for example, due to lack of
      resources). If R2 has a PSB but no RSB, go to the next downstream router R3
      to investigate. If R2 has a PSB and an RSB, this means the reservation is
      not making it from R2 to R1 or is being rejected.
```

Step 2 **show rsvp counters messages summary**

Verifies whether the RSVP message is being transmitted and received.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp counters messages summary

All RSVP Interfaces Recv Xmit Recv Xmit Path 0 25
      Resv 30 0 PathError 0 0 ResvError 0 1 PathTear 0 30 ResvTear 12 0
      ResvConfirm 0 0 Ack 24 37 Bundle 0 Hello 0 5099 SRefresh 8974 9012
      OutOfOrder 0 Retransmit 20 Rate Limited 0
```

Step 3 **show rsvp counters events**

Verifies how many RSVP states have expired. Because RSVP uses a soft-state mechanism, some failures will lead to RSVP states to expire due to lack of refresh from the neighbor.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp counters events

mgmtEthernet0/0/0/0 tunnel6 Expired Path states 0 Expired
      Path states 0 Expired Resv states 0 Expired Resv states 0 NACKs received 0
      NACKs received 0 POS0/3/0/0                              POS0/3/0/1 Expired
      Path states 0 Expired Path states 0 Expired Resv states 0 Expired Resv
      states 0 NACKs received 0 NACKs received 0 POS0/3/0/2
                                  POS0/3/0/3 Expired Path states 0 Expired Path
      states 0 Expired Resv states 0 Expired Resv states 1 NACKs received 0 NACKs
      received 1
```

Step 4 **show rsvp interface** *type interface-path-id* [**detail**]

Verifies that refresh reduction is working on a particular interface.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp interface pos0/3/0/3 detail

INTERFACE: POS0/3/0/3 (ifh=0x4000D00). BW
      (bits/sec): Max=1000M. MaxFlow=1000M. Allocated=1K (0%). MaxSub=0.
      Signalling: No DSCP marking. No rate limiting. States in: 1. Max missed
      msgs: 4. Expiry timer: Running (every 30s). Refresh interval: 45s. Normal
      Refresh timer: Not running. Summary refresh timer: Running. Refresh
      reduction local: Enabled. Summary Refresh: Enabled (4096 bytes max).
      Reliable summary refresh: Disabled. Ack hold: 400 ms, Ack max size: 4096
      bytes. Retransmit: 900ms. Neighbor information: Neighbor-IP Nbor-MsgIds
      States-out Refresh-Reduction Expiry(min::sec) -------------- --------------
      ---------- ------------------ ---------------- 64.64.64.65 1 1 Enabled
      14::45
```

Step 5 **show rsvp graceful-restart**

Verifies that graceful restart is enabled locally.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp graceful-restart

Graceful restart: enabled Number of global
      neighbors: 1 Local MPLS router id: 10.51.51.51 Restart time: 60 seconds
      Recovery time: 0 seconds Recovery timer: Not running Hello interval: 5000
      milliseconds Maximum Hello miss-count: 3
```

Step 6 **show rsvp graceful-restart** [**neighbors** *ip-address* | **detail**]

Verifies that graceful restart is enabled on the neighbor(s). These examples show that neighbor 192.168.60.60 is not responding to hello messages.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp graceful-restart neighbors 192.168.60.60

Neighbor App State Recovery Reason
      Since LostCnt --------------- ----- ------ -------- ------------
      -------------------- -------- 192.168.60.60 MPLS INIT DONE N/A 12/06/2003
      19:01:49 0
RP/0/RSP0/CPU0:router# show rsvp graceful-restart neighbors detail

Neighbor: 192.168.60.60 Source: 10.51.51.51
      (MPLS) Hello instance for application MPLS Hello State: INIT (for 3d23h)
      Number of times communications with neighbor lost: 0 Reason: N/A Recovery
      State: DONE Number of Interface neighbors: 1 address: 10.64.64.65 Restart
      time: 0 seconds Recovery time: 0 seconds Restart timer: Not running Recovery
      timer: Not running Hello interval: 5000 milliseconds Maximum allowed missed
      Hello messages: 3
```

Step 7 **show rsvp interface**

Verifies the available RSVP bandwidth.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp interface
```

```
Interface MaxBW MaxFlow Allocated MaxSub -----------
      -------- -------- --------------- -------- Et0/0/0/0 0 0 0 ( 0%) 0 PO0/3/0/0
      1000M 1000M 0 ( 0%) 0 PO0/3/0/1 1000M 1000M 0 ( 0%) 0 PO0/3/0/2 1000M 1000M
      0 ( 0%) 0 PO0/3/0/3 1000M 1000M 1K ( 0%) 0
```

Step 8 **show rsvp neighbor**

Verifies the RSVP neighbors.

Example:

```
RP/0/RSP0/CPU0:router# show rsvp neighbor detail
Global Neighbor: 40.40.40.40 Interface Neighbor: 10.0.0.1
      Interface: POS0/0/0/0 Refresh Reduction: "Enabled" or "Disabled". Remote
      epoch: 0xXXXXXXXX Out of order messages: 0 Retransmitted messages: 0
      Interface Neighbor: 172.16.0.1 Interface: POS0/1/0/0 Refresh Reduction:
      "Enabled" or "Disabled". Remote epoch: 0xXXXXXXXX Out of order messages: 0
      Retransmitted messages: 0
```

Related Topics

Overview of RSVP for MPLS-TE, on page 146

Enabling RSVP Traps

With the exception of the RSVP MIB traps, no action is required to activate the MIBs. This MIB feature is automatically enabled when RSVP is turned on; however, RSVP traps must be enabled.

Perform this task to enable all RSVP MIB traps, NewFlow traps, and LostFlow traps.

SUMMARY STEPS

1. **configure**
2. **snmp-server traps rsvp lost-flow**
3. **snmp-server traps rsvp new-flow**
4. **snmp-server traps rsvp all**
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**snmp-server traps rsvp lost-flow** **Example:** `RP/0/RSP0/CPU0:router(config)# snmp-server traps`	Sends RSVP notifications to enable RSVP LostFlow traps.

	Command or Action	Purpose
	`rsvp lost-flow`	
Step 3	**snmp-server traps rsvp new-flow** **Example:** `RP/0/RSP0/CPU0:router(config)# snmp-server traps rsvp new-flow`	Sends RSVP notifications to enable RSVP NewFlow traps.
Step 4	**snmp-server traps rsvp all** **Example:** `RP/0/RSP0/CPU0:router(config)# snmp-server traps rsvp all`	Sends RSVP notifications to enable all RSVP MIB traps.
Step 5	**commit**	

Related Topics

RSVP MIB, on page 150
Enable RSVP Traps: Example, on page 184

How to Implement RSVP Authentication

There are three types of RSVP authentication modes—global, interface, and neighbor. These topics describe how to implement RSVP authentication for each mode:

Configuring Global Configuration Mode RSVP Authentication

These tasks describe how to configure RSVP authentication in global configuration mode:

Enabling RSVP Authentication Using the Keychain in Global Configuration Mode

Perform this task to enable RSVP authentication for cryptographic authentication by specifying the keychain in global configuration mode.

Note You must configure a keychain before completing this task (see *System Security Configuration Guide for Cisco ASR 9000 Series Routers*).

SUMMARY STEPS

1. **configure**
2. **rsvp authentication**
3. **key-source key-chain** *key-chain-name*

4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**rsvp authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config)# rsvp authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)#`
		Enters RSVP authentication configuration mode.

Step 3	**key-source key-chain** *key-chain-name* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-auth)# key-source key-chain mpls-keys`	Specifies the source of the key information to authenticate RSVP signaling messages. ***key-chain-name*** Name of the keychain. The maximum number of characters is 32.
Step 4	**commit**	

Related Topics

Key-source Key-chain, on page 156
RSVP Authentication Global Configuration Mode: Example, on page 185

Configuring a Lifetime for RSVP Authentication in Global Configuration Mode

Perform this task to configure a lifetime value for RSVP authentication in global configuration mode.

SUMMARY STEPS

1. **configure**
2. **rsvp authentication**
3. **life-time** *seconds*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp authentication** **Example:**	Enters RSVP authentication configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# rsvp authentication` `RP/0/RSP0/CPU0:router(config-rsvp-auth)#`	
Step 3	**life-time** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-auth)# life-time 2000`	Controls how long RSVP maintains security associations with other trusted RSVP neighbors. ***seconds*** Length of time (in seconds) that RSVP maintains idle security associations with other trusted RSVP neighbors. Range is from 30 to 86400. The default value is 1800.
Step 4	**commit**	

Related Topics

Global, Interface, and Neighbor Authentication Modes, on page 153
RSVP Authentication Global Configuration Mode: Example, on page 185

Configuring the Window Size for RSVP Authentication in Global Configuration Mode

Perform this task to configure the window size for RSVP authentication in global configuration mode.

SUMMARY STEPS

1. **configure**
2. **rsvp authentication**
3. **window-size** *N*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**rsvp authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config)# rsvp authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)#`
		Enters RSVP authentication configuration mode.

Step 3	**window-size** *N* **Example:**	Specifies the maximum number of RSVP authenticated messages that can be received out-of-sequence.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-rsvp-auth)# window-size 33`	*N* Size of the window to restrict out-of-sequence messages. The range is from 1 to 64. The default value is 1, in which case all out-of-sequence messages are dropped.
Step 4	**commit**	

Related Topics

Guidelines for Window-Size and Out-of-Sequence Messages, on page 156
RSVP Authentication by Using All the Modes: Example, on page 186
RSVP Authentication for an Interface: Example, on page 185

Configuring an Interface for RSVP Authentication

These tasks describe how to configure an interface for RSVP authentication:

Specifying the RSVP Authentication Keychain in Interface Mode

Perform this task to specify RSVP authentication keychain in interface mode.

You must configure a keychain first (see *System Security Configuration Guide for Cisco ASR 9000 Series Routers*).

SUMMARY STEPS

1. **configure**
2. **rsvp interface** *type interface-path-id*
3. **authentication**
4. **key-source key-chain** *key-chain-name*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**rsvp interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# rsvp interface POS 0/2/1/0`
	`RP/0/RSP0/CPU0:router(config-rsvp-if)#`
		Enters RSVP interface configuration mode.

	Command or Action	Purpose

Step 3	**authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#`
		Enters RSVP authentication configuration mode.

Step 4	**key-source key-chain** *key-chain-name* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# key-source key-chain mpls-keys`	Specifies the source of the key information to authenticate RSVP signaling messages. ***key-chain-name*** Name of the keychain. The maximum number of characters is 32.
Step 5	**commit**	

Related Topics

Global, Interface, and Neighbor Authentication Modes, on page 153
RSVP Authentication by Using All the Modes: Example, on page 186

Configuring a Lifetime for an Interface for RSVP Authentication

Perform this task to configure a lifetime for the security association for an interface.

SUMMARY STEPS

1. **configure**
2. **rsvp interface** *type interface-path-id*
3. **authentication**
4. **life-time** *seconds*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**rsvp interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# rsvp interface POS 0/2/1/0`
	`RP/0/RSP0/CPU0:router(config-rsvp-if)#`
		Enters RSVP interface configuration mode.

	Command or Action	Purpose

Step 3	**authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#`
		Enters RSVP authentication configuration mode.

Step 4	**life-time** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if-auth)# life-time 2000`	Controls how long RSVP maintains security associations with other trusted RSVP neighbors. ***seconds*** Length of time (in seconds) that RSVP maintains idle security associations with other trusted RSVP neighbors. Range is from 30 to 86400. The default value is 1800.
Step 5	**commit**	

Related Topics

RSVP Authentication Design, on page 153
RSVP Authentication by Using All the Modes: Example, on page 186

Configuring the Window Size for an Interface for RSVP Authentication

Perform this task to configure the window size for an interface for RSVP authentication to check the validity of the sequence number received.

SUMMARY STEPS

1. **configure**
2. **rsvp interface** *type interface-path-d*
3. **authentication**
4. **window-size** *N*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp interface** *type interface-path-d* **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp interface POS 0/2/1/0`	Enters RSVP interface configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-rsvp-if)#`	

Step 3	**authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp-if)#`
	`authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#`
		Enters RSVP interface authentication configuration mode.

Step 4	**window-size** *N* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if-auth)#` **`window-size 33`**	Specifies the maximum number of RSVP authenticated messages that can be received out-of-sequence. ***N*** Size of the window to restrict out-of-sequence messages. The range is from 1 to 64. The default value is 1, in which case all out-of-sequence messages are dropped.
Step 5	**commit**	

Related Topics

Guidelines for Window-Size and Out-of-Sequence Messages, on page 156
RSVP Authentication by Using All the Modes: Example, on page 186
RSVP Authentication for an Interface: Example, on page 185

Configuring RSVP Neighbor Authentication

These tasks describe how to configure the RSVP neighbor authentication:

- Specifying the Keychain for RSVP Neighbor Authentication, on page 175
- Configuring a Lifetime for RSVP Neighbor Authentication, on page 176
- Configuring the Window Size for RSVP Neighbor Authentication, on page 177

Specifying the Keychain for RSVP Neighbor Authentication

Perform this task to specify the keychain RSVP neighbor authentication.

You must configure a keychain first (see *System Security Configuration Guide for Cisco ASR 9000 Series Routers*).

SUMMARY STEPS

1. **configure**
2. **rsvp neighbor** *IP-address* **authentication**
3. **key-source key-chain** *key-chain-name*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**rsvp neighbor** *IP-address* **authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config)# rsvp neighbor 10.0.0.1 authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)#`
		Enters neighbor authentication configuration mode. Use the **rsvp neighbor** command to activate RSVP cryptographic authentication for a neighbor.
		IP address
		IP address of the neighbor. A single IP address for a specific neighbor; usually one of the neighbor's physical or logical (loopback) interfaces.
		authentication
		Configures the RSVP authentication parameters.

Step 3	**key-source key-chain** *key-chain-name* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# key-source key-chain mpls-keys`	Specifies the source of the key information to authenticate RSVP signaling messages. ***key-chain-name*** Name of the keychain. The maximum number of characters is 32.
Step 4	**commit**	

Related Topics

Key-source Key-chain, on page 156
Security Association, on page 154
RSVP Neighbor Authentication: Example, on page 186

Configuring a Lifetime for RSVP Neighbor Authentication

Perform this task to configure a lifetime for security association for RSVP neighbor authentication mode.

SUMMARY STEPS

1. **configure**
2. **rsvp neighbor** *IP-address* **authentication**
3. **life-time** *seconds*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**rsvp neighbor** *IP-address* **authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config)# rsvp neighbor 10.0.0.1 authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)#`
		Enters RSVP neighbor authentication configuration mode. Use the **rsvp neighbor** command to specify a neighbor under RSVP.
		IP address
		IP address of the neighbor. A single IP address for a specific neighbor; usually one of the neighbor's physical or logical (loopback) interfaces.
		authentication
		Configures the RSVP authentication parameters.

Step 3	**life-time** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# life-time 2000`	Controls how long RSVP maintains security associations with other trusted RSVP neighbors. The argument specifies the ***seconds*** Length of time (in seconds) that RSVP maintains idle security associations with other trusted RSVP neighbors. Range is from 30 to 86400. The default value is 1800.
Step 4	**commit**	

Related Topics

Security Association, on page 154
RSVP Authentication Global Configuration Mode: Example, on page 185

Configuring the Window Size for RSVP Neighbor Authentication

Perform this task to configure the RSVP neighbor authentication window size to check the validity of the sequence number received.

SUMMARY STEPS

1. **configure**
2. **rsvp neighbor** *IP address* **authentication**
3. **window-size** *N*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**rsvp neighbor** *IP address* **authentication**
	Example:
	`RP/0/RSP0/CPU0:router(config)# rsvp neighbor 10.0.0.1 authentication`
	`RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)#`
		Enters RSVP neighbor authentication configuration mode. Use the **rsvp neighbor** command to specify a neighbor under RSVP.
		IP address
		IP address of the neighbor. A single IP address for a specific neighbor; usually one of the neighbor's physical or logical (loopback) interfaces.
		authentication
		Configures the RSVP authentication parameters.

Step 3	**window-size** *N* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-nbor-auth)# window-size 33`	Specifies the maximum number of RSVP authenticated messages that is received out-of-sequence. ***N*** Size of the window to restrict out-of-sequence messages. The range is from 1 to 64. The default value is 1, in which case all out-of-sequence messages are dropped.
Step 4	**commit**	

Related Topics

Guidelines for Window-Size and Out-of-Sequence Messages, on page 156
RSVP Authentication by Using All the Modes: Example, on page 186
RSVP Authentication for an Interface: Example, on page 185

MPLS-TE PCE authentication

The PCEP session authentication is a security mechanism that

- establishes a secure and trusted communication channel between a PCC and a PCE,
- ensures that only authorized devices can participate in PCEP sessions, and
- protects against unauthorized access and data tampering.

Methods of MPLS-TE PCE authentication

Before Release 26.1.1, you can perform MPLS-TE PCE authentication using TCP Message Digest 5 (MD5) authentication. This method uses a clear text or encrypted password for authentication. The Cisco IOS XR software rejects segments that lack a Message Authentication Code (MAC) matching the configured password.

From Release 26.1.1, you can perform MPLS-TE PCE authentication using TCP Authentication Option (TCP-AO).

TCP-AO uses Message Authentication Codes (MACs), which provides the following benefits:

- It protects against replay attacks for long-lived TCP connections.
- It provides more detailed security association with TCP connections than TCP MD5.
- It supports a larger set of MAC algorithms with minimal system and operational changes.

TCP-AO is compatible with Master Key Tuple (MKT) configuration, protecting connections by deriving traffic keys from the MKT and coordinating changes between endpoints. The Cisco IOS XR software rejects segments that lack a MAC matching the configured key chain.

Note TCP-AO and TCP MD5 are never permitted to be used simultaneously. TCP-AO supports IPv6, and is fully compatible with the proposed requirements for the replacement of TCP MD5.

Configure MPLS-TE PCE authentication

Procedure

Step 1 Before Release 26.1.1, you can configure MPLS-TE PCE authentication using TCP MD5 authentication. Specify if the password is encrypted or clear text.

Example:

```
Router# configure terminal
Router(config)# mpls traffic-eng
Router(config-mpls-te)# pce password [{clear | encrypted} <password>]
```

Step 2 From Release 26.1.1, you can configure MPLS-TE PCE authentication using TCP Authentication Option (TCP-AO). Use the **include-tcp-options** keyword to include other TCP options in the header for MAC calculation.

Example:

```
Router# configure terminal
Router(config)# mpls traffic-eng
Router(config-mpls-te)# pce tcp-ao <password> include-tcp-options
```

Step 3 Run the **show mpls traffic-eng pce peer** command to verify the PCE up status.

Example:

```
Router# show mpls traffic-eng pce peer

Address Precedence State Learned From
--------------- ------------ ------------ --------------------
192.168.1.4 255 Up Static config
```

Step 4 Run the **show tcp detail** command to verify the TCP session details.

Example:

```
Router# show tcp detail pcb all
```

```
==============================================================
Connection state is ESTAB, I/O status: 0, socket status: 0
Established at Thu Feb 26 05:36:17 2026

PCB 0x00007fc85c0049d0, SO 0x7fc85c0045b0, TCPCB 0x7fc85c004ce0, vrfid 0x60000000,
Pak Prio: Medium, TOS: 192, TTL: 255, Hash index: 1854
Local host: 192.168.0.1, Local port: 52364 (Local App PID: 8630)
Foreign host: 192.168.1.4, Foreign port: 4189
(Local App PID/instance/SPL_APP_ID: 8630/0/0)

Current send queue size in bytes: 0 (max 512000)
Current receive queue size in bytes: 0 (max 512000) mis-ordered: 0 bytes
Current receive queue size in packets: 0 (max 60)


Num of peers with authentication info: 1
Authentication peer details:
Peer: 192.168.1.4/32, OBJ_ID: 0x40002fc0
Port: 4189, vrf_id: 0x60000000, type: AO, debug_on:0
Keychain_name: test11, options: 0x00000001, linked peer: 0x7fc864004770
Send_SNE: 0, Receive_SNE: 0, Send_SNE_flag: 0
Recv_SNE_flag: 0, Prev_send_seq: 3997493771, Prev_receive_seq: 401915492
ISS: 3997493682, IRS: 401915403
Current key: 1
Traffic keys: send_non_SYN: ffd64ea3, recv_non_SYN: 00000000
RNext key: 1
Traffic keys: send_non_SYN: 00000000, recv_non_SYN: 00000000
Last 1 keys used:
key: 1, time: Feb 26 05:36:17.344.766, reason: No current key set
```

The above sample displays only a part of the actual output; the actual output displays more details.

Verifying the Details of the RSVP Authentication

To display the security associations that RSVP has established with other RSVP neighbors, use the **show rsvp authentication** command.

Eliminating Security Associations for RSVP Authentication

To eliminate RSVP authentication SA's, use the **clear rsvp authentication** command. To eliminate RSVP counters for each SA, use the **clear rsvp counters authentication** command.

Configuration Examples for RSVP

Sample RSVP configurations are provided for some of the supported RSVP features.

- #unique_207
- #unique_208
- #unique_209
- Refresh Reduction and Reliable Messaging Configuration: Examples, on page 181

- Configure Graceful Restart: Examples, on page 183
- Configure ACL-based Prefix Filtering: Example, on page 183
- Set DSCP for RSVP Packets: Example, on page 184
- Enable RSVP Traps: Example, on page 184

Bandwidth Configuration (Prestandard): Example

The example shows the configuration of bandwidth on an interface using prestandard DS-TE mode. The example configures an interface for a reservable bandwidth of 7500, specifies the maximum bandwidth for one flow to be 1000 and adds a sub-pool bandwidth of 2000.

```
rsvp interface hundredGigE 0/0/0/0
 bandwidth 7500 1000 sub-pool 2000
```

Bandwidth Configuration (MAM): Example

The example shows the configuration of bandwidth on an interface using MAM. The example shows how to limit the total of all RSVP reservations on the hundredGigE 0/0/0/0 interface to 7500 kbps, and allow each single flow to reserve no more than 1000 kbps.

```
rsvp interface hundredGigE 0/0/0/0
 bandwidth mam 7500 1000
```

Related Topics

Confirming DiffServ-TE Bandwidth, on page 157
Differentiated Services Traffic Engineering, on page 208

Bandwidth Configuration (RDM): Example

The example shows the configuration of bandwidth on an interface using RDM. The example shows how to limit the total of all RSVP reservations on the hundredGigE 0/0/0/0 interface to 7500 kbps, and allows each single flow to reserve no more than 1000 kbps.

```
rsvp interface hundredGigE 0/0/0/0
 bandwidth rdm 7500 1000
```

Related Topics

Confirming DiffServ-TE Bandwidth, on page 157
Differentiated Services Traffic Engineering, on page 208

Refresh Reduction and Reliable Messaging Configuration: Examples

Refresh reduction feature as defined by RFC 2961 is supported and enabled by default. The examples illustrate the configuration for the refresh reduction feature. Refresh reduction is used with a neighbor only if the neighbor supports it also.

Refresh Interval and the Number of Refresh Messages Configuration: Example

The example shows how to configure the refresh interval to 30 seconds on POS 0/3/0/0 and how to change the number of refresh messages the node can miss before cleaning up the state from the default value of 4 to 6.

```
rsvp interface pos 0/3/0/0
 signalling refresh interval 30
 signalling refresh missed 6
```

Retransmit Time Used in Reliable Messaging Configuration: Example

The example shows how to set the retransmit timer to 2 seconds. To prevent unnecessary retransmits, the retransmit time value configured on the interface must be greater than the ACK hold time on its peer.

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction reliable retransmit-time 2000
```

Acknowledgement Times Configuration: Example

The example shows how to change the acknowledge hold time from the default value of 400 ms, to delay or speed up sending of ACKs, and the maximum acknowledgment message size from default size of 4096 bytes. The example shows how to change the acknowledge hold time from the default value of 400 ms and how to delay or speed up sending of ACKs. The maximum acknowledgment message default size is from 4096 bytes.

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction reliable ack-hold-time 1000
rsvp interface pos 0/4/0/1
 signalling refresh reduction reliable ack-max-size 1000
```

Note Ensure retransmit time on the peers' interface is at least twice the amount of the ACK hold time to prevent unnecessary retransmissions.

Summary Refresh Message Size Configuration: Example

The example shows how to set the summary refresh message maximum size to 1500 bytes.

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction summary max-size 1500
```

Disable Refresh Reduction: Example

If the peer node does not support refresh reduction, or for any other reason you want to disable refresh reduction on an interface, the example shows how to disable refresh reduction on that interface.

```
rsvp interface pos 0/4/0/1
 signalling refresh reduction disable
```

Configure Graceful Restart: Examples

RSVP graceful restart is configured globally or per interface (as are refresh-related parameters). These examples show how to enable graceful restart, set the restart time, and change the hello message interval.

Enable Graceful Restart: Example

The example shows how to enable the RSVP graceful restart by default. If disabled, enable it with the following command.

```
rsvp signalling graceful-restart
```

Related Topics

Enabling Graceful Restart, on page 158
Graceful Restart: Standard and Interface-Based, on page 148

Enable Interface-Based Graceful Restart: Example

The example shows how to enable the RSVP graceful restart feature on an interface.

```
RP/0/RSP0/CPU0:router#configure
RP/0/RSP0/CPU0:router(config-rsvp)#interface bundle-ether 17
RP/0/RSP0/CPU0:router(config-rsvp-if)#signalling hello graceful-restart ?
  interface-based  Configure Interface-based Hello
RP/0/RSP0/CPU0:router(config-rsvp-if)#signalling hello graceful-restart interface-based
RP/0/RSP0/CPU0:router(config-rsvp-if)#
```

Related Topics

Enabling Graceful Restart, on page 158
Graceful Restart: Standard and Interface-Based, on page 148

Change the Restart-Time: Example

The example shows how to change the restart time that is advertised in hello messages sent to neighbor nodes.

```
rsvp signalling graceful-restart restart-time 200
```

Change the Hello Interval: Example

The example shows how to change the interval at which RSVP graceful restart hello messages are sent per neighbor, and change the number of hellos missed before the neighbor is declared down.

```
rsvp signalling hello graceful-restart refresh interval 4000
rsvp signalling hello graceful-restart refresh misses 4
```

Configure ACL-based Prefix Filtering: Example

The example shows when RSVP receives a Router Alert (RA) packet from source address 10.0.0.1 and 10.0.0.1 is not a local address. The packet is forwarded with IP TTL decremented. Packets destined to 172.16.0.1 are dropped. All other RA packets are processed as normal RSVP packets.

```
show run ipv4 access-list
  ipv4 access-list rsvpacl
  10 permit ip host 10.0.0.1 any
```

```
    20 deny ip any host 172.16.0.1
    !
  show run rsvp
    rsvp
    signalling prefix-filtering access-list rsvpacl
    !
```

Related Topics

Configuring ACLs for Prefix Filtering, on page 159
ACL-based Prefix Filtering, on page 150

Set DSCP for RSVP Packets: Example

The configuration example sets the Differentiated Services Code Point (DSCP) field in the IP header of RSVP packets.

```
rsvp interface pos0/2/0/1
 signalling dscp 20
```

Related Topics

Configuring RSVP Packet Dropping, on page 160
Overview of RSVP for MPLS-TE, on page 146

Enable RSVP Traps: Example

The example enables the router to send all RSVP traps:

```
configure
 snmp-server traps rsvp all
```

The example enables the router to send RSVP LostFlow traps:

```
configure
 snmp-server traps rsvp lost-flow
```

The example enables the router to send RSVP RSVP NewFlow traps:

```
configure
 snmp-server traps rsvp new-flow
```

Related Topics

Enabling RSVP Traps, on page 168
RSVP MIB, on page 150

Configuration Examples for RSVP Authentication

These configuration examples are used for RSVP authentication:

- RSVP Authentication Global Configuration Mode: Example, on page 185

- RSVP Authentication for an Interface: Example, on page 185
- RSVP Neighbor Authentication: Example, on page 186
- RSVP Authentication by Using All the Modes: Example, on page 186

RSVP Authentication Global Configuration Mode: Example

The configuration example enables authentication of all RSVP messages and increases the default lifetime of the SAs.

```
rsvp
 authentication
  key-source key-chain default_keys
  life-time 3600
 !
!
```

Note The specified keychain (default_keys) must exist and contain valid keys, or signaling will fail.

Related Topics

Enabling RSVP Authentication Using the Keychain in Global Configuration Mode, on page 169
Key-source Key-chain, on page 156
Configuring a Lifetime for RSVP Authentication in Global Configuration Mode, on page 170
Global, Interface, and Neighbor Authentication Modes, on page 153
Configuring a Lifetime for RSVP Neighbor Authentication, on page 176
Security Association, on page 154

RSVP Authentication for an Interface: Example

The configuration example enables authentication of all RSVP messages that are being sent or received on one interface only, and sets the window-size of the SAs.

```
rsvp
 interface GigabitEthernet0/6/0/0
  authentication
   window-size 64
  !
 !
```

Note Because the key-source keychain configuration is not specified, the global authentication mode keychain is used and inherited. The global keychain must exist and contain valid keys or signaling fails.

Related Topics

Configuring the Window Size for RSVP Authentication in Global Configuration Mode, on page 171

Configuring the Window Size for an Interface for RSVP Authentication, on page 174
Configuring the Window Size for RSVP Neighbor Authentication, on page 177
Guidelines for Window-Size and Out-of-Sequence Messages, on page 156

RSVP Neighbor Authentication: Example

The configuration example enables authentication of all RSVP messages that are being sent to and received from only a particular IP address.

```
rsvp
 neighbor 10.0.0.1
  authentication
   key-source key-chain nbr_keys
  !
 !
!
```

Related Topics

Specifying the Keychain for RSVP Neighbor Authentication, on page 175
Key-source Key-chain, on page 156
Security Association, on page 154

RSVP Authentication by Using All the Modes: Example

The configuration example shows how to perform the following functions:

- Authenticates all RSVP messages.
- Authenticates the RSVP messages to or from 10.0.0.1 by setting the keychain for the **key-source key-chain** command to nbr_keys, SA lifetime is set to 3600, and the default window-size is set to 1.
- Authenticates the RSVP messages not to or from 10.0.0.1 by setting the keychain for the **key-source key-chain** command to default_keys, SA lifetime is set to 3600, and the window-size is set 64 when using GigabitEthernet0/6/0/0; otherwise, the default value of 1 is used.

```
rsvp
 interface GigabitEthernet0/6/0/0
  authentication
   window-size 64
  !
 !
 neighbor 10.0.0.1
  authentication
   key-source key-chain nbr_keys
  !
 !
 authentication
  key-source key-chain default_keys
  life-time 3600
 !
!
```

Note If a keychain does not exist or contain valid keys, this is considered a configuration error because signaling fails. However, this can be intended to prevent signaling. For example, when using the above configuration, if the nbr_keys does not contain valid keys, all signaling with 10.0.0.1 fails.

Related Topics

Configuring the Window Size for RSVP Authentication in Global Configuration Mode, on page 171
Configuring the Window Size for an Interface for RSVP Authentication, on page 174
Configuring the Window Size for RSVP Neighbor Authentication, on page 177
Guidelines for Window-Size and Out-of-Sequence Messages, on page 156
Specifying the RSVP Authentication Keychain in Interface Mode, on page 172
Global, Interface, and Neighbor Authentication Modes, on page 153
Configuring a Lifetime for an Interface for RSVP Authentication, on page 173
RSVP Authentication Design, on page 153

Additional References

For additional information related to implementing GMPLS UNI, refer to the following references:

Related Documents

Related Topic	Document Title
GMPLS UNI commands	*GMPLS UNI Commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*
MPLS Traffic Engineering commands	*MPLS Traffic Engineering commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*
RSVP commands	*RSVP commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*
Getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Information about user groups and task IDs	*Configuring AAA Services* module in *System Security Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

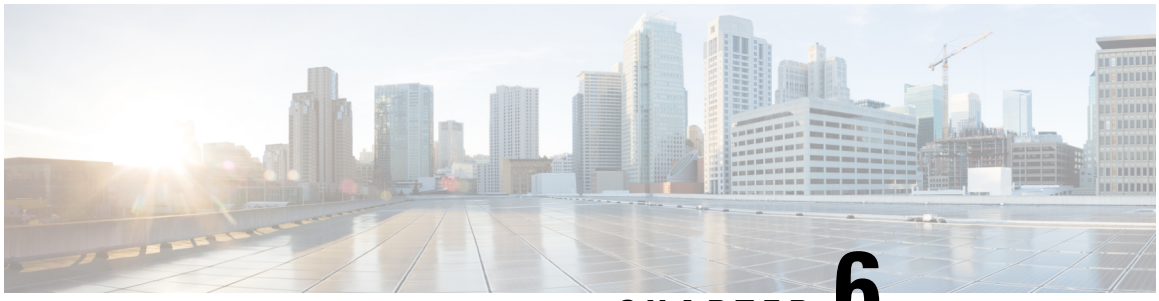
MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
RFC 3471	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*
RFC 3473	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*
RFC 4208	*Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model*
RFC 4872	*RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*
RFC 4874	*Exclude Routes - Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)*
RFC 6205	*Generalized Labels for Lambda-Switch-Capable (LSC) Label Switching Routers*

Technical Assistance

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



CHAPTER 6

Implementing MPLS Forwarding

This module describes how to implement MPLS Forwarding on Cisco ASR 9000 Series Aggregation Services Routers.

All Multiprotocol Label Switching (MPLS) features require a core set of MPLS label management and forwarding services; the MPLS Forwarding Infrastructure (MFI) supplies these services.

Feature History for Implementing MPLS-TE

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.0	No modification.
Release 6.0	The Label Security for BGP Inter-AS Option-B feature was modified.

- Prerequisites for Implementing Cisco MPLS Forwarding, on page 189
- Restrictions for Implementing Cisco MPLS Forwarding, on page 190
- Information About Implementing MPLS Forwarding, on page 190
- How to Implement MPLS Forwarding, on page 192
- Enable Per-Prefix Statistics Collection, on page 193
- Additional References, on page 196

Prerequisites for Implementing Cisco MPLS Forwarding

These prerequisites are required to implement MPLS Forwarding:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- Router that runs Cisco IOS XR software.
- Installed composite mini-image and the MPLS package, or a full composite image.

Restrictions for Implementing Cisco MPLS Forwarding

- Label switching on a Cisco router requires that Cisco Express Forwarding (CEF) be enabled.
- CEF is mandatory for Cisco IOS XR software and it does not need to be enabled explicitly.

Information About Implementing MPLS Forwarding

To implement MPLS Forwarding, you should understand these concepts:

MPLS Forwarding Overview

MPLS combines the performance and capabilities of Layer 2 (data link layer) switching with the proven scalability of Layer 3 (network layer) routing. MPLS enables service providers to meet the challenges of growth in network utilization while providing the opportunity to differentiate services without sacrificing the existing network infrastructure. The MPLS architecture is flexible and can be employed in any combination of Layer 2 technologies. MPLS support is offered for all Layer 3 protocols, and scaling is possible well beyond that typically offered in today's networks.

Based on routing information that is stored in the VRF IP routing table and VRF CEF table, packets are forwarded to their destination using MPLS.

A PE router binds a label to each customer prefix learned from a CE router and includes the label in the network reachability information for the prefix that it advertises to other PE routers. When a PE router forwards a packet received from a CE router across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet it pops the label and uses it to direct the packet to the correct CE router. Label forwarding across the provider backbone, is based on either dynamic label switching or traffic engineered paths. A customer data packet carries two levels of labels when traversing the backbone:

- Top label directs the packet to the correct PE router
- Second label indicates how that PE router should forward the packet to the CE router

Label Switching Functions

In conventional Layer 3 forwarding mechanisms, as a packet traverses the network, each router extracts all the information relevant to forwarding the packet from the Layer 3 header. This information is then used as an index for a routing table lookup to determine the next hop for the packet.

In the most common case, the only relevant field in the header is the destination address field, but in some cases, other header fields might also be relevant. As a result, the header analysis must be done independently at each router through which the packet passes. In addition, a complicated table lookup must also be done at each router.

In label switching, the analysis of the Layer 3 header is done only once. The Layer 3 header is then mapped into a fixed-length, unstructured value called a *label*.

Many different headers can map to the same label, as long as those headers always result in the same choice of next hop. In effect, a label represents a forwarding equivalence class—that is, a set of packets which, however different they may be, are indistinguishable by the forwarding function.

The initial choice of a label need not be based exclusively on the contents of the Layer 3 packet header; for example, forwarding decisions at subsequent hops can also be based on routing policy.

Once a label is assigned, a short label header is added at the front of the Layer 3 packet. This header is carried across the network as part of the packet. At subsequent hops through each MPLS router in the network, labels are swapped and forwarding decisions are made by means of MPLS forwarding table lookup for the label carried in the packet header. Hence, the packet header does not need to be reevaluated during packet transit through the network. Because the label is of fixed length and unstructured, the MPLS forwarding table lookup process is both straightforward and fast.

Distribution of Label Bindings

Each label switching router (LSR) in the network makes an independent, local decision as to which label value to use to represent a forwarding equivalence class. This association is known as a label binding.

Note The distribution of label bindings cannot be done statically for the Layer 2 VPN pseudowire.

Each LSR informs its neighbors of the label bindings it has made. This awareness of label bindings by neighboring routers is facilitated by these protocols:

Label Distribution Protocol (LDP)

Supports MPLS forwarding along normally routed paths.

Resource Reservation Protocol (RSVP)

Supports MPLS traffic engineering.

Border Gateway Protocol (BGP)

Supports MPLS virtual private networks (VPNs).

When a labeled packet is sent from LSR A to the neighboring LSR B, the label value carried by the IP packet is the label value that LSR B assigned to represent the forwarding equivalence class of the packet. Thus, the label value changes as the IP packet traverses the network.

MFI Control-Plane Services

The MFI control-plane provides services to MPLS applications, such as Label Distribution Protocol (LDP) and Traffic Engineering (TE), that include enabling and disabling MPLS on an interface, local label allocation, MPLS rewrite setup (including backup links), management of MPLS label tables, and the interaction with other forwarding paths (IP Version 4 [IPv4] for example) to set up imposition and disposition.

MFI Data-Plane Services

The MFI data-plane provides a software implementation of MPLS forwarding in all of these forms:

- Imposition

- Disposition
- Label swapping

MPLS Maximum Transmission Unit

MPLS maximum transmission unit (MTU) indicates that the maximum size of the IP packet can still be sent on a data link, without fragmenting the packet. In addition, data links in MPLS networks have a specific MTU, but for labeled packets. All IPv4 packets have one or more labels. This does imply that the labeled packets are slightly bigger than the IP packets, because for every label, four bytes are added to the packet. So, if n is the number of labels, n * 4 bytes are added to the size of the packet when the packet is labeled. The MPLS MTU parameter pertains to labeled packets.

Label Security for BGP Inter-AS Option-B

Option-B is a method to exchange VPNv4/VPNv6 routes between Autonomous Systems (AS), as described in RFC-4364. When a router configured with Option-B, peers with a router from another confederation, or an autonomous system, and receives a labeled packet from such an external peer, the router ensures the following:

- the top label is advertised to the source of traffic
- label stack on the packet received from the external peer contains at least one label (explicit null label is not included)

How to Implement MPLS Forwarding

These topics explain how to configure a router for MPLS forwarding.

Configuring MPLS Label Security

Perform this task to configure the MPLS label security on the interface.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **mpls label-security rpf**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)#interface tunnel-te 1`	Enters the interface configuration mode.
Step 3	**mpls label-security rpf** **Example:** `RP/0/RSP0/CPU0:router(config-if)#mpls label-security rpf`	Configures the MPLS label security on the specified interface and checks for RPF label on incoming packets.
Step 4	**commit**	

Enable Per-Prefix Statistics Collection

Table 7: Feature History Table

Feature Name	Release Information	Feature Description
Enable Per-Prefix Statistics Collection	Release 7.10.1	You can now enable the router to collect only the per-prefix statistics, that is, the aggregate statistics for all paths available for a destination prefix. This helps conserve the hardware resources of the router. In earlier releases, there was no option to disable per-path statistics collection. The router collected both per-prefix statistics and per-path statistics for each destination prefix. When there were multiple paths for a destination prefix, the router required much more hardware resources to store the per-path statistics. This feature introduces these changes: **CLI:** • **hw-module l3 feature per-prefix-egress-stats enable** **YANG Data Model:** • New XPaths for `Cisco-IOS-XR-um-hw-module-l3-cfg.yang` (see GitHub, YANG Data Models Navigator)

In large networks, each destination prefix has multiple paths. The router requires a lot of hardware resources to collect and store statistics for each of the various paths for every destination prefix. Hence per-path statistics collection is resource-intensive.

Now you can enable the router to collect only the aggregate statistics for destination prefixes, that is, the per-prefix statistics collection. Hence the router doesn't have to allocate memory for statistics collection for each path of a destination prefix. For every destination prefix, the router collects only one set of statistics.

This frees up the platform hardware resources and allows you to scale up the number of destination prefixes in a router. You can enable this feature with the **hw-module l3 feature per-prefix-egress-stats enable** command.

Configure Per-Prefix Statistics Collection

```
Router(config)#hw-module l3 feature per-prefix-egress-stats enable
Router(config)#commit
Router(config)#exit
Router#reload location all
```



Note Reload the router after you enable or disable the per-prefix egress statistics collection. By default, per-prefix egress statistics collection is disabled.

Verification of Per-Prefix Statistics Collection

When you enable the **hw-module l3 feature per-prefix-egress-stats enable** command, the following changes apply for the command outputs for **show mpls forwarding labels** :

- The field **Bytes Switched** is 0 for every path of a destination prefix in the output of the command **show mpls forwarding labels** *label* **detail**
- The router displays **Total Packets/Bytes Switched** at the bottom of the command output for **show mpls forwarding labels** *label* **detail**.
- The command **show mpls forwarding labels** *label* displays a value of 0 for the **Bytes Switched** field for every path of a destination prefix.

```
Router#show mpls forwarding labels 24001 detail
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
24001  Pop         30.30.30.1/32      Hu0/0/0/2    11.1.1.2        0 <-- per-path stats is
 0
     Updated: Oct  7 03:29:30.877
     Version: 129, Priority: 3
     Label Stack (Top -> Bottom): { Imp-Null }
     NHID: 0xa, Encap-ID: N/A, Path idx: 0, Backup path idx: 0, Weight: 0
     MAC/Encaps: 4/4, MTU: 1500
     Outgoing Interface: HundredGigE0/0/0/2 (ifhandle 0x000000c0)
     Packets Switched: 0

       Pop         30.30.30.1/32      Hu0/0/0/1    12.1.1.2        0  <-- per-path stats
is 0
     Updated: Oct  7 03:29:30.877
     Version: 129, Priority: 3
     Label Stack (Top -> Bottom): { Imp-Null }
     NHID: 0x9, Encap-ID: N/A, Path idx: 1, Backup path idx: 0, Weight: 0
     MAC/Encaps: 4/4, MTU: 1500
     Outgoing Interface: HundredGigE0/0/0/1 (ifhandle 0x00000140)
     Packets Switched: 0

  Total Packets/Bytes Switched: 30/3000              <---- Per-Prefix Stats (aggregate
packets/bytes switched from all paths)

Router#show mpls forwarding labels 24000
```

```
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
24000  24000       10.10.10.1/32      Hu0/0/0/2    11.1.1.1        0  <-- per-path stats
is 0
       24000       10.10.10.1/32      Hu0/0/0/1    12.1.1.1        0  <-- per-path stats
is 0
```

When you disable the per-prefix egress statistics collection mode with the **no hw-module l3 feature per-prefix-egress-stats enable** command, the router populates the **Bytes Switched** field for each path of a destination prefix.

```
Router#show mpls forwarding labels 24001 detail
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
24001  Pop         10.3.1.0/24        Te0/0/0/1/0  10.1.1.1        76636        <--per-path
 stats is displayed
     Updated: May  5 03:22:33.070
     Version: 17, Priority: 3
     Label Stack (Top -> Bottom): { Imp-Null }
     NHID: 0x0, Encap-ID: N/A, Path idx: 0, Backup path idx: 0, Weight: 0
     MAC/Encaps: 4/4, MTU: 1500
     Outgoing Interface: TenGigE0/0/0/1/0 (ifhandle 0x000004c0)
     Packets Switched: 1666

       Pop         10.3.1.0/24        Te0/0/0/1/1  10.2.1.1        153318       <--per-path
 stats is displayed
     Updated: May  5 03:22:33.070
     Version: 17, Priority: 3
     Label Stack (Top -> Bottom): { Imp-Null }
     NHID: 0x0, Encap-ID: N/A, Path idx: 1, Backup path idx: 0, Weight: 0
     MAC/Encaps: 4/4, MTU: 1500
     Outgoing Interface: TenGigE0/0/0/1/1 (ifhandle 0x00000500)
     Packets Switched: 3333

       Pop         10.3.1.0/24        Te0/0/0/1/5  10.4.1.1        230046       <--per-path
 stats is displayed
     Updated: May  5 03:22:40.033
     Version: 17, Priority: 3
     Label Stack (Top -> Bottom): { Imp-Null }
     NHID: 0x0, Encap-ID: N/A, Path idx: 2, Backup path idx: 0, Weight: 0
     MAC/Encaps: 4/4, MTU: 1500
     Outgoing Interface: TenGigE0/0/0/1/5 (ifhandle 0x00000600)
     Packets Switched: 5001

  Total Packets/Bytes Switched: 10000/460000
<--Per-Prefix Stats (aggregate packets/bytes switched from all paths)

Router#show mpls forwarding labels 24001
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
------ ----------- ------------------ ------------ --------------- ------------
24001  Pop         10.3.1.0/24        Te0/0/0/1/0  10.1.1.1        76636        <--per-path
 stats is displayed
       Pop         10.3.1.0/24        Te0/0/0/1/1  10.2.1.1        153318       <--per-path
 stats is displayed
       Pop         10.3.1.0/24        Te0/0/0/1/5  10.4.1.1        230046       <--per-path
 stats is displayed
```

Additional References

For additional information related to implementing MPLS Forwarding, refer to the following references:

Related Documents

Related Topic	Document Title
MPLS Forwarding commands	*MPLS Forwarding Commands on Cisco ASR 9000 Series Router* module in *Cisco ASR 9000 Series Aggregation Services Routers MPLS Command Reference*
Getting started material	*Cisco ASR 9000 Series Aggregation Services Routers Getting Started Guide*

Related Topic	Document Title
MPLS Forwarding commands	*MPLS Forwarding Commands on Cisco IOS XR Software* module in *Cisco IOS XR MPLS Command Reference for the Cisco ASR 9000 Series Router*
Getting started material	*Cisco IOS XR Getting Started Guide for the Cisco ASR 9000 Series Router*
Information about user groups and task IDs	*Configuring AAA Services on Cisco IOS XR Software* module of *Cisco IOS XR System Security Configuration Guide for the Cisco ASR 9000 Series Router*

Standards

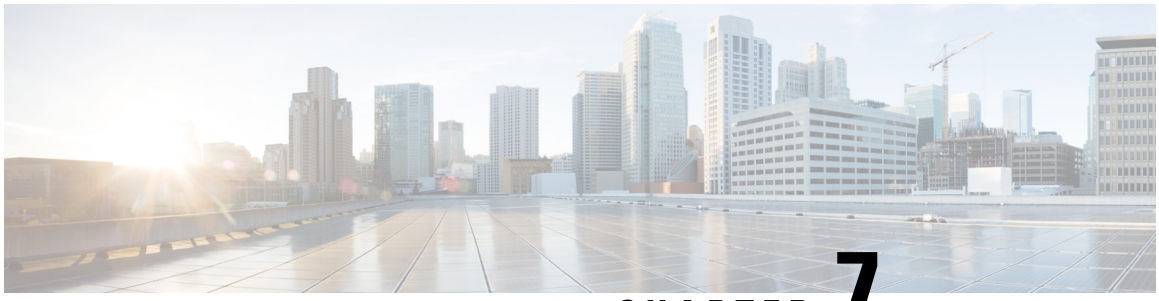
Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
RFC 3031	*Multiprotocol Label Switching Architecture*
RFC 3443	*Time to Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*
RFC 4105	*Requirements for Inter-Area MPLS Traffic Engineering*



CHAPTER 7

Implementing MPLS Traffic Engineering

This module describes how to implement MPLS Traffic Engineering on Cisco ASR 9000 Series Router.

Multiprotocol Label Switching (MPLS) is a standards-based solution driven by the Internet Engineering Task Force (IETF) that was devised to convert the Internet and IP backbones from best-effort networks into business-class transport mediums.

MPLS, with its label switching capabilities, eliminates the need for an IP route look-up and creates a virtual circuit (VC) switching function, allowing enterprises the same performance on their IP-based network services as with those delivered over traditional networks such as Frame Relay or Asynchronous Transfer Mode (ATM).

MPLS traffic engineering (MPLS-TE) software enables an MPLS backbone to replicate and expand upon the TE capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what now can be achieved only by overlaying a Layer 3 network on a Layer 2 network.

Note The LMP and GMPLS-NNI features are not supported on PRP hardware.

Feature History for Implementing MPLS-TE

Release	Modification
Release 3.7.2	This feature was introduced.
Release 3.9.0	The MPLS Traffic Engineering (TE): Path Protection feature was added.
Release 3.9.1	The MPLS-TE automatic bandwidth feature is supported.
Release 4.1.0	Support was added for the following features: • Ignore Intermediate System-to-Intermediate System Overload Bit Setting in MPLS-TE • Point-to-Multipoint Traffic-Engineering
Release 4.1.1	The Auto-Tunnel Mesh feature was added.

Release	Modification
Release 4.2.0	Support was added for the following features: • Soft-Preemption • Path Option Attributes
Release 4.2.1	The Auto-Tunnel Attribute-set feature was added for auto-backup tunnels.
Release 4.2.3	Support was added for the following features: • End-to-End TE Path Protection Enhancements — Explicit Path Protection and Co-existence of Path Protection with Fast Reroute • P2MP-TE Inter-area Enhancements
	Support was added for the following features: • P2MP-TE Auto-tunnels • Set DF Bit
Release 5.2.2	Make-Before-Break feature was added.
Release 5.3.2	Policy-Based Tunnel Selection for IPv6 feature was added.
Release 5.3.2	Stateful PCE Enhancements were made.
Release 6.0	Introduced Service Path Preference
Release 6.0.1	Point-to-Multipoint Implicit Null feature was added.
Release 6.1.2	Named Tunnel feature was added.
Release 6.4.1	Enabling Forward Class Zero in PBTS feature was added.
Release 7.1.1	IS-IS autoroute announce function was enhanced. Traffic from MPLS-TE tunnel traffic source IP address prefixes can be steered towards matching IP addresses assigned on tunnel destination interfaces.
Release 7.3.2	In case of an LSP error on a head-end router, this feature introduces the flexibility to either set a timer for the router to retry sending traffic, or resend traffic across a different LSP without a waiting period.

- Prerequisites for Implementing Cisco MPLS Traffic Engineering, on page 201
- Information About Implementing MPLS Traffic Engineering, on page 201
- How to Implement Traffic Engineering, on page 260
- Configuration Examples for Cisco MPLS-TE, on page 386
- Regular expressions in MPLS-TE tunnel names, on page 418
- Configuring Performance Measurement, on page 421
- Additional References, on page 423

Prerequisites for Implementing Cisco MPLS Traffic Engineering

These prerequisites are required to implement MPLS TE:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- Router that runs Cisco IOS XR software .
- Installed composite mini-image and the MPLS package, or a full composite image.
- IGP activated.

Information About Implementing MPLS Traffic Engineering

To implement MPLS-TE, you should understand these concepts:

Overview of MPLS Traffic Engineering

MPLS-TE software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what now can be achieved only by overlaying a Layer 3 network on a Layer 2 network.

MPLS-TE is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures. MPLS-TE provides an integrated approach to traffic engineering. With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

Note MPLS-TE Nonstop Routing (NSR) is enabled by default without any user configuration and cannot be disabled.

MPLS-TE NSR means the application is in hot-standby mode and standby MPLS-TE instance is ready to take over from the active instance quickly on RP failover.

Note that the MPLS-TE does not do routing. If there is standby card available then the MPLS-TE instance is in a hot-standby position.

The following output shows the status of MPLS-TE NSR:

```
Router#show mpls traffic-eng nsr status

TE Process Role        : V1 Active
Current Status      : Ready
    Ready since        : Tue Nov 01 10:42:34 UTC 2022 (1w3d ago)
   IDT started         : Tue Nov 01 03:28:48 UTC 2022 (1w3d ago)
    IDT ended          : Tue Nov 01 03:28:48 UTC 2022 (1w3d ago)
Previous Status        : Not ready
    Not ready reason   : Collaborator disconnected
    Not ready since    : Tue Nov 01 10:42:34 UTC 2022 (1w3d ago)
```

During any issues with the MPLS-TE, the NSR on the router gets affected which is displayed in the show redundancy output as follows:

```
Router#show mpls traffic-eng nsr status details
.
.
.

Current active rmf state: 4 (I_READY)
All standby not-ready bits clear - standby should be ready

Current active rmf state for NSR: Not ready
<jid> <node> <name> Reason for standby not NSR-ready
1082 0/RP0/CPU0 te_control TE NSR session not synchronized
Not ready set Wed Nov 19 17:28:14 2022: 5 hours, 23 minutes ago
1082 0/RP1/CPU0 te_control Standby not connected
Not ready set Wed Nov 19 17:29:11 2022: 5 hours, 22 minutes ago
```

Note If you have disabled MPLS-TE NSR and configured only MPLS-TE nonstop forwarding (NSF), performing an RP failover results in a verification error causing unprotected LSPs to flap and triggering FRR on protected LSPs. To avoid the verification error, you must block the path verification using the **mpls traffic-eng topology block-verify-after-rpfo** command.

Related Topics

Configuring Forwarding over the MPLS-TE Tunnel, on page 268

Benefits of MPLS Traffic Engineering

MPLS-TE enables ISPs to route network traffic to offer the best service to their users in terms of throughput and delay. By making the service provider more efficient, traffic engineering reduces the cost of the network.

Currently, some ISPs base their services on an overlay model. In the overlay model, transmission facilities are managed by Layer 2 switching. The routers see only a fully meshed virtual topology, making most

destinations appear one hop away. If you use the explicit Layer 2 transit layer, you can precisely control how traffic uses available bandwidth. However, the overlay model has numerous disadvantages. MPLS-TE achieves the TE benefits of the overlay model without running a separate network and without a non-scalable, full mesh of router interconnects.

How MPLS-TE Works

MPLS-TE automatically establishes and maintains label switched paths (LSPs) across the backbone by using RSVP. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth. Available resources are flooded by means of extensions to a link-state-based Interior Gateway Protocol (IGP).

MPLS-TE tunnels are calculated at the LSP headend router, based on a fit between the required and available resources (constraint-based routing). The IGP automatically routes the traffic to these LSPs.

Typically, a packet crossing the MPLS-TE backbone travels on a single LSP that connects the ingress point to the egress point. MPLS-TE is built on these mechanisms:

Tunnel interfaces

From a Layer 2 standpoint, an MPLS tunnel interface represents the headend of an LSP. It is configured with a set of resource requirements, such as bandwidth and media requirements, and priority. From a Layer 3 standpoint, an LSP tunnel interface is the headend of a unidirectional virtual link to the tunnel destination.

MPLS-TE path calculation module

This calculation module operates at the LSP headend. The module determines a path to use for an LSP. The path calculation uses a link-state database containing flooded topology and resource information.

RSVP with TE extensions

RSVP operates at each LSP hop and is used to signal and maintain LSPs based on the calculated path.

MPLS-TE link management module

This module operates at each LSP hop, performs link call admission on the RSVP signaling messages, and performs bookkeeping on topology and resource information to be flooded.

Link-state IGP (Intermediate System-to-Intermediate System [IS-IS] or Open Shortest Path First [OSPF]—each with traffic engineering extensions)

These IGPs are used to globally flood topology and resource information from the link management module.

Enhancements to the shortest path first (SPF) calculation used by the link-state IGP (IS-IS or OSPF)

The IGP automatically routes traffic to the appropriate LSP tunnel, based on tunnel destination. Static routes can also be used to direct traffic to LSP tunnels.

Label switching forwarding

This forwarding mechanism provides routers with a Layer 2-like ability to direct traffic across multiple hops of the LSP established by RSVP signaling.

One approach to engineering a backbone is to define a mesh of tunnels from every ingress device to every egress device. The MPLS-TE path calculation and signaling modules determine the path taken by the LSPs for these tunnels, subject to resource availability and the dynamic state of the network.

The IGP (operating at an ingress device) determines which traffic should go to which egress device, and steers that traffic into the tunnel from ingress to egress. A flow from an ingress device to an egress device might be so large that it cannot fit over a single link, so it cannot be carried by a single tunnel. In this case, multiple tunnels between a given ingress and egress can be configured, and the flow is distributed using load sharing among the tunnels.

Note GRE over MPLS-TE tunnel is not supported. Hence, you cannot carry GRE traffic over an LSP established for MPLS-TE tunnel using RSVP-TE. This restriction also applies to SR-TE tunnels.

Related Topics

Building MPLS-TE Topology, on page 260
Creating an MPLS-TE Tunnel, on page 262
Build MPLS-TE Topology and Tunnels: Example, on page 387

MPLS Traffic Engineering

Multiprotocol Label Switching (MPLS) is an Internet Engineering Task Force (IETF)-specified framework that provides efficient designation, routing, forwarding, and switching of traffic flows through the network.

TE is the process of adjusting bandwidth allocations to ensure that enough bandwidth is available for high-priority traffic.

In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream and sets the bandwidth available for that tunnel.

Backup AutoTunnels

The MPLS Traffic Engineering AutoTunnel Backup feature enables a router to dynamically build backup tunnels on the interfaces that are configured with MPLS TE tunnels. This feature enables a router to dynamically build backup tunnels when they are needed. This prevents you from having to build MPLS TE tunnels **statically**.

The MPLS Traffic Engineering (TE)—AutoTunnel Backup feature has these benefits:

- Backup tunnels are built automatically, eliminating the need for users to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface.
- Protection is expanded—FRR does not protect IP traffic that is not using the TE tunnel or Label Distribution Protocol (LDP) labels that are not using the TE tunnel.

This feature protects against these failures:

- **P2P Tunnel NHOP protection**—Protects against link failure for the associated P2P protected tunnel
- **P2P Tunnel NNHOP protection**—Protects against node failure for the associated P2P protected tunnel
- **P2MP Tunnel NHOP protection**—Protects against link failure for the associated P2MP protected tunnel

Related Topics

Enabling an AutoTunnel Backup, on page 277
Removing an AutoTunnel Backup, on page 278
Establishing MPLS Backup AutoTunnels to Protect Fast Reroutable TE LSPs, on page 279

Establishing Next-Hop Tunnels with Link Protection, on page 280
Configure the MPLS-TE Auto-Tunnel Backup: Example, on page 401

AutoTunnel Attribute-set

This feature supports auto-tunnels configuration using attribute templates, known as attribute-set. The TE attribute-set template that specifies a set of TE tunnel attributes, is locally configured at the head-end of auto-tunnels. The control plane triggers the automatic provisioning of a corresponding TE tunnel, whose characteristics are specified in the respective attribute-set.

Currently, auto-tunnel backups are created with the default values of all tunnel attributes. To support configurable attributes for auto-tunnel backup, it is required to configure attribute-set and assign it to the backup tunnels. The attribute-set consists of a set of tunnel attributes such as priority, affinity, signaled bandwidth, logging, policy-class, record-route and so on.

The following rules (consistent across all auto-tunnels) apply while configuring the attribute-set:

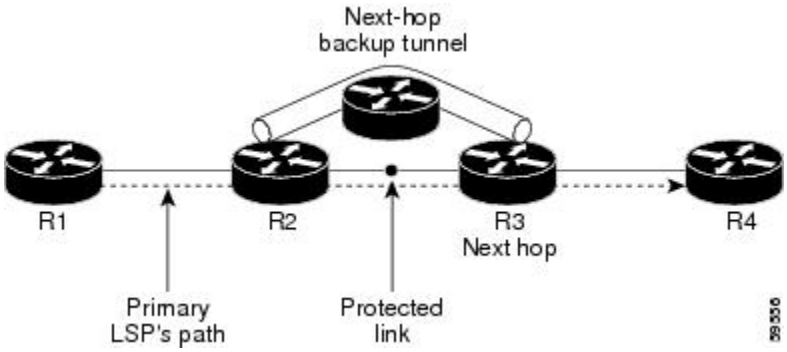
- If no attribute-set template is defined, the auto-tunnels is created using default attribute values.
- If an attribute-set is defined and the attribute-set template is already configured, the auto-tunnel is created using the attributes specified in the associated attribute-set.
- If an attribute-set is assigned, but it is not defined or configured, auto-tunnel is not created.
- Any number of attribute-sets can be configured with same attribute settings.
- Empty tunnel attribute implies all parameters have default values.
- When specific attribute is not specified in the attribute-set, a default value for that attribute is used.

Link Protection

The backup tunnels that bypass only a single link of the LSP path provide link protection. They protect LSPs, if a link along their path fails, by rerouting the LSP traffic to the next hop, thereby bypassing the failed link. These are referred to as NHOP backup tunnels because they terminate at the LSP's next hop beyond the point of failure.

This figure illustrates link protection.

Figure 15: Link Protection



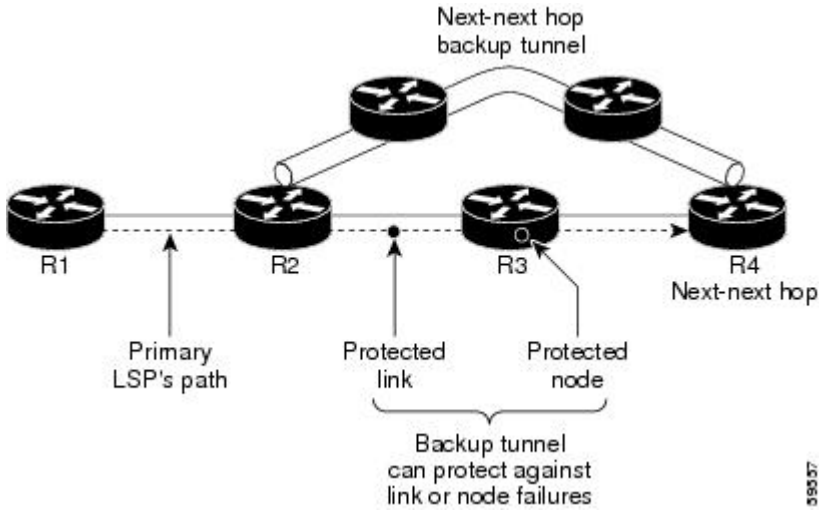
Node Protection

The backup tunnels that bypass next-hop nodes along LSP paths are called NNHOP backup tunnels because they terminate at the node following the next-hop node of the LSPs, thereby bypassing the next-hop node.

They protect LSPs by enabling the node upstream of a link or node failure to reroute the LSPs and their traffic around a node failure to the next-hop node. NNHOP backup tunnels also provide protection from link failures because they bypass the failed link and the node.

This figure illustrates node protection.

Figure 16: Node Protection



Backup AutoTunnel Assignment

At the head or mid points of a tunnel, the backup assignment finds an appropriate backup to protect a given primary tunnel for FRR protection.

The backup assignment logic is performed differently based on the type of backup configured on the output interface used by the primary tunnel. Configured backup types are:

- Static Backup
- AutoTunnel Backup
- No Backup (In this case no backup assignment is performed and the tunnels is unprotected.)

Note Static backup and Backup AutoTunnel cannot exist together on the same interface or link.

Note Node protection is always preferred over link protection in the Backup AutoTunnel assignment.

In order that the Backup AutoTunnel feature operates successfully, the following configuration must be applied at global configuration level:

```
ipv4 unnumbered mpls traffic-eng Loopback 0
```

Note The Loopback 0 is used as router ID.

Explicit Paths

Explicit paths are used to create backup autotunnels as follows:

For NHOP Backup Autotunnels:

- NHOP excludes the protected link's local IP address.
- NHOP excludes the protected link’s remote IP address.
- The explicit-path name is _autob_nhop_tunnelxxx, where xxx matches the dynamically created backup tunnel ID.

For NNHOP Backup Autotunnels:

- NNHOP excludes the protected link’s local IP address.
- NNHOP excludes the protected link’s remote IP address (link address on next hop).
- NNHOP excludes the NHOP router ID of the protected primary tunnel next hop.
- The explicit-path name is _autob_nnhop_tunnelxxx, where xxx matches the dynamically created backup tunnel ID.

Periodic Backup Promotion

The periodic backup promotion attempts to find and assign a better backup for primary tunnels that are already protected.

With AutoTunnel Backup, the only scenario where two backups can protect the same primary tunnel is when both an NHOP and NNHOP AutoTunnel Backups get created. The backup assignment takes place as soon as the NHOP and NNHOP backup tunnels come up. So, there is no need to wait for the periodic promotion.

Although there is no exception for AutoTunnel Backups, periodic backup promotion has no impact on primary tunnels protected by AutoTunnel Backup.

One exception is when a manual promotion is triggered by the user using the **mpls traffic-eng fast-reroute timers promotion** command, where backup assignment or promotion is triggered on all FRR protected primary tunnels--even unprotected ones. This may trigger the immediate creation of some AutoTunnel Backup, if the command is entered within the time window when a required AutoTunnel Backup has not been yet created.

You can configure the periodic promotion timer using the global configuration **mpls traffic-eng fast-reroute timers promotion** *sec* command. The range is 0 to 604800 seconds.

Note A value of 0 for the periodic promotion timer disables the periodic promotion.

Protocol-Based CLI

Cisco IOS XR software provides a protocol-based command line interface. The CLI provides commands that can be used with the multiple IGP protocols supported by MPLS-TE.

Differentiated Services Traffic Engineering

MPLS Differentiated Services (Diff-Serv) Aware Traffic Engineering (DS-TE) is an extension of the regular MPLS-TE feature. Regular traffic engineering does not provide bandwidth guarantees to different traffic classes. A single bandwidth constraint is used in regular TE that is shared by all traffic. To support various classes of service (CoS), users can configure multiple bandwidth constraints. These bandwidth constraints can be treated differently based on the requirement for the traffic class using that constraint.

MPLS DS-TE provides the ability to configure multiple bandwidth constraints on an MPLS-enabled interface. Available bandwidths from all configured bandwidth constraints are advertised using IGP. TE tunnel is configured with bandwidth value and class-type requirements. Path calculation and admission control take the bandwidth and class-type into consideration. RSVP is used to signal the TE tunnel with bandwidth and class-type requirements.

MPLS DS-TE is deployed with either Russian Doll Model (RDM) or Maximum Allocation Model (MAM) for bandwidth calculations.

Cisco IOS XR software supports two DS-TE modes: Prestandard and IETF.

Related Topics

Confirming DiffServ-TE Bandwidth, on page 157
Bandwidth Configuration (MAM): Example, on page 181
Bandwidth Configuration (RDM): Example, on page 181

Prestandard DS-TE Mode

Prestandard DS-TE uses the Cisco proprietary mechanisms for RSVP signaling and IGP advertisements. This DS-TE mode does not interoperate with third-party vendor equipment. Note that prestandard DS-TE is enabled only after configuring the sub-pool bandwidth values on MPLS-enabled interfaces.

Prestandard Diff-Serve TE mode supports a single bandwidth constraint model a Russian Doll Model (RDM) with two bandwidth pools: global-pool and sub-pool.

TE class map is not used with Prestandard DS-TE mode.

Related Topics

Configuring a Prestandard DS-TE Tunnel, on page 282
Configure IETF DS-TE Tunnels: Example, on page 388

IETF DS-TE Mode

IETF DS-TE mode uses IETF-defined extensions for RSVP and IGP. This mode interoperates with third-party vendor equipment.

IETF mode supports multiple bandwidth constraint models, including RDM and MAM, both with two bandwidth pools. In an IETF DS-TE network, identical bandwidth constraint models must be configured on all nodes.

TE class map is used with IETF DS-TE mode and must be configured the same way on all nodes in the network.

Bandwidth Constraint Models

IETF DS-TE mode provides support for the RDM and MAM bandwidth constraints models. Both models support up to two bandwidth pools.

Cisco IOS XR software provides global configuration for the switching between bandwidth constraint models. Both models can be configured on a single interface to preconfigure the bandwidth constraints before swapping to an alternate bandwidth constraint model.

Note NSF is not guaranteed when you change the bandwidth constraint model or configuration information.

By default, RDM is the default bandwidth constraint model used in both pre-standard and IETF mode.

Maximum Allocation Bandwidth Constraint Model

The MAM constraint model has the following characteristics:

- Easy to use and intuitive.
- Isolation across class types.
- Simultaneously achieves isolation, bandwidth efficiency, and protection against QoS degradation.

Related Topics

Configuring an IETF DS-TE Tunnel Using MAM, on page 285

Russian Doll Bandwidth Constraint Model

The RDM constraint model has these characteristics:

- Allows greater sharing of bandwidth among different class types.
- Ensures bandwidth efficiency simultaneously and protection against QoS degradation of all class types.
- Specifies that it is used in conjunction with preemption to simultaneously achieve isolation across class-types such that each class-type is guaranteed its share of bandwidth, bandwidth efficiency, and protection against QoS degradation of all class types.

Note We recommend that RDM not be used in DS-TE environments in which the use of preemption is precluded. Although RDM ensures bandwidth efficiency and protection against QoS degradation of class types, it does guarantee isolation across class types.

Related Topics

Configuring an IETF DS-TE Tunnel Using RDM, on page 283

TE Class Mapping

Each of the eight available bandwidth values advertised in the IGP corresponds to a TE class. Because the IGP advertises only eight bandwidth values, there can be a maximum of only eight TE classes supported in an IETF DS-TE network.

TE class mapping must be exactly the same on all routers in a DS-TE domain. It is the responsibility of the operator configure these settings properly as there is no way to automatically check or enforce consistency.

The operator must configure TE tunnel class types and priority levels to form a valid TE class. When the TE class map configuration is changed, tunnels already up are brought down. Tunnels in the down state, can be set up if a valid TE class map is found.

The default TE class and attributes are listed. The default mapping includes four class types.

Table 8: TE Classes and Priority

TE Class	Class Type	Priority
0	0	7
1	1	7
2	Unused	—
3	Unused	—
4	0	0
5	1	0
6	Unused	—
7	Unused	—

Flooding

Available bandwidth in all configured bandwidth pools is flooded on the network to calculate accurate constraint paths when a new TE tunnel is configured. Flooding uses IGP protocol extensions and mechanisms to determine when to flood the network with bandwidth.

Flooding Triggers

TE Link Management (TE-Link) notifies IGP for both global pool and sub-pool available bandwidth and maximum bandwidth to flood the network in these events:

- Periodic timer expires (this does not depend on bandwidth pool type).
- Tunnel origination node has out-of-date information for either available global pool or sub-pool bandwidth, causing tunnel admission failure at the midpoint.
- Consumed bandwidth crosses user-configured thresholds. The same threshold is used for both global pool and sub-pool. If one bandwidth crosses the threshold, both bandwidths are flooded.

Flooding Thresholds

Flooding frequently can burden a network because all routers must send out and process these updates. Infrequent flooding causes tunnel heads (tunnel-originating nodes) to have out-of-date information, causing tunnel admission to fail at the midpoints.

You can control the frequency of flooding by configuring a set of thresholds. When locked bandwidth (at one or more priority levels) crosses one of these thresholds, flooding is triggered.

Thresholds apply to a percentage of the maximum available bandwidth (the global pool), which is locked, and the percentage of maximum available guaranteed bandwidth (the sub-pool), which is locked. If, for one or more priority levels, either of these percentages crosses a threshold, flooding is triggered.



Note Setting up a global pool TE tunnel can cause the locked bandwidth allocated to sub-pool tunnels to be reduced (and hence to cross a threshold). A sub-pool TE tunnel setup can similarly cause the locked bandwidth for global pool TE tunnels to cross a threshold. Thus, sub-pool TE and global pool TE tunnels can affect each other when flooding is triggered by thresholds.

Fast Reroute

Fast Reroute (FRR) provides link protection to LSPs enabling the traffic carried by LSPs that encounter a failed link to be rerouted around the failure. The reroute decision is controlled locally by the router connected to the failed link. The headend router on the tunnel is notified of the link failure through IGP or through RSVP. When it is notified of a link failure, the headend router attempts to establish a new LSP that bypasses the failure. This provides a path to reestablish links that fail, providing protection to data transfer.

FRR (link or node) is supported over sub-pool tunnels the same way as for regular TE tunnels. In particular, when link protection is activated for a given link, TE tunnels eligible for FRR are redirected into the protection LSP, regardless of whether they are sub-pool or global pool tunnels.



Note The ability to configure FRR on a per-LSP basis makes it possible to provide different levels of fast restoration to tunnels from different bandwidth pools.

You should be aware of these requirements for the backup tunnel path:

- Backup tunnel must not pass through the element it protects.
- Primary tunnel and a backup tunnel should intersect at least at two points (nodes) on the path: point of local repair (PLR) and merge point (MP). PLR is the headend of the backup tunnel, and MP is the tailend of the backup tunnel.



Note When you configure TE tunnel with multiple protection on its path and merge point is the same node for more than one protection, you must configure record-route for that tunnel.

Note If FRR is greater than 50ms, it might lead to a loss of traffic.

Related Topics

Protecting MPLS Tunnels with Fast Reroute, on page 270

MPLS-TE and Fast Reroute over Link Bundles

MPLS Traffic Engineering (TE) and Fast Reroute (FRR) are supported over bundle interfaces and virtual local area network (VLAN) interfaces. Bidirectional forwarding detection (BFD) over VLAN is used as an FRR trigger to obtain less than 50 milliseconds of switchover time.

These link bundle types are supported for MPLS-TE/FRR:

- Over Ethernet link bundles.
- Over VLANs over Ethernet link bundles.
- Number of links are limited to 100 for MPLS-TE and FRR.
- VLANs go over any Ethernet interface (for example, GigabitEthernet and TenGigE).

FRR is supported over bundle interfaces in the following ways:

- Uses minimum links as a threshold to trigger FRR over a bundle interface.
- Uses the minimum total available bandwidth as a threshold to trigger FRR.

Ignore Intermediate System-to-Intermediate System Overload Bit Setting in MPLS-TE

The Ignore Intermediate System-to-Intermediate System (IS-IS) overload bit avoidance feature allows network administrators to prevent RSVP-TE label switched paths (LSPs) from being disabled, when a router in that path has its Intermediate System-to-Intermediate System (IS-IS) overload bit set.

The IS-IS overload bit avoidance feature is activated using this command:

```
mpls traffic-eng path-selection ignore overload
```

The IS-IS overload bit avoidance feature is deactivated using the **no** form of this command:

```
no mpls traffic-eng path-selection ignore overload
```

When the IS-IS overload bit avoidance feature is activated, all nodes, including head nodes, mid nodes, and tail nodes, with the overload bit set, are ignored. This means that they are still available for use with RSVP-TE label switched paths (LSPs). This feature enables you to include an overloaded node in CSPF.

Enhancement Options of IS-IS OLA

You can restrict configuring IS-IS overload bit avoidance with the following enhancement options:

- **path-selection ignore overload head**

The tunnels stay up if **set-overload-bit** is set by IS-IS on the head router. Ignores overload during CSPF for LSPs originating from an overloaded node. In all other cases (mid, tail, or both), the tunnel stays down.

- **path-selection ignore overload mid**

  The tunnels stay up if **set-overload-bit** is set by IS-IS on the mid router. Ignores overload during CSPF for LSPs transiting from an overloaded node. In all other cases (head, tail, or both), the tunnel stays down.

- **path-selection ignore overload tail**

  The tunnels stay up if **set-overload-bit** is set by IS-IS on the tail router. Ignores overload during CSPF for LSPs terminating at an overloaded node. In all other cases (head, mid, or both), the tunnel stays down.

- **path-selection ignore overload**

  The tunnels stay up irrespective of on which router the **set-overload-bit** is set by IS-IS.

Note When you do not select any of the options, including head nodes, mid nodes, and tail nodes, you get a behavior that is applicable to all nodes. This behavior is backward compatible in nature.

For more information related to IS-IS overload avoidance related commands, see *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Related Topics

Configuring the Ignore Integrated IS-IS Overload Bit Setting in MPLS-TE, on page 289
Configure the Ignore IS-IS Overload Bit Setting in MPLS-TE: Example, on page 389

Flexible Name-based Tunnel Constraints

MPLS-TE Flexible Name-based Tunnel Constraints provides a simplified and more flexible means of configuring link attributes and path affinities to compute paths for MPLS-TE tunnels.

In the traditional TE scheme, links are configured with attribute-flags that are flooded with TE link-state parameters using Interior Gateway Protocols (IGPs), such as Open Shortest Path First (OSPF).

MPLS-TE Flexible Name-based Tunnel Constraints lets you assign, or map, up to 32 color names for affinity and attribute-flag attributes instead of 32-bit hexadecimal numbers. After mappings are defined, the attributes can be referred to by the corresponding color name in the command-line interface (CLI). Furthermore, you can define constraints using *include*, *include-strict*, *exclude*, and *exclude-all* arguments, where each statement can contain up to 10 colors, and define include constraints in both loose and strict sense.

Note You can configure affinity constraints using attribute flags or the Flexible Name Based Tunnel Constraints scheme; however, when configurations for both schemes exist, only the configuration pertaining to the new scheme is applied.

Related Topics

Assigning Color Names to Numeric Values, on page 290

Associating Affinity-Names with TE Links, on page 291
Associating Affinity Constraints for TE Tunnels, on page 292
Configure Flexible Name-based Tunnel Constraints: Example, on page 390

MPLS Traffic Engineering Interarea Tunneling

These topics describe the following new extensions of MPLS-TE:

- Interarea Support, on page 214
- Multiarea Support, on page 215
- Loose Hop Expansion, on page 216
- Loose Hop Reoptimization, on page 216
- Fast Reroute Node Protection, on page 216

Interarea Support

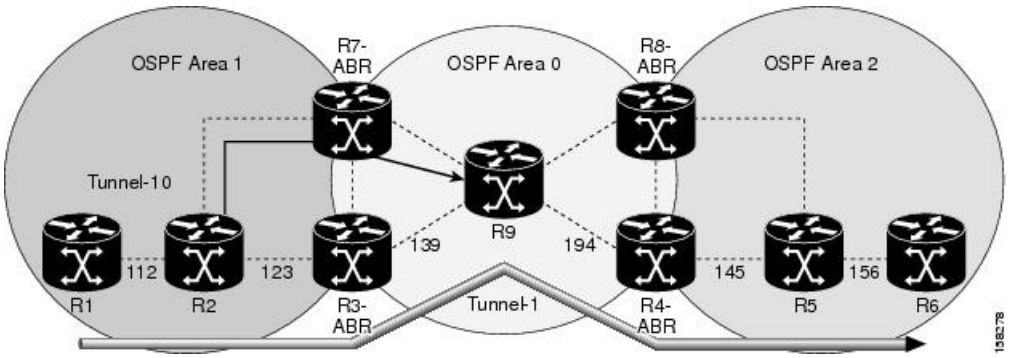
The MPLS-TE interarea tunneling feature allows you to establish P2P and P2MP TE tunnels spanning multiple Interior Gateway Protocol (IGP) areas and levels, thereby eliminating the requirement that headend and tailend routers reside in a single area.

Interarea support allows the configuration of a TE LSP that spans multiple areas, where its headend and tailend label switched routers (LSRs) reside in different IGP areas.

Multiarea and Interarea TE are required by the customers running multiple IGP area backbones (primarily for scalability reasons). This lets you limit the amount of flooded information, reduces the SPF duration, and lessens the impact of a link or node failure within an area, particularly with large WAN backbones split in multiple areas.

Figure 17: Interarea (OSPF) TE Network Diagram

This figure shows a typical interarea TE network.



Note Interarea MPLS-TE tunnels per-area path computation based on ERO expansion on the head-end LSR and on ABRs have the following options while selecting ABR:

- Static configuration of ABRs as loose hops at the head-end LSR.
- Dynamic ABR selection.

When a static configuration is used, a loosely routed explicit path must be defined for the tunnel LSP that identifies each ABR the LSP should traverse. The head-end router and the ABRs along the specified explicit path must expand automatically the loose hops, each one computing the strict path segment to the next ABR or tunnel destination.

Restrictions

MPLS-TE Interarea tunnels cannot use **next-address strict** to the ABRs.

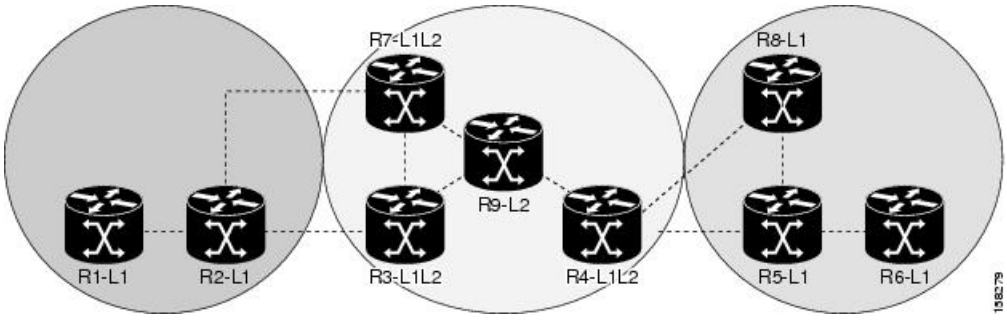
Multiarea Support

Multiarea support allows an area border router (ABR) LSR to support MPLS-TE in more than one IGP area. A TE LSP is still confined to a single area.

Multiarea and Interarea TE are required when you run multiple IGP area backbones. The Multiarea and Interarea TE allows you to:

- Limit the volume of flooded information.
- Reduce the SPF duration.
- Decrease the impact of a link or node failure within an area.

Figure 18: Interlevel (IS-IS) TE Network



As shown in the figure, R2, R3, R7, and R4 maintain two databases for routing and TE information. For example, R3 has TE topology information related to R2, flooded through Level-1 IS-IS LSPs plus the TE topology information related to R4, R9, and R7, flooded as Level 2 IS-IS Link State PDUs (LSPs) (plus, its own IS-IS LSP).

Note You can configure multiple areas within an IS-IS Level 1. This is transparent to TE. TE has topology information about the IS-IS level, but not the area ID.

Loose Hop Expansion

Loose hop optimization allows the reoptimization of tunnels spanning multiple areas and solves the problem which occurs when an MPLS-TE LSP traverses hops that are not in the LSP's headend's OSPF area and IS-IS level.

Interarea MPLS-TE allows you to configure an interarea traffic engineering (TE) label switched path (LSP) by specifying a loose source route of ABRs along the path. It is the then the responsibility of the ABR (having a complete view of both areas) to find a path obeying the TE LSP constraints within the next area to reach the next hop ABR (as specified on the headend). The same operation is performed by the last ABR connected to the tailend area to reach the tailend LSR.

For P2MP-TE tunnels, ABRs support loose hop ERO expansion to find path to the next ABR until it reaches to the tail-end LSR, without introducing remerge.

You must be aware of these considerations when using loose hop optimization:

- You must specify the router ID of the ABR node (as opposed to a link address on the ABR).
- When multiarea is deployed in a network that contains subareas, you must enable MPLS-TE in the subarea for TE to find a path when loose hop is specified.
- You must specify the reachable explicit path for the interarea tunnel.

Loose Hop Reoptimization

Loose hop reoptimization allows the reoptimization of the tunnels spanning multiple areas and solves the problem which occurs when an MPLS-TE headend does not have visibility into other IGP areas.

Whenever the headend attempts to reoptimize a tunnel, it tries to find a better path to the ABR in the headend area. If a better path is found then the headend initiates the setup of a new LSP. In case a suitable path is not found in the headend area, the headend initiates a querying message. The purpose of this message is to query the ABRs in the areas other than the headend area to check if there exist any better paths in those areas. The purpose of this message is to query the ABRs in the areas other than the headend area, to check if a better path exists. If a better path does not exist, ABR forwards the query to the next router downstream. Alternatively, if better path is found, ABR responds with a special Path Error to the headend to indicate the existence of a better path outside the headend area. Upon receiving the Path Error that indicates the existence of a better path, the headend router initiates the reoptimization.

ABR Node Protection

Because one IGP area does not have visibility into another IGP area, it is not possible to assign backup to protect ABR node. To overcome this problem, node ID sub-object is added into the record route object of the primary tunnel so that at a PLR node, backup destination address can be checked against primary tunnel record-route object and assign a backup tunnel.

Fast Reroute Node Protection

If a link failure occurs within an area, the upstream router directly connected to the failed link generates an RSVP path error message to the headend. As a response to the message, the headend sends an RSVP path tear message and the corresponding path option is marked as invalid for a specified period and the next path-option (if any) is evaluated.

To retry the ABR immediately, a second path option (identical to the first one) should be configured. Alternatively, the retry period (path-option hold-down, 2 minutes by default) can be tuned to achieve a faster retry.

Related Topics

Protecting MPLS Tunnels with Fast Reroute, on page 270

Make-Before-Break

The MPLS TE Make-Before-Break (MBB) explicit path and path option feature allows tunnels whose explicit paths or path options are modified to be reoptimized without losing any data. An explicit path or a path option modification is entirely configuration driven. Any change to an in-use path option or an in-use explicit path of a tunnel triggers the MBB procedure.

MBB lets the LSP hold on to the existing resources until the new path is successfully established and traffic has been directed over to the new LSP before the original LSP is torn down. This ensures that no data packets are lost during the transition to the new LSP.

With this feature the flapping of tunnels whose explicit paths or path options are modified, is avoided. This feature is enabled by default.

MPLS-TE Forwarding Adjacency

The MPLS-TE Forwarding Adjacency feature allows a network administrator to handle a traffic engineering, label-switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the Shortest Path First (SPF) algorithm. A forwarding adjacency can be created between routers regardless of their location in the network.

MPLS-TE Forwarding Adjacency Benefits

TE tunnel interfaces are advertised in the IGP network just like any other links. Routers can then use these advertisements in their IGPs to compute the SPF even if they are not the head end of any TE tunnels.

Related Topics

Configuring MPLS-TE Forwarding Adjacency, on page 296
Configure Forwarding Adjacency: Example, on page 392

MPLS-TE Forwarding Adjacency Restrictions

The MPLS-TE Forwarding Adjacency feature has these restrictions:

- Using the MPLS-TE Forwarding Adjacency increases the size of the IGP database by advertising a TE tunnel as a link.
- The MPLS-TE Forwarding Adjacency is supported by Intermediate System-to-Intermediate System (IS-IS).
- When the MPLS-TE Forwarding Adjacency is enabled on a TE tunnel, the link is advertised in the IGP network as a Type-Length-Value (TLV) 22 without any TE sub-TLV.
- MPLS-TE forwarding adjacency tunnels must be configured bidirectionally.
- Multicast intact is not supported with MPLS-TE Forwarding Adjacency.

MPLS-TE Forwarding Adjacency Prerequisites

Your network must support the following features before enabling the MPLS -TE Forwarding Adjacency feature:

- MPLS
- IP Cisco Express Forwarding
- Intermediate System-to-Intermediate System (IS-IS)
- OSPF

Path Computation Element

Path Computation Element (PCE) solves the specific issue of inter-domain path computation for MPLS-TE label switched path (LSPs), when the head-end router does not possess full network topology information (for example, when the head-end and tail-end routers of an LSP reside in different IGP areas).

PCE uses area border routers (ABRs) to compute a TE LSP spanning multiple IGP areas as well as computation of Inter-AS TE LSP.

PCE is usually used to define an overall architecture, which is made of several components, as follows:

Path Computation Element (PCE)

Represents a software module (which can be a component or application) that enables the router to compute paths applying a set of constraints between any pair of nodes within the router's TE topology database. PCEs are discovered through IGP.

Path Computation Client (PCC)

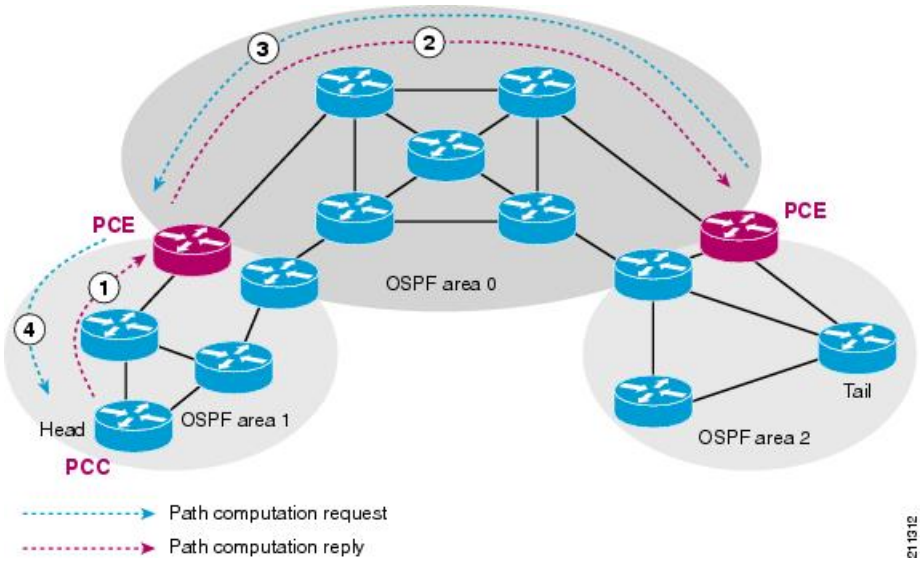
Represents a software module running on a router that is capable of sending and receiving path computation requests and responses to and from PCEs. The PCC is typically an LSR (Label Switching Router).

PCC-PCE communication protocol (PCEP)

Specifies that PCEP is a TCP-based protocol defined by the IETF PCE WG, and defines a set of messages and objects used to manage PCEP sessions and to request and send paths for multi-domain TE LSPs. PCEP is used for communication between PCC and PCE (as well as between two PCEs) and employs IGP extensions to dynamically discover PCE.

Figure 19: Path Computation Element Network Diagram

This figure shows a typical PCE implementation.



Path computation elements provides support for the following message types and objects:

- Message types: Open, PCReq, PCRep, PCErr, Close
- Objects: OPEN, CLOSE, RP, END-POINT, LSPA, BANDWIDTH, METRIC, and NO-PATH

Related Topics

Configuring a Path Computation Client, on page 297
Configuring a Path Computation Element Address, on page 298
Configuring PCE Parameters, on page 299
Configure PCE: Example, on page 392

Policy-Based Tunnel Selection

These topics provide information about policy-based tunnel selection (PBTS):

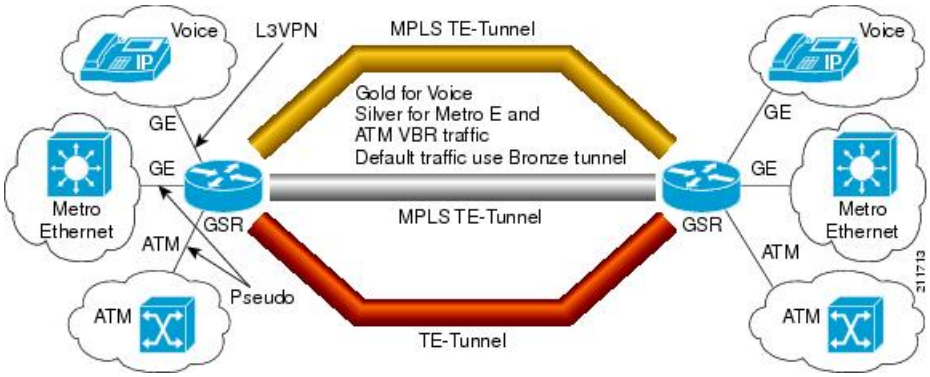
Policy-Based Tunnel Selection

Policy-Based Tunnel Selection (PBTS) provides a mechanism that lets you direct traffic into specific TE tunnels based on different criteria. PBTS will benefit Internet service providers (ISPs) who carry voice and data traffic through their MPLS and MPLS/VPN networks, who want to route this traffic to provide optimized voice service.

PBTS works by selecting tunnels based on the classification criteria of the incoming packets, which are based on the IP precedence, experimental (EXP), differentiated services code point (DSCP), or type of service (ToS) field in the packet. Default-class configured for paths is always zero (0). If there is no TE for a given forward-class, then the default-class (0) will be tried. If there is no default-class, then the packet is dropped.PBTS supports up to seven (exp 1 - 7) EXP values associated with a single TE tunnel.

Figure 20: Policy-Based Tunnel Selection Implementation

This figure illustrates a PBTS implementation.



Related Topics

Configuring Forwarding Path, on page 304

Policy-Based Tunnel Selection Functions

The following PBTS functions are supported on the Cisco ASR 9000 series router:

- Classify the IPv4 packets based on 5-Tuple values (source IP, destination IP, source port, destination port, and protocol) specified via ACL.
- Classify the IPv4 packets based on DSCP/ToS/IPP value carried in the packet, configured via ACL.
- Classify the MPLS packets based on EXP bit value carried in the packet.
- Classify the MPLS packets based on remarked EXP value (i.e., the value after taking QoS marking action).
- Ability to associate the class-map with forwarding group.
- Ability to define the forward-class for TE interface. Only one forward-class can be associated with a TE at any time. The forward-class provides ability to map multiple/any EXP or multiple classes of packets to the same forward-class.
- Support for default forward-class (0). If the TE interface is not explicitly associated with a forward-class, it is by default associated with default forward-class (0).
- PBTS is turned on the ingress interface by applying the service-policy at the targeted input interface(s).
- PBTS can be enabled on any of the L3 interfaces—physical, sub-interface, and bundle interface.
- PBTS allows in-place modification of the configuration (both class-map and forward-group to TE association).

Related Topics

Configuring Forwarding Path, on page 304

PBTS Forward Class

In PBTS, a class-map is defined for various types of packet, and associating this class-map with a forward-class. The class-map defines the matching criteria for classifying a particular type of traffic, while the forward-class defines the forwarding path these packets should take. Once a class-map is associated with a forwarding-class in the policy map, all the packets that match the class-map are forwarded as defined in the policy-map. The egress traffic engineering (TE) tunnel interfaces that the packets should take for each forwarding-class is

specified by associating the TE interface explicitly, or implicitly in the case of default value, with the forward-group. When the TE interfaces are associated with the forward-class, they can be exported to the routing protocol module using the **auto-route** command, which will then associate the route in the FIB database with these tunnels. If the TE interface is not explicitly associated with a forward-class, it gets associated with a default-class (0). All non-TE interfaces through the destination route was learned will be pushed down by routing protocol to the forwarding plane with forwarding class set to default-class.

When PBR is configured, TE tunnel interfaces are selected to forward traffic based on matching class-types in policy-map. When a forward-class value for a TE tunnel is configured, that TE process pass to LSD process as part of the label rewrite for the tunnel head. The TE allows one 32-bit value for a forward-class per tunnel that is opaque to TE and TE will use it to program the tunnel in forwarding.

PBTS supports a maximum of eight forward-class and eight TE tunnels with in each forward-class. A maximum of 32 TE tunnels can be associated with the destination route.

Forward-class configuration is supported for auto-mesh tunnels and forward-class can be configured in the attribute-set used by the auto-mesh tunnels. Changing the forward-class configuration does not affect the tunnel state. TE updates the forwarding with the new forward-class value. For TE path protection, both primary and standby LSPs use the same forward-class value for the tunnel. Unequal load-sharing of traffic is supported for the ECMP TE tunnels across forward-classes.

Forward-class configuration does not apply to the FRR backup tunnels and will be ignored. The forward-class configuration is not supported for the auto-backup tunnels and P2MP-TE (MTE) tunnels.

PBTS Restrictions

When implementing PBTS, the following restrictions are listed:

- When QoS EXP remarking on an interface is enabled, the EXP value is used to determine the egress tunnel interface, not the incoming EXP value.
- Egress-side remarking does not affect PBTS tunnel selection.
- When no default tunnel is available for forwarding, traffic is dropped.
- PBTS does not support selecting a TE tunnel for the route driven from Access Based Forwarding (ABF) lookup result.
- PBTS does not support generic routing encapsulation over traffic engineering (GREoTE).
- PBTS is supported only on L3 interfaces.
- Configuring PBTS using policy-map command is not supported. Instead, you should use forward-class configuration.
- PBTS tunnel selection is not supported on the tunnels with L2VPN configuration.
- PBTS does not support VidMon feature.
- PBTS does not support slow path, instead, default forward class is used.
- PBTS does not support subscriber sessions.
- Forward-class configuration does not apply to the FRR backup tunnels and will be ignored.
- Note that forward-class configuration will not be supported for the auto-backup tunnels.
- Forward-class configuration is not supported for P2MP-TE (MTE) tunnels.

- The policy-class configuration does not co-exist with forward-class configuration.
- DSCP, precedence, or ToS based classification has to be configured through ACL.
- PBTS supports multi-pass implementation only for IPv4 packets.

PBTS Default Class Enhancement

Policy Based Tunnel Selection (PBTS) provides a mechanism that directs traffic into TE tunnels based on incoming packets TOS/EXP bits. The PBTS default class enhancement can be explained as follows:

- Add a new class called default so that you can configure a tunnel of class (1-7 or default). You can configure more than one default tunnels. By default, tunnels of class 0 no longer serves as default tunnel.
- The control plane can pick up to 8 default tunnels to carry default traffic.
- The forwarding plane applies the same load-balancing logic on the default tunnels such that default traffic load is shared over them.
- Default tunnels are not used to forward traffic if each class of traffic is served by at least one tunnel of the respective class.
- A tunnel is implicitly assigned to class 0 if the tunnel is not configured with a specific class.
- If no default tunnel is available for forwarding, the traffic is dropped.
- Both LDP and IGP paths are assigned to a new default class. LDP and IGP no longer statically associate to class 0 in the platforms, which support this new default class enhancement.

PBTS Default Class Enhancement Restrictions

The class 0 tunnel is not the default tunnel. The **default** class that does not associate with any of existing classes starting from 1 to 7. For a class of traffic that does not have a respective class tunnel to serve it, the forwarding plane uses the available default tunnels and IGP and LDP paths to carry that class of traffic.

The new behavior becomes effective only when the control plan resolves a prefix to use at least one default tunnel to forward the traffic. When a prefix is resolved to not use any default tunnel to forward traffic, it will fall back to the existing behavior. The lowest class tunnels are used to serve as default tunnels. The class 0 tunnels are used as default tunnels, if no default tunnel is configured, supporting the backward compatibility to support the existing configurations.

Enabling Forward Class Zero in PBTS

This PBTS feature enhancement allows you to configure forward class zero or the default class as a PBTS forwarding class effective with Cisco IOS-XR release 6.4.1. Earlier, only values from one to seven were configurable as PBTS forwarding classes.

Set DF Bit

The Set DF Bit feature enables to apply 'set df (do not fragment)' policy to an interface. Any packet that matches with the set df policy will either clear the bit or set the bit.

The set df bit policy can be enabled to clear the df bit before forwarding the packet in IPv4 traffic.

For more information on Set DF Bit, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on Set DF Bit commands,

see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Policy-Based Tunnel Selection for IPv6

Policy-Based Tunnel Selection (PBTS) for IPv6 (Internet Protocol version 6) feature allows a user to manually configure the manner received packets should be routed into specific TE tunnels for IPv6. PBTS allows the user to identify packets using several attributes and to specify the TE tunnel to which a packet should be sent. For example, one selection criterion is TE tunnel selection based on differentiated services code point (DSCP) values. This is accomplished by mapping multiple DCSPs to a single forwarding class. Other criteria for selecting tunnels are based on the IP precedence, experimental (EXP), or type of service (ToS) field in the packet.

The PBTS for IPv6 feature lets the IPv6 traffic acknowledge the PBTS configuration.

Policies can be based on IPv6 address, port numbers, protocols, or packet size. For a simple policy, you use any one of the descriptors; for a complex policy, you use all descriptors.

Enabling PBTS for IPv6 on an Interface

To enable the PBTS for IPv6 feature, a prerequisite is to enable IPv6 on the core interfaces, so that the tunnel can handle IPv6 traffic. The IPv6 forwarding adjacency (FA) configuration should be made to send IPv6 traffic over IPv6 tunnels.

IPv6 PBTS allows users to override normal destination IPv6 address-based routing and forwarding results. Virtual Private Network (VPN) Routing and Forwarding (VRF) allows multiple routing instances in the Cisco IOS XR Software. The PBTS feature is VRF-aware; this means it works under multiple routing instances, beyond the default or global routing table.

Service Path Preference for MPLS VPN Sessions

Service Path Preference feature (SPP) helps control transport path for L3VPN services in traffic engineering (TE) tunnels. SPP feature provides a way for services to influence path selection while forwarding in Multiprotocol Label Switching (MPLS) or Segment Routing networks. SPP is achieved by associating a control plane policy with a forward-class based on attributes like community, next hop, or vrf (virtual routing and forwarding).

This is helpful to the service provider in situations where instead of assigning a tunnel for a specific data type like VOIP or Data, the service provider can use a BGP-attribute for a customer and traffic for this customer can be directed towards a specific TE tunnel. This helps the service provider maintain the service level agreements (SLA) for data and voice value-added services.

For more information on this feature, see the *Implementing Service Path Preference* chapter in the Cisco ASR 9000 Aggregation Services Router MPLS Configuration Guide.

For complete command reference of this feature specific commands, see the*MPLS Traffic Engineering Commands* chapter in the Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference.

Features of Service Path Preference

Service Path Preference (SPP) includes the following features:

- SPP and BGP Flow Spec are mutually exclusive

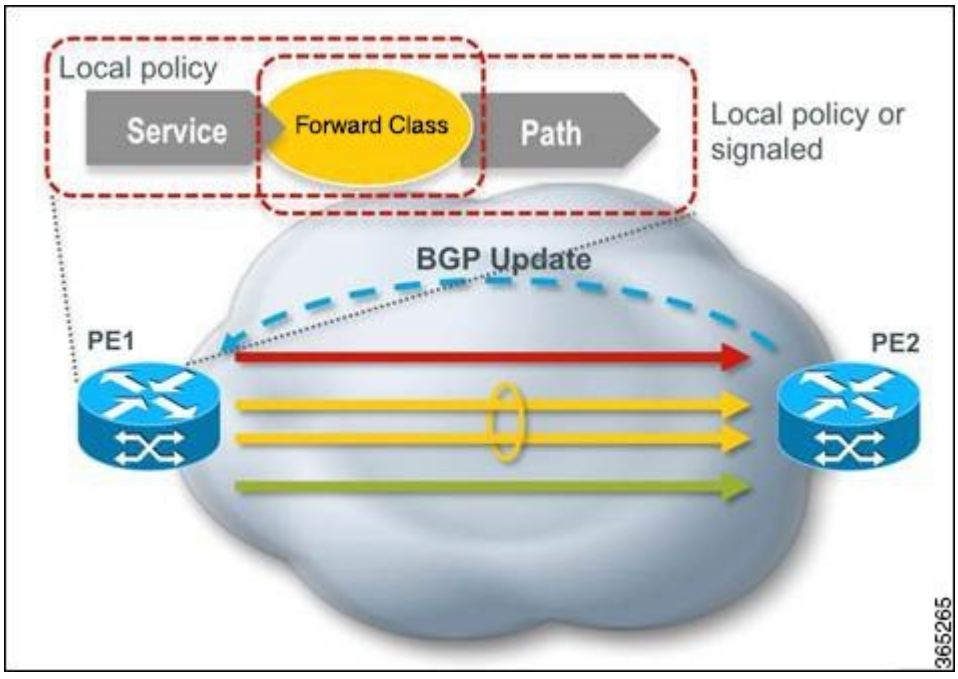
- SPP is service agnostic and can be applied to L3VPN services on an MPLS or Segment Routing core network
- SPP provides the facility to separate L3VPN services in dedicated LSPs or tunnels within the core transport network based on SLA. Therefore service delivery on PE devices is simplified.
- If you configure SPP in a setup where PBTS is already configured, the PBTS configuration is given preference. If a packet matches the PBTS lookup, the specified forwarding class is used and SPP configuration is ignored.
- SPP extends the concept PBTS by associating a control plane policy with a forwarding class. The route policy is configured to use a forward-class when specific conditions are met
- SPP is supported for interface paths such as Traffic-Engineering Tunnels, RSVP-TE, and Segment Routing Tunnels (SR-TE).

Understanding How Service Path Preference Works

SPP allows services to select a path based on policies configured in the control plane or based on the preferences set in the egress PE node.

Consider a scenario where you have two Provider Edge (PE) routers in a setup. PE1 functions as ingress node and PE2 functions as egress node.

Figure 21: Sample Service Path Preference scenario



The egress PE (PE2) receives the routes from the customers and assigns the routes with prefixes such as BGP community, next hop attribute or vrf attribute. The local policies determine the attribute to be assigned to the customer.

PE1 associates a forward-class to the prefix based on the local policies that are created based on a combination of vrf, address-family, next-hop, and community, to match a forward-class. The pre-configured tunnel with matching forward-class is selected for forwarding the traffic.

Configuring Service Path Preference

Perform this task to configure Service Path Preference:

SUMMARY STEPS

1. **configure**
2. **route-policy** *name*
3. **set forward-class** *range*
4. **end policy**

DETAILED STEPS

Procedure

Step 1 **configure**

Enters global configuration mode.

Example:

```
RP/0/RSP0/CPU0:router(config)#configure
```

Step 2 **route-policy** *name*

Defines a route policy and enters the route-policy configuration mode.

Example:

```
RP/0/RSP0/CPU0:router(config)#route-policy SPP_POLICY
```

Step 3 **set forward-class** *range*

If the community value matches the specified condition, forward class 1 is set.

Note
This task uses community attribute as an example to explain how to configure SPP. In the same manner, you can use vrf, address family, or next hop to configure route policies for SPP.

For details on configuring route policies, see *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration guide*.

Example:

```
RP/0/RSP0/CPU0:router(config-dynamic-template)#type ipsubscriber ipoe_ipv6
```

Step 4 **end policy**

(Optional) Ends the definition of a route policy and exits route policy configuration mode.

Sample Routing Policies to Configure Service Path Preference

The following samples explain how to configure route policies for service path preference:

Configuring a Route Policy to Select a Forward Class that Matches a Specific Community Attribute

```
route-policy  C1
  if community matches-any (6500:1) then
      set forward-class 1
  end-if
end-policy
!
router bgp 55
 bgp router-id 20.0.0.1
 address-family ipv4 unicast
   table-policy C1
  !
!

interface tunnel-te1
   forward-class 1
!
```

In this example, BGP on the receiving PE is configured with a table policy.

The policy logic matches against specific community value (signaled by egress PE) and sets forward-class 1. From the available TE paths, the tunnel with forward-class 1 is selected for forwarding.

Configuring a Route Policy to Select a Forward Class that Matches a Specific VRF

The following example explains how to configure route policies with a VRF attribute and set a forward class.

```
route-policy  C1
      set forward-class 1
end-policy
!
route-policy C2
      set forward-class 2
 end-policy
!

router bgp 55
 bgp router-id 20.0.0.1
 address-family vpnv4 unicast
 !
 vrf one
  rd 1:1
  address-family ipv4 unicast
   table-policy C1
  !
 !
 vrf two
  rd 2:2
  address-family ipv4 unicast
   table-policy C2
  !
 !
!

interface tunnel-te1
   forward-class 1
!
interface tunnel-te2
   forward-class 2
```

```
!
```

In this example, BGP on receiving PE is configured with a table-policy (C1) and (C2) for two different VRFs.

The policy (C1) sets forward-class 1. From the available TE paths, tunnel-te1 with forward-class 1 is selected for forwarding. Similarly for VRF two, traffic tunnel-te2 associated with forward-class 2 is selected for forwarding.

Configuring a Route Policy to Select a Forward Class that Matches an Address Family

The following example explains how to configure route policies with an address family and set a forward class.

```
route-policy  C1
      set forward-class 1
end-policy
!
route-policy C2
     set forward-class 2
!

router bgp 55
 bgp router-id 20.0.0.1
 address-family vpnv4 unicast
    vrf all
       table-policy  C1
   !
 !
 vrf one
  rd 1:1
  address-family ipv4 unicast
  !
 !
 vrf two
  rd 2:2
  address-family ipv4 unicast
  !
 !
!

interface tunnel-te1
   forward-class 1
!
interface tunnel-te2
   forward-class 2
!
```

In this example, BGP on receiving PE is configured with a table-policy (C1) for vpnv4 address family routes. The policy (C1) sets forward-class 1. The vpnv4 prefixes are imported into VRFs and downloaded into RIB/FIB with this forward-class info.

From the available TE paths, forward-class 1 is selected for forwarding.

Configuring a Route Policy to Select a Forward Class that Matches a Next Hop

The following example explains how you can configure route policies with next hop and set a forward class.

```
prefix-set   nh-set-1
  10.10.0.1
end-set

route-policy  C1
  if  next-hop in nh-set-1 then
      set forward-class 1
  end-if
end-policy
!

router bgp 55
 bgp router-id 20.0.0.1
 address-family ipv4 unicast
   table-policy C1
  !

!
interface tunnel-te1
   forward-class 1

!
```

In this example, BGP on receiving PE is configured with a table-policy (C1) on ipv4 unicast address family (AF). The policy (C1) sets forward-class. From the available TE paths, tunnel-te1 with forward-class 1 is selected for forwarding.

Path Protection

Path protection provides an end-to-end failure recovery mechanism (that is, a full path protection) for MPLS-TE tunnels. A secondary Label Switched Path (LSP) is established, in advance, to provide failure protection for the protected LSP that is carrying a tunnel's TE traffic. When there is a failure on the protected LSP, the source router immediately enables the secondary LSP to temporarily carry the tunnel's traffic. If there is a failure on the secondary LSP, the tunnel no longer has path protection until the failure along the secondary path is cleared. Path protection can be used within a single area (OSPF or IS-IS), external BGP [eBGP], and static routes.

The failure detection mechanisms triggers a switchover to a secondary tunnel by:

- Path error or resv-tear from Resource Reservation Protocol (RSVP) signaling
- Notification from the Bidirectional Forwarding Detection (BFD) protocol that a neighbor is lost
- Notification from the Interior Gateway Protocol (IGP) that the adjacency is down
- Local teardown of the protected tunnel's LSP due to preemption in order to signal higher priority LSPs, a Packet over SONET (POS) alarm, online insertion and removal (OIR), and so on

An alternate recovery mechanism is Fast Reroute (FRR), which protects MPLS-TE LSPs only from link and node failures, by locally repairing the LSPs at the point of failure.

Although not as fast as link or node protection, presignaling a secondary LSP is faster than configuring a secondary primary path option, or allowing the tunnel's source router to dynamically recalculate a path. The actual recovery time is topology-dependent, and affected by delay factors such as propagation delay or switch fabric latency.

Related Topics

Enabling Path Protection for an Interface, on page 305
Assigning a Dynamic Path Option to a Tunnel, on page 306
Forcing a Manual Switchover on a Path-Protected Tunnel, on page 307
Configuring the Delay the Tunnel Takes Before Reoptimization, on page 308
Configure Tunnels for Path Protection: Example, on page 396

Pre-requisites for Path Protection

These are the pre-requisites for enabling path protection:

- Ensure that your network supports MPLS-TE, Cisco Express Forwarding, and Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).
- Enable MPLS.
- Configure TE on the routers.
- Configure a TE tunnel with a dynamic path option by using the **path-option** command with the **dynamic** keyword.

Related Topics

Enabling Path Protection for an Interface, on page 305
Assigning a Dynamic Path Option to a Tunnel, on page 306
Forcing a Manual Switchover on a Path-Protected Tunnel, on page 307
Configuring the Delay the Tunnel Takes Before Reoptimization, on page 308
Configure Tunnels for Path Protection: Example, on page 396

Restrictions for Path Protection

- Only Point-to-Point (P2P) tunnels are supported.
- Point-to-Multipoint (P2MP) TE tunnels are not supported.
- A maximum of one standby LSP is supported.
- There can be only one secondary path for each dynamic path option.
- Explicit path option can be configured for the path protected TE with the secondary path option as dynamic.
- A maximum number of path protected tunnel TE heads is 2000.
- A maximum number of TE tunnel heads is equal to 4000.
- When path protection is enabled for a tunnel, and the primary label switched path (LSP) is not assigned a backup tunnel, but the standby LSP is assigned fast-reroute (FRR), the MPLS TE FRR protected value displayed is different from the Cisco express forwarding (CEF) fast-reroute value.

Related Topics

Enabling Path Protection for an Interface, on page 305
Assigning a Dynamic Path Option to a Tunnel, on page 306
Forcing a Manual Switchover on a Path-Protected Tunnel, on page 307
Configuring the Delay the Tunnel Takes Before Reoptimization, on page 308

Configure Tunnels for Path Protection: Example, on page 396

MPLS-TE Automatic Bandwidth

The MPLS-TE automatic bandwidth feature measures the traffic in a tunnel and periodically adjusts the signaled bandwidth for the tunnel.

These topics provide information about MPLS-TE automatic bandwidth:

MPLS-TE Automatic Bandwidth Overview

MPLS-TE automatic bandwidth is configured on individual Label Switched Paths (LSPs) at every head-end. MPLS-TE monitors the traffic rate on a tunnel interface. Periodically, MPLS-TE resizes the bandwidth on the tunnel interface to align it closely with the traffic in the tunnel. MPLS-TE automatic bandwidth can perform these functions:

- Monitors periodic polling of the tunnel output rate
- Resizes the tunnel bandwidth by adjusting the highest rate observed during a given period

For every traffic-engineered tunnel that is configured for an automatic bandwidth, the average output rate is sampled, based on various configurable parameters. Then, the tunnel bandwidth is readjusted automatically based upon either the largest average output rate that was noticed during a certain interval, or a configured maximum bandwidth value.

This table lists the automatic bandwidth functions.

Table 9: Automatic Bandwidth Variables

Function	Command	Description	Default Value
Application frequency	**application** command	Configures how often the tunnel bandwidths changed for each tunnel. The application period is the period of A minutes between the bandwidth applications during which the output rate collection is done.	24 hours
Requested bandwidth	**bw-limit** command	Limits the range of bandwidth within the automatic-bandwidth feature that can request a bandwidth.	0 Kbps
Collection frequency	**auto-bw collect** command	Configures how often the tunnel output rate is polled globally for all tunnels.	5 min
Highest collected bandwidth	—	You cannot configure this value.	—
Delta	—	You cannot configure this value.	—

The output rate on a tunnel is collected at regular intervals that are configured by using the **application** command in MPLS-TE auto bandwidth interface configuration mode. When the application period timer expires, and when the difference between the measured and the current bandwidth exceeds the adjustment

threshold, the tunnel is reoptimized. Then, the bandwidth samples are cleared to record the new largest output rate at the next interval.

When reoptimizing the LSP with the new bandwidth, a new path request is generated. If the new bandwidth is not available, the last good LSP continues to be used. This way, the network experiences no traffic interruptions.

If minimum or maximum bandwidth values are configured for a tunnel, the bandwidth, which the automatic bandwidth signals, stays within these values.



Note When more than 100 tunnels are **auto-bw** enabled, the algorithm will jitter the first application of every tunnel by a maximum of 20% (max 1hour). The algorithm does this to avoid too many tunnels running auto bandwidth applications at the same time.

If a tunnel is shut down, and is later brought again, the adjusted bandwidth is lost and the tunnel is brought back with the initial configured bandwidth. In addition, the application period is reset when the tunnel is brought back.

Related Topics

Configuring the Collection Frequency, on page 309
Configuring the Automatic Bandwidth Functions, on page 311
Configure Automatic Bandwidth: Example, on page 397

Adjustment Threshold

Adjustment Threshold is defined as a percentage of the current tunnel bandwidth and an absolute (minimum) bandwidth. Both thresholds must be fulfilled for the automatic bandwidth to resignal the tunnel. The tunnel bandwidth is resized only if the difference between the largest sample output rate and the current tunnel bandwidth is larger than the adjustment thresholds.

For example, assume that the automatic bandwidth is enabled on a tunnel in which the highest observed bandwidth B is 30 Mbps. Also, assume that the tunnel was initially configured for 45 Mbps. Therefore, the difference is 15 mbit/s. Now, assuming the default adjustment thresholds of 10% and 10kbps, the tunnel is signalled with 30 Mbps when the application timer expires. This is because 10% of 45Mbit/s is 4.5 Mbit/s, which is smaller than 15 Mbit/s. The absolute threshold, which by default is 10kbps, is also crossed.

Overflow Detection

Overflow detection is used if a bandwidth must be resized as soon as an overflow condition is detected, without having to wait for the expiry of an automatic bandwidth application frequency interval.

For overflow detection one configures a limit N, a percentage threshold Y% and optionally, a minimum bandwidth threshold Z. The percentage threshold is defined as the percentage of the actual signalled tunnel bandwidth. When the difference between the measured bandwidth and the actual bandwidth are both larger than Y% and Z threshold, for N consecutive times, then the system triggers an overflow detection.

The bandwidth adjustment by the overflow detection is triggered only by an increase of traffic volume through the tunnel, and not by a decrease in the traffic volume. When you trigger an overflow detection, the automatic bandwidth application interval is reset.

By default, the overflow detection is disabled and needs to be manually configured.

Underflow Detection

Underflow detection is used when the bandwidth on a tunnel drops significantly, which is similar to overflow but in reverse.

Underflow detection applies the highest bandwidth value from the samples which triggered the underflow. For example, if you have an underflow limit of three, and the following samples trigger the underflow for 10 kbps, 20 kbps, and 15 kbps, then, 20 kbps is applied.

Unlike overflow, the underflow count is not reset across an application period. For example, with an underflow limit of three, you can have the first two samples taken at the end of an application period and then the underflow gets triggered by the first sample of the next application period.

Restrictions for MPLS-TE Automatic Bandwidth

When the automatic bandwidth cannot update the tunnel bandwidth, the following restrictions are listed:

- Tunnel is in a fast reroute (FRR) backup, active, or path protect active state. This occurs because of the assumption that protection is a temporary state, and there is no need to reserve the bandwidth on a backup tunnel. You should prevent taking away the bandwidth from other primary or backup tunnels.
- Reoptimization fails to occur during a lockdown. In this case, the automatic bandwidth does not update the bandwidth unless the bandwidth application is manually triggered by using the **mpls traffic-eng auto-bw apply** command in EXEC mode.

Point-to-Multipoint Traffic-Engineering

Point-to-Multipoint Traffic-Engineering Overview

The Point-to-Multipoint (P2MP) Resource Reservation Protocol-Traffic Engineering (RSVP-TE) solution allows service providers to implement IP multicast applications, such as IPTV and real-time video, broadcast over the MPLS label switch network. The RSVP-TE protocol is extended to signal point-to-point (P2P) and P2MP label switched paths (LSPs) across the MPLS networks.

By using RSVP-TE extensions as defined in RFC 4875, multiple subLSPs are signaled for a given TE source. The P2MP tunnel is considered as a set of Source-to-Leaf (S2L) subLSPs that connect the TE source to multiple leaf Provider Edge (PE) nodes.

At the TE source, the ingress point of the P2MP-TE tunnel, IP multicast traffic is encapsulated with a unique MPLS label, which is associated with the P2MP-TE tunnel. The traffic continues to be label-switched in the P2MP tree. If needed, the labeled packet is replicated at branch nodes along the P2MP tree. When the labeled packet reaches the egress leaf (PE) node, the MPLS label is removed and forwarded onto the IP multicast tree across the PE-CE link.

To enable end-to-end IP multicast connectivity, RSVP is used in the MPLS-core for P2MP-TE signaling and PIM is used for PE-CE link signaling.

- All edge routers are running PIM-SSM or Source-Specific Multicast (SSM) to exchange multicast routing information with the directly-connected Customer Edge (CE) routers.
- In the MPLS network, RSVP P2MP-TE replaces PIM as the tree building mechanism, RSVP-TE grafts or prunes a given P2MP tree when the end-points are added or removed in the TE source configuration (explicit user operation).

These are the definitions for Point-to-Multipoint (P2MP) tunnels:

Source

Configures the node in which Label Switched Path (LSP) signaling is initiated.

Mid-point

Specifies the transit node in which LSP signaling is processed (for example, not a source or receiver).

Receiver, Leaf, and Destination

Specifies the node in which LSP signaling ends.

Branch Point

Specifies the node in which packet replication is performed.

Bud Node

Specifies the node that not only acts as a transit for some S2Ls but also acts as a termination point for a S2L of a P2MP TE tunnel.

Source-to-Leaf (S2L) SubLSP

Specifies the P2MP-TE LSP segment that runs from the source to one leaf.

Point-to-Multipoint Traffic-Engineering Features

- P2MP RSVP-TE (RFC 4875) is supported. RFC 4875 is based on nonaggregate signaling; for example, per S2L signaling. Only P2MP LSP is supported.
- **interface tunnel-mte** command identifies the P2MP interface type .
- P2MP tunnel setup is supported with label replication.
- Fast-Reroute (FRR) link protection is supported with sub-50 msec for traffic loss.
- Explicit routing is supported by using under utilized links.
- Reoptimization is supported by calculating a better set of paths to the destination with no traffic loss.



Note Per-S2L reoptimization is not supported.

- IPv4 and IPv6 payloads are supported.
- IPv4 and IPv6 multicast forwarding are supported on a P2MP tunnel interface through a static IGMP and MLD group configuration .
- Both IP multicast and P2MP Label Switch Multicast (LSM) coexist in the same network; therefore, both use the same forwarding plane (LFIB or MPLS Forwarding Infrastructure [MFI]).
- P2MP label replication supports only Source-Specific Multicast (SSM) traffic. SSM configuration supports the default value, none.
- Static mapping for multicast groups to the P2MP-TE tunnel is required .

Point-to-Multipoint Traffic-Engineering Benefits

- Single point of traffic control ensures that signaling and path engineering parameters (for example, protection and diversity) are configured only at the TE source node.
- Ability to configure explicit paths to enable optimized traffic distribution and prevention of single point of failures in the network.
- Link protection of MPLS-labeled traffic traversing branch paths of the P2MP-TE tree.
- Ability to do bandwidth Admission Control (AC) during set up and signaling of P2MP-TE paths in the MPLS network.

Related Topics

Configure Point-to-Multipoint for the Source: Example, on page 413
Configure the Point-to-Multipoint Solution: Example, on page 414
Disable a Destination: Example, on page 414
Configure the Point-to-Multipoint Tunnel: Example, on page 413
Point-to-Multipoint RSVP-TE , on page 234

Point-to-Multipoint RSVP-TE

RSVP-TE signals a P2MP tunnel base that is based on a manual configuration. If all Source-to-Leaf (S2L)s use an explicit path, the P2MP tunnel creates a static tree that follows a predefined path based on a constraint such as a deterministic Label Switched Path (LSP). If the S2L uses a dynamic path, RSVP-TE creates a P2MP tunnel base on the best path in the RSVP-TE topology. RSVP-TE supports bandwidth reservation for constraint-based routing.

When an explicit path option is used, specify both the local and peer IP addresses in the explicit path option, provided the link is a GigabitEthernet or a TenGigE based interface. For point-to-point links like POS or bundle POS, it is sufficient to mention the remote or peer IP address in the explicit path option.

RSVP-TE distributes stream information in which the topology tree does not change often (where the source and receivers are). For example, large scale video distribution between major sites is suitable for a subset of multicast applications. Because multicast traffic is already in the tunnel, the RSVP-TE tree is protected as long as you build a backup path.

Fast-Reroute (FRR) capability is supported for P2MP RSVP-TE by using the unicast link protection. You can choose the type of traffic to go to the backup link.

The P2MP tunnel is applicable for all TE Tunnel destination (IntraArea and InterArea). Inter-AS is not supported.

The P2MP tunnel is signaled by the dynamic and explicit path option in the IGP intra area. Only interArea and interAS, which are used for the P2MP tunnels, are signaled by the verbatim path option.

Related Topics

Configure Point-to-Multipoint for the Source: Example, on page 413
Configure the Point-to-Multipoint Solution: Example, on page 414
Point-to-Multipoint Fast Reroute , on page 234

Point-to-Multipoint Fast Reroute

MPLS-TE Fast Reroute (FRR) is a mechanism to minimize interruption in traffic delivery to a TE Label Switched Path (LSP) destination as a result of link failures. FRR enables temporarily fast switching of LSP

traffic along an alternative backup path around a network failure, until the TE tunnel source signals a new end-to-end LSP.

Both Point-to-Point (P2P) and P2MP-TE support only the Facility FRR method from RFC 4090.

P2P LSPs are used to backup P2MP S2L (source 2 Leaf). Only link and bandwidth protection for P2MP S2Ls are supported. Node protection is not supported.

MPLS-TE link protection relies on the fact that labels for all primary LSPs and subLSPs are using the MPLS global label allocation. For example, one single (global) label space is used for all MPLS-TE enabled physical interfaces on a given MPLS LSP.

Related Topics

Point-to-Multipoint Traffic-Engineering Overview , on page 232
Point-to-Multipoint RSVP-TE , on page 234

Point-to-Multipoint Label Switch Path

The Point-to-Multipoint Label Switch Path (P2MP LSP) has only a single root, which is the Ingress Label Switch Router (LSR). The P2MP LSP is created based on a receiver that is connected to the Egress LSR. The Egress LSR initiates the creation of the tree (for example, tunnel grafting or pruning is done by performing an individual sub-LSP operation) by creating the Forwarding Equivalency Class (FEC) and Opaque Value.



Note Grafting and pruning operate on a per destination basis.

The Opaque Value contains the stream information that uniquely identifies the tree to the root. To receive label switched multicast packets, the Egress Provider Edge (PE) indicates to the upstream router (the next hop closest to the root) which label it uses for the multicast source by applying the label mapping message.

The upstream router does not need to have any knowledge of the source; it needs only the received FEC to identify the correct P2MP LSP. If the upstream router does not have any FEC state, it creates it and installs the assigned downstream outgoing label into the label forwarding table. If the upstream router is not the root of the tree, it must forward the label mapping message to the next hop upstream. This process is repeated hop-by-hop until the root is reached.

By using downstream allocation, the router that wants to receive the multicast traffic assigns the label for it. The label request, which is sent to the upstream router, is similar to an unsolicited label mapping (that is, the upstream does not request it). The upstream router that receives that label mapping uses the specific label to send multicast packets downstream to the receiver. The advantage is that the router, which allocates the labels, does not get into a situation where it has the same label for two different multicast sources. This is because it manages its own label space allocation locally.

Path Option for Point-to-Multipoint RSVP-TE

P2MP tunnels are signaled by using the dynamic and explicit path-options in an IGP intra area. InterArea cases for P2MP tunnels are signaled by the verbatim path option.

Path options for P2MP tunnels are individually configured for each sub-LSP. Only one path option per sub-LSP (destination) is allowed. You can choose whether the corresponding sub-LSP is dynamically or explicitly routed. For the explicit option, you can configure the verbatim path option to bypass the topology database lookup and verification for the specified destination.

Both dynamic and explicit path options are supported on a per destination basis by using the **path-option (P2MP-TE)** command. In addition, you can combine both path options.

Explicit Path Option

Configures the intermediate hops that are traversed by a sub-LSP going from the TE source to the egress MPLS node. Although an explicit path configuration enables granular control sub-LSP paths in an MPLS network, multiple explicit paths are configured for specific network topologies with a limited number of (equal cost) links or paths.

Dynamic Path Option

Computes the IGP path of a P2MP tree sub-LSP that is based on the OSPF and ISIS algorithm. The TE source is dynamically calculated based on the IGP topology.



Note Dynamic path option can only compute fully-diverse standby paths. While, explicit path option supports partially diverse standby paths as well.

Dynamic Path Calculation Requirements

Dynamic path calculation for each sub-LSP uses the same path parameters as those for the path calculation of regular point-to-point TE tunnels. As part of the sub-LSP path calculation, the link resource (bandwidth) is included, which is flooded throughout the MPLS network through the existing RSVP-TE extensions to OSPF and ISIS. Instead of dynamic calculated paths, explicit paths are also configured for one or more sub-LSPs that are associated with the P2MP-TE tunnel.

- OSPF or ISIS are used for each destination.
- TE topology and tunnel constraints are used to input the path calculation.
- Tunnel constraints such as affinity, bandwidth, and priorities are used for all destinations in a tunnel.
- Path calculation yields an explicit route to each destination.

Static Path Calculation Requirements

The static path calculation does not require any new extensions to IGP to advertise link availability.

- Explicit path is required for every destination.
- Offline path calculation is used.
- TE topology database is not needed.
- If the topology changes, reoptimization is not required.

Related Topics

Configure the Point-to-Multipoint Tunnel: Example, on page 413
Configure the Point-to-Multipoint Solution: Example, on page 414
Point-to-Multipoint Traffic-Engineering Overview , on page 232
Point-to-Multipoint RSVP-TE , on page 234

Point-to-Multipoint Implicit Null

The Point-to-Multipoint (P2MP) implicit null feature enables the forwarding of unicast traffic over P2MP tunnels. This feature is enabled by default and requires no configuration.

In a P2MP tunnel, the tailend router signals the implicit null label to the midpoint router. If the given MPI leg of the P2MP tunnel is implicit null capable (where the penultimate router is capable to do penultimate hop popping), the FIB (Forwarding Information Base) creates two NRLDI (Non Recursive Load Distribution Index) entries, one for forwarding the IPv6 labeled packets, and the other for non-labeled IPv4 unicast traffic.

The headend and the tailend routers handle the unicast traffic arriving on the P2MP tunnel. The midpoint router forwards the unicast traffic to its bud and tailend routers.

The use of implicit null at the end of a tunnel is called penultimate hop popping (PHP). The FIB entry for the tunnel on the PHP router shows a "pop label" as the outgoing label.

In some cases, it could be that the packets have two or three or more labels in the label stack. Then the implicit null label used at the tailend router would signal the penultimate hop router to pop one label and send the labeled packet with one label less to the tailend router. Then the tailend router does not have to perform two label lookups. The use of the implicit null label does not mean that all labels of the label stack must be removed; only one label is "popped" off (remove the top label on the stack). In any case, the use of the implicit null label prevents the tailend router from performing two lookups.

Restriction

The P2MP implicit null feature may cause multicast traffic drop with implicit null label on the tailend routers. This is because the P2MP implicit null feature does not support forwarding of multicast traffic when no label is received on the tailend router.

MPLS Traffic Engineering Shared Risk Link Groups

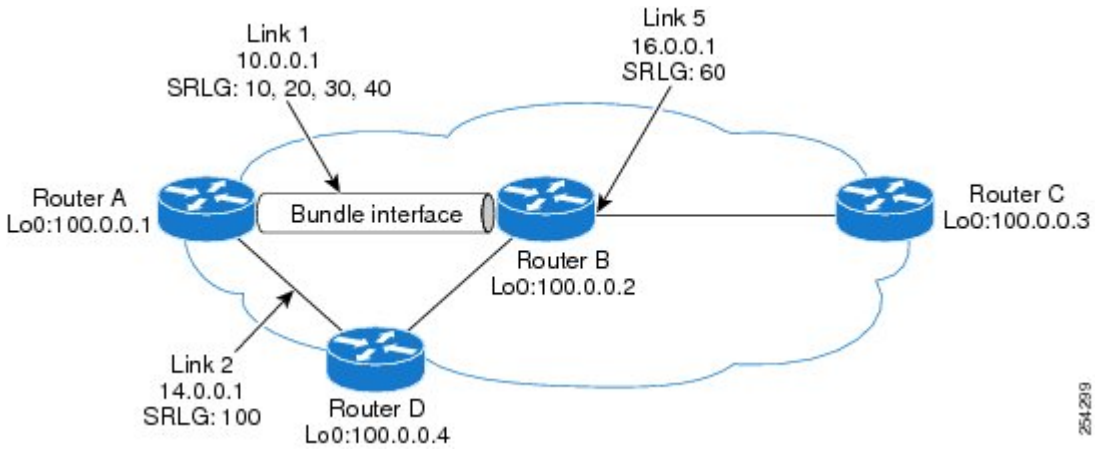
Shared Risk Link Groups (SRLG) in MPLS traffic engineering refer to situations in which links in a network share a common fiber (or a common physical attribute). These links have a shared risk, and that is when one link fails, other links in the group might fail too.

OSPF and Intermediate System-to-Intermediate System (IS-IS) flood the SRLG value information (including other TE link attributes such as bandwidth availability and affinity) using a sub-type length value (sub-TLV), so that all routers in the network have the SRLG information for each link.

To activate the SRLG feature, configure the SRLG value of each link that has a shared risk with another link. A maximum of 30 SRLGs per interface is allowed. You can configure this feature on multiple interfaces including the bundle interface.

Figure illustrates the MPLS TE SRLG values configured on the bundle interface.

Figure 22: Shared Risk Link Group



Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Explicit Path

The Explicit Path configuration allows you to configure the explicit path. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

The MPLS Traffic Engineering (TE)—IP Explicit Address Exclusion feature provides a means to exclude a link or node from the path for an Multiprotocol Label Switching (MPLS) TE label-switched path (LSP).

This feature is enabled through the **explicit-path** command that allows you to create an IP explicit path and enter a configuration submode for specifying the path. The feature adds to the submode commands of the **exclude-address** command for specifying addresses to exclude from the path.

The feature also adds to the submode commands of the **exclude-srlg** command that allows you to specify the IP address to get SRLGs to be excluded from the explicit path.

If the excluded address or excluded srlg for an MPLS TE LSP identifies a flooded link, the constraint-based shortest path first (CSPF) routing algorithm does not consider that link when computing paths for the LSP. If the excluded address specifies a flooded MPLS TE router ID, the CSPF routing algorithm does not allow paths for the LSP to traverse the node identified by the router ID.

Related Topics

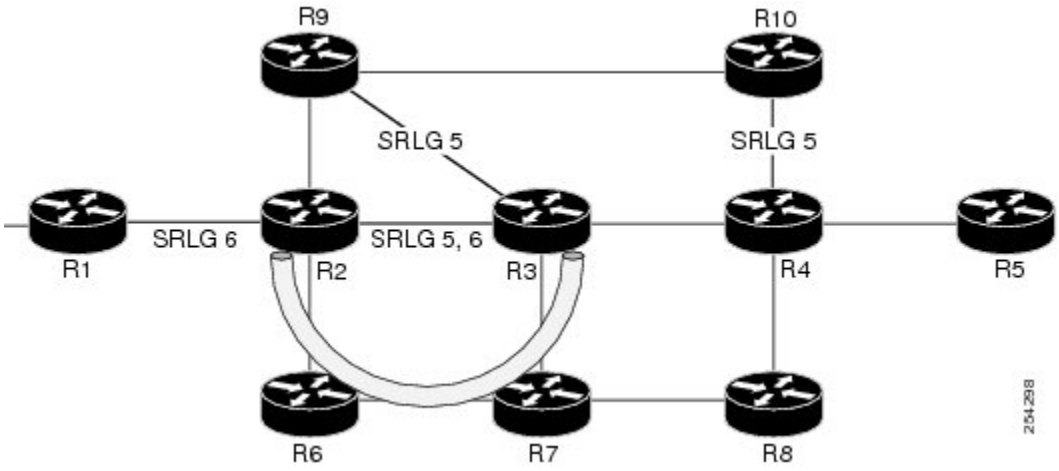
Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Fast ReRoute with SRLG Constraints

Fast ReRoute (FRR) protects MPLS TE Label Switch Paths (LSPs) from link and node failures by locally repairing the LSPs at the point of failure. This protection allows data to continue to flow on LSPs, while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

Backup tunnels that bypass only a single link of the LSP's path provide Link Protection. They protect LSPs by specifying the protected link IP addresses to extract SRLG values that are to be excluded from the explicit path, thereby bypassing the failed link. These are referred to as **next-hop (NHOP) backup tunnels** because they terminate at the LSP's next hop beyond the point of failure. Figure 1 illustrates an NHOP backup tunnel.

Figure 23: NHOP Backup Tunnel with SRLG constraint

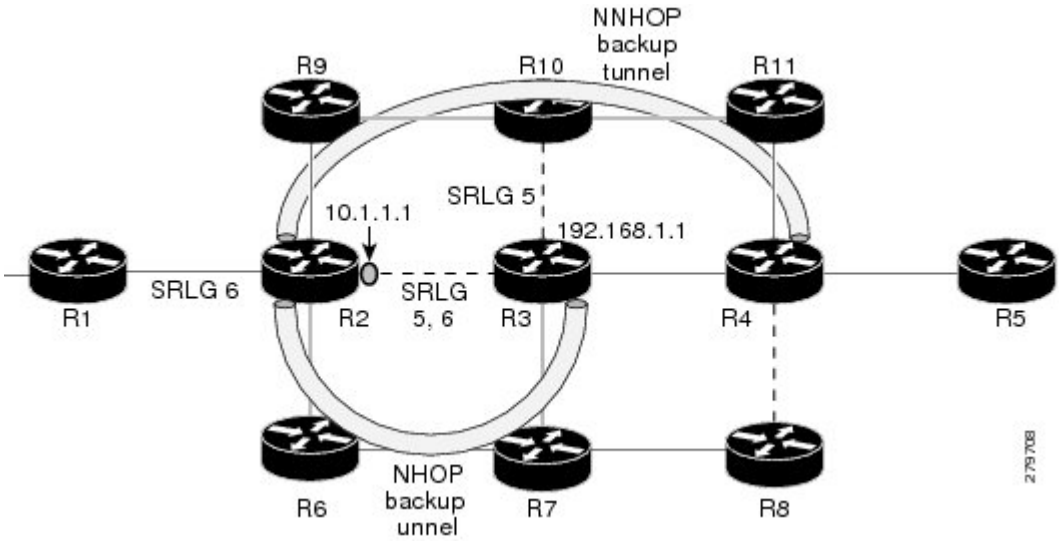


In the topology shown in the above figure, the backup tunnel path computation can be performed in this manner:

- Get all SRLG values from the exclude-SRLG link (SRLG values 5 and 6)
- Mark all the links with the same SRLG value to be excluded from SPF
- Path computation as CSPF R2->R6->R7->R3

FRR provides Node Protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called **NNHOP backup tunnels** because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs when a node along their path fails, by enabling the node upstream to the point of failure to reroute the LSPs and their traffic, around the failed node to the next-next hop. They also protect LSPs by specifying the protected link IP addresses that are to be excluded from the explicit path, and the SRLG values associated with the IP addresses excluded from the explicit path. NNHOP backup tunnels also provide protection from link failures by bypassing the failed link as well as the node. Figure 2 illustrates an NNHOP backup tunnel.

Figure 24: NNHOP Backup Tunnel with SRLG constraint



In the topology shown in the above figure, the backup tunnel path computation can be performed in this manner:

- Get all SRLG values from the exclude-SRLG link (SRLG values 5 and 6)
- Mark all links with the same SRLG value to be excluded from SPF
- Verify path with SRLG constraint
- Path computation as CSPF R2->R9->R10->R4

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Importance of Protection

This section describes the following:

- Delivery of Packets During a Failure
- Multiple Backup Tunnels Protecting the Same Interface

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321

Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Delivery of Packets During a Failure

Backup tunnels that terminate at the NNHOP protect both the downstream link and node. This provides protection for link and node failures.

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Multiple Backup Tunnels Protecting the Same Interface

- Redundancy—If one backup tunnel is down, other backup tunnels protect LSPs.
- Increased backup capacity—If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link falls over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels).

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Weighted-SRLG Auto-backup Path Computation

In shared-risk link groups (SRLG) fate-sharing, links are assigned one or more numbers to represent risks. When two links are assigned a common number then this indicates that these two links are sharing fate. In the weighted-SRLG auto-backup path computation mode, the links that share SRLG numbers with the protected link are not excluded from the topology. The admin-weight of these links is set to reflect the sharing of SRLG with the protected link. Setting the admin weight consists of adding a penalty metric to make using the link less desirable.

For more information about Weighted-SRLG auto-backup path computation, see *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information about Weighted-SRLG auto-backup path computation, see *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318

Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

SRLG Limitations

There are few limitations to the configured SRLG feature:

- The **exclude-address** and **exclude-srlg** options are not allowed in the IP **explicit path strict-address** network.
- Whenever SRLG values are modified after tunnels are signalled, they are verified dynamically in the next path verification cycle.

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

MPLS TE SRLG Scale Enhancements

MPLS Traffic Engineering Shared Risk Link Groups (SRLG) feature has been enhanced to support:

- Increase from 32 to 64 (59 for ISIS) groups.
- Increase from 250 to 500 interfaces.

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Soft-Preemption

MPLS-TE preemption consists of freeing the resources of an established LSP, and assigning them to a new LSP. The freeing of resources causes a traffic disruption to the LSP that is being preempted. Soft preemption is an extension to the RSVP-TE protocol to minimize and even eliminate such traffic disruption over the preempted LSP.

The soft-preemption feature attempts to preempt the LSPs in a graceful manner to minimize or eliminate traffic loss. However, the link might be over-subscribed for a period of time.

In a network that implements soft preemption, zero traffic loss is achieved in this manner:

- When signaling a new LSP, the ingress router indicates to all the intermediate nodes that the existing LSP is to be softly preempted, in case its resources are needed and is to be reassigned.

- When a given intermediate node needs to soft-preempt the existing LSP, it sends a new or special path error (preemption pending) to the ingress router. The intermediate node does not dismantle the LSP and maintains its state.
- When the ingress router receives the path error (preemption pending) from the intermediate node, it immediately starts a re-optimization that avoids the link that caused the preemption.
- When the re-optimization is complete, the ingress router tears down the soft-preempted LSP.

Related Topics

Enabling Soft-Preemption on a Node, on page 335
Enabling Soft-Preemption on a Tunnel, on page 336

Path Option Attributes

The path option attributes are configurable through a template configuration. This template, named **attribute-set**, is configured globally in the MPLS traffic-engineering mode.

You can apply an **attribute-set** to a path option on a per-LSP basis. The path option configuration is extended to take a path option attribute name. LSPs computed with a particular path option uses the attributes as specified by the attribute-set under that path option.

These prerequisites are required to implement path option attributes:

- Path option type attribute-set is configured in the MPLS TE mode
- Path option CLI extended to accept an attribute-set name

Note The **signalled-bandwidth** and **affinity** attributes are supported under the attribute-set template.

Related Topics

Configuring Attributes within a Path-Option Attribute, on page 337

Configuration Hierarchy of Path Option Attributes

You can specify a value for an attribute within a path option **attribute-set** template. This does not prevent the configuring of the same attribute at a tunnel level. However, it is important to note that only one level is taken into account. So, the configuration at the LSP level is considered more specific than the one at the level of the tunnel, and it is used from this point onwards.

Attributes that are not specified within an attribute-set take their values as usual--configuration at the tunnel level, configuration at the global MPLS level, or default values. Here is an example:

```
attribute-set path-option MYSET
   affinity 0xBEEF mask 0xBEEF

interface tunnel-te 10
   affinity 0xCAFE mask 0xCAFE
   signalled-bandwidth 1000
   path-option 1 dynamic attribute-set name MYSET
   path-option 2 dynamic
```

In this example, the attribute-set named **MYSET** is specifying affinity as 0xBEEF. The signalled bandwidth has not been configured in this **MYSET**. The **tunnel 10**, meanwhile, has affinity 0xCAFE configured. LSPs computed from path-option 1 uses the affinity 0xBEEF/0xBEEF, while LSPs computed from path-option 2 uses the affinity 0xCAFE/0xCAFE. All LSPs computed using any of these path-options use **signalled-bandwidth** as 1000, as this is the only value that is specified only at the tunnel level.

Note The attributes configured in a path option **attribute-set** template takes precedence over the same attribute configured under a tunnel. An attribute configured under a tunnel is used only if the equivalent attribute is **not** specified by the in-use path option **attribute-set** template.

Related Topics

Configuring Attributes within a Path-Option Attribute, on page 337

Traffic Engineering Bandwidth and Bandwidth Pools

MPLS traffic engineering allows constraint-based routing (CBR) of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Regular TE tunnel bandwidth is called the **global pool**. The **subpool bandwidth** is a portion of the global pool. If it is not in use, the subpool bandwidth is not reserved from the global pool. Therefore, subpool tunnels require a priority higher than that of non-subpool tunnels.

You can configure the signalled-bandwidth path option attribute to use either the global pool (default) or the subpool bandwidth. The signalled-bandwidth value for the path option may be any valid value and the pool does not have to be the same as that which is configured on the tunnel.

Note When you configure signalled-bandwidth for path options with the **signalled-bandwidth bandwidth [sub-pool | global]** *kbps* command, use either all subpool bandwidths or all global-pool bandwidth values.

Related Topics

Configuring Attributes within a Path-Option Attribute, on page 337

Path Option Switchover

Reoptimization to a particular path option is not possible if the in-use path option and the new path option do not share the same bandwidth class. The path option switchover operation would fail in such a scenario. Use this command at the EXEC configuration mode to switchover to a newer path option :

```
mpls traffic-eng switchover tunnel-xx ID path-option index
```

The switchover to a newer path option is achieved, in these instances:

- when a lower index path option is available
- when any signalling message or topology update causes the primary LSP to go down
- when a local interface fails on the primary LSP or a path error is received on the primary LSP

Note Path option switchover between various path options with different bandwidth classes is not allowed.

Related Topics

Configuring Attributes within a Path-Option Attribute, on page 337

Path Option and Path Protection

When path-protection is enabled, a standby LSP is established to protect traffic going over the tunnel. The standby LSP may be established using either the same path option as the primary LSP, or a different one.

The standby LSP is computed to be diverse from the primary LSP, so bandwidth class differences does not matter. This is true in all cases of diversity except node-diversity. With node diversity, it is possible for the standby LSP to share up to two links with the primary LSP, the link exiting the head node, and the link entering the tail node.

If you want to switchover from one path option to another path option and these path options have different classes, the path option switchover is rejected. However, the path option switchover can not be blocked in the path-protection feature. When the standby LSP becomes active using another path option of a different class type, the path option switchover cannot be rejected at the head end. It might get rejected by the downstream node.

Node-diversity is only possible under limited conditions. The conditions that must be met are:

- there is no second path that is both node and link diverse
- the current LSP uses a shared-media link at the head egress or tail ingress
- the shared-media link used by the current LSP permits computation of a node-diverse path

In Cisco IOS XR, reoptimization between different class types would actually be rejected by the next hop. This rejection will occur by an admission failure.

Related Topics

Configuring Attributes within a Path-Option Attribute, on page 337

Auto-Tunnel Mesh

The MPLS traffic engineering auto-tunnel mesh (Auto-mesh) feature allows you to set up full mesh of TE P2P tunnels automatically with a minimal set of MPLS traffic engineering configurations. You may configure one or more mesh-groups. Each mesh-group requires a destination-list (IPv4 prefix-list) listing destinations, which are used as destinations for creating tunnels for that mesh-group.

You may configure MPLS TE auto-mesh type attribute-sets (templates) and associate them to mesh-groups. LSR creates tunnels using the tunnel properties defined in the attribute-set.

Auto-Tunnel mesh provides benefits:

- Minimizes the initial configuration of the network.

  You may configure tunnel properties template and mesh-groups or destination-lists on each TE LSRs that further creates full mesh of TE tunnels between those LSRs.

- Minimizes future configurations resulting due to network growth.

It eliminates the need to reconfigure each existing TE LSR in order to establish a full mesh of TE tunnels whenever a new TE LSR is added in the network.

Related Topics

Configuring Auto-Tunnel Mesh Tunnel ID, on page 338
Configuring Auto-tunnel Mesh Unused Timeout, on page 339
Configuring Auto-Tunnel Mesh Group, on page 340
Configuring Tunnel Attribute-Set Templates, on page 342
Enabling LDP on Auto-Tunnel Mesh, on page 343

Destination List (Prefix-List)

Auto-mesh tunnels can be automatically created using prefix-list. Each TE enabled router in the network learns about the TE router IDs through a existing IGP extension.

You can view the router IDs on the router using this command:

```
show mpls traffic-eng topology | include TE Id
IGP Id: 0001.0000.0010.00, MPLS TE Id:10.1.1.1 Router Node  (ISIS 1 level-2)
IGP Id: 0001.0000.0011.00, MPLS TE Id:10.2.2.2 Router Node  (ISIS 1 level-2)
IGP Id: 0001.0000.0012.00, MPLS TE Id:10.3.3.3 Router Node  (ISIS 1 level-2)
```

A prefix-list may be configured on each TE router to match a desired set of router IDs (MPLS TE ID as shown in the above output). For example, if a prefix-list is configured to match addresses of 10.0.0.0 with wildcard 0.255.255.255, then all 10.x.x.x router IDs are included in the auto-mesh group.

When a new TE router is added in the network and its router ID is also in the block of addresses described by the prefix-list, for example, 10.x.x.x, then it is added in the auto-mesh group on each existing TE router without having to explicitly modify the prefix-list or perform any additional configuration.

Auto-mesh does not create tunnels to its own (local) TE router IDs.

Note When prefix-list configurations on all routers are not identical, it can result in non- symmetrical mesh of tunnels between those routers.

Related Topics

Configuring Auto-Tunnel Mesh Tunnel ID, on page 338
Configuring Auto-tunnel Mesh Unused Timeout, on page 339
Configuring Auto-Tunnel Mesh Group, on page 340
Configuring Tunnel Attribute-Set Templates, on page 342
Enabling LDP on Auto-Tunnel Mesh, on page 343

P2MP-TE Auto-tunnels

The MPLS point-to-multi point traffic-engineering auto-tunnels (P2MP-TE Auto-tunnels) feature enables dynamic creation and management of P2MP auto-tunnels for the transport of VPLS traffic on Cisco IOS XR Software. The P2MP-TE auto-tunnel configuration is disabled by default. Use the **auto-tunnel p2mp-te tunnel-id** configuration to enable P2MP-TE Auto-tunnel. This configures the tunnel ID range that can be

allocated to P2MP auto-tunnels. This also determines the maximum number of P2MP auto-tunnels that can be created.

For more information on P2MP_TE Auto-tunnels, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on Set DF Bit commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Related Topics

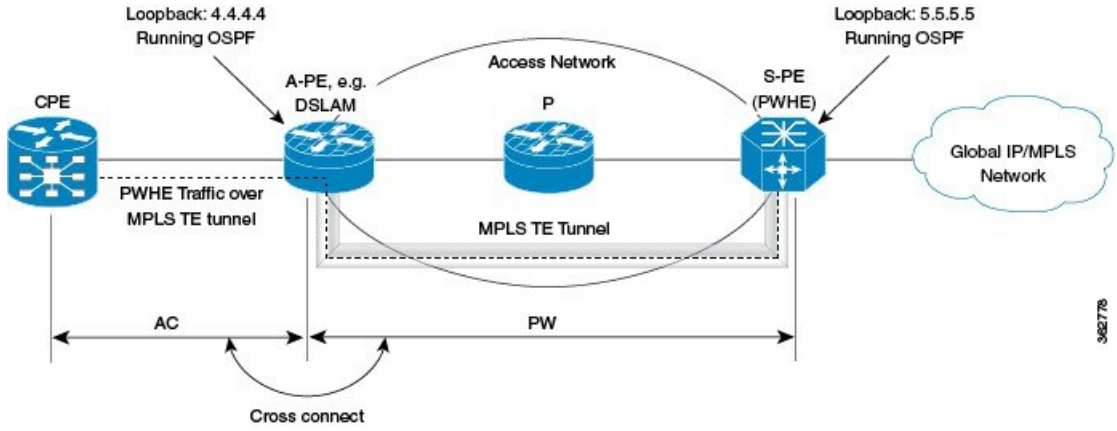
Configuring P2MP TE Auto-tunnels, on page 344

PWHE over MPLS TE Tunnels

The Pseudowire Headend (PWHE) over MPLS TE Tunnels feature enables the PWHE traffic to pass through MPLS traffic engineering (TE) tunnels.

The PWHE and the MPLS TE tunnels are configured independently. No specific configuration is required for a TE tunnel to forward PWHE traffic through it. The pseudowire traffic automatically passes through the TE tunnel, after the routing protocol is configured in such a way that the routing algorithm considers the TE tunnel as the route to reach the pseudowire endpoint.

Figure 25: PWHE over MPLS TE Tunnel



In this figure, S-PE is the PWHE and OSPF manages the routing. A MPLS TE tunnel is configured between A-PE and S-PE. After the MPLS TE tunnel is defined (either by defining a static route or using the **autoroute announce** command) as the path through which to forward traffic to S-PE, the PWHE traffic passes through that tunnel.

Workflow - Sending PWHE Traffic over MPLS TE Tunnels

Complete these configurations on the S-PE to enable PWHE traffic to flow through the MPLS TE tunnel.

Task Number	Task Description	Sample Configuration	Details

1	Configure interfaces that connect to A-PE.	`interface Bundle-Ether1`
		` description TO-APE`
		` ipv4 address 145.0.2.5 255.255.255.0`
		` load-interval 30`
		`!`
		`interface TenGigE0/2/1/2`
		` description TO-APE-VKG4-0-1-1-0`
		` bundle id 1 mode on`
		` load-interval 30`
		`!`
		`interface TenGigE0/2/1/3`
		` description TO-APE-VKG4-0-1-1-1`
		` bundle id 1 mode on`
		` load-interval 30`
			See the *Configuring Ethernet Link Bundles* task in Chapter *Configuring Link Bundling* of *Interface and Hardware Component Configuration Guide for Cisco ASR 9000 Series Routers*.
			Note You can configure any supported interface; not just bundle interfaces.

2	Define loopback address.	`interface Loopback0`
		` ipv4 address 5.5.5.5 255.255.255.255`
		`!`	

3	Configure tunnel interface.
	TE tunnels can be configured with either an "explicit" or a "dynamic" path.
		`interface tunnel-te1`
		` bandwidth 10000000`
		` ipv4 unnumbered Loopback0`
		` autoroute announce`
		` destination 4.4.4.4`
		` fast-reroute`
		` path-option 10 explicit name main-path`
		`!`
			See Creating an MPLS-TE Tunnel, on page 262

4	Provide path definition of path that the tunnel uses as the forwarding path.	`explicit-path name main-path`
		` index 10 next-address strict ipv4 unicast 145.0.2.4`
		`!`
			See Configuring Explicit Paths with ABRs Configured as Loose Addresses, on page 296

5	Specify tunnel bandwidth.	`rsvp`
		` interface Bundle-Ether1`
		`  bandwidth mam max-reservable-bw 10000000 1000000`
		`  !`
		` signalling graceful-restart`
		`!`
		`mpls traffic-eng`
		` interface Bundle-Ether1`
		`!`
			See Configuring an IETF DS-TE Tunnel Using MAM, on page 285

Task Number	Task Description	Sample Configuration	Details

6	Configure PWHE.	`interface PW-Ether1`
		` mtu 1518`
		` mac-address 4000.5.1`
		` load-interval 30`
		` attach generic-interface-list il1`
		`!`
			See the *Configuring PWHE Interfaces* task in Chapter *Implementing Multipoint Layer 2 Services* of *L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers*.

7	Define, for PWHE, the list of interfaces that PW uses to forward traffic.	`generic-interface-list il1`
		` interface Bundle-Ether1`
		`!`
			See the *Configuring Generic Interface List* task in Chapter *Implementing Multipoint Layer 2 Services* of *L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers*.

8	Define PW source address.	`l2vpn`
		` pw-class pwhe`
		`  encapsulation mpls`
		`  control-word`
		`  ipv4 source 5.5.5.5`
		`  !`
		` !`
			See the *Configuring the Source Address* task in Chapter *Implementing Multipoint Layer 2 Services* of *L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers*.

9	Define PWHE cross-connect.	`xconnect group xc452`
		`  p2p pwhe452`
		`  interface PW-Ether2`
		`  neighbor ipv4 4.4.4.4 pw-id 452`
		`  mpls static label local 5542 remote 5452`
		`  pw-class pwhe`
		`  !`
			See the *Configuring PWHE Crossconnect* task in Chapter *Implementing Multipoint Layer 2 Services* of *L2VPN and Ethernet Services Configuration Guide for Cisco ASR 9000 Series Routers*.

10	Setup interfaces running LDP.	`mpls ldp`
		` nsr`
		` graceful-restart`
		` graceful-restart reconnect-timeout 60`
		` graceful-restart forwarding-state-holdtime 60`
		` interface Bundle-Ether1`
		` !`
		`!`
			See Setting Up LDP NSF Using Graceful Restart, on page 54

Task Number	Task Description	Sample Configuration	Details

11	Configure routing.	`router ospf 100`
		` nsr`
		` router-id 5.5.5.5`
		` nsf cisco`
		` area 0`
		`  mpls traffic-eng`
		`  interface Bundle-Ether1`
		`  !`
		`  interface Loopback0`
		`  !`
		`mpls traffic-eng router-id 192.168.70.1`
		`!`
			See the *Configuring OSPF Version 2 for MPLS Traffic Engineering* task in Chapter *Implementing OSPF* of *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Note A-PE has a similar configuration, except for the fact that there is no PWHE defined on it.

In a PWHE-based pseudowire configuration, the TE tunnel cannot be configured as the preferred-path for pseudowire traffic. Therefore, the preferred-path tunnel-te option under the L2VPN XConnect PW-Class is not supported. However, the TE tunnel redundancy and TE fast-reroute mechanisms are supported with PWHE over MPLS TE tunnels.

VRF Redirection to MPLS TE Tunnels

The VRF redirection to MPLS TE tunnels feature adds automatic route MPLS TE tunnels through autoroute destination configuration. The VRF redirection to MPLS TE tunnels maps VRF prefixes over TE tunnels in the core to reach the same egress provider edge (PE). This enables to load-balance prefix traffic on multiple tunnels based on equal cost multi-path (ECMP). The ECMP is used to load-share the flow(s) on multiple available paths towards the destination PE. The route added by autoroute destination inherits the same IGP computed metric to the tunnel endpoint. Any changes to the IGP route metric to the tunnel endpoint is automatically reflected on the autoroute destination route too.

In a typical VPN deployment over a TE core network, an operator creates a mesh of TE tunnels between PE routers and then configures autoroute announce to these tunnels. This leads to a mix of default VRF and VPNv4 traffic on the same tunnel connecting the PE routers. An operator my want to segregate their VPNv4 traffic on different tunnels. This can be achieved by creating multiple tunnels to the egress PE(s). The limitation of this approach is that the static routes are added with zero metrics. The VRF Redirection to MPLS TE Tunnels feature is a solution to resolve this limitation. Multiple VRFs can be mapped on the same tunnel by adding multiple autoroute destination addresses (BGP next-hops) to the same tunnel.

Routes added by static route are always added with zero cost metric. This results in traffic that is mapped on multiple tunnels to always load-balance due to ECMP. This may be undesirable when some of those tunnels have sub-optimal paths (have higher underlying cost to the endpoint). With autoroute destination, only the tunnel whose IGP cost to its endpoint is lowest will be considered for carrying traffic.

VRF redirection over TE tunnels feature supports:

- Automatic redirection of VRF traffic over TE tunnels.

- Multiple autoroute destinations under one tunnel to aggregate VRF traffic. If two VRFs are to be mapped on same tunnel, then two autoroute destination prefixes (BGP next-hops) will be configured under the tunnel.
- One autoroute destination under multiple tunnels to enable ECMP load-balance of VRF traffic.
- Implicit /32 mask for each route. Only host addresses residing on the tunnel endpoint are supported.
- High availability, RP failover, and non-stop forwarding (NSF) scenarios by proving hitless to traffic mechanisms.



Note Configuring Segment Routing and Autoroute Destination together is not supported. If autoroute functionality is required in an Segment Routing network, we recommend you to configure Autoroute Announce.

For more information on VRF Redirection to MPLS TE Tunnels, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on VRF Redirection to MPLS TE Tunnels commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

MPLS TE Extended Admin Groups

The MPLS TE extended admin groups (EAG) configuration assigns EAG/AG name to bit-position and associates affinity-names with TE links. The configuration extends to assign names, up to 256, to TE links over the selected interface and assigns 32 names per attribute-set and index.

For more information on MPLS TE Extended Admin Groups, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on MPLS TE Extended Admin Groups commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Stateful Path Computation Element

The stateful path computation element (PCE) describes a set of procedures by which a path computation client (PCC) can report and delegate control of head-end tunnels sourced from the PCC to a PCE peer. The PCE peer can request the PCC to update and modify parameters of label switched paths (LSPs) it controls. The stateful model also enables a PCC to allow the PCE to initiate computations allowing the PCE to perform network-wide orchestration.

For more information on Stateful PCE, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on Stateful PCE commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

- Request types
  - PCReq—requests used by current stateless PCE implementation
  - PCCreate—LSP instantiation requests
  - PCUpd—LSP update requests

- LSP Objects
  - Operational flag
  - Delegation flag
  - Remove flag
  - Symbolic path name
  - LSP Identifiers
- Path List
  - ERO

Stateful PCE State Reporting

State reporting refers to the PCC sending information to PCEs about the state of LSPs. This is done as state changes occur and is used to keep PCEs informed of changes to the LSP as they occur. State reporting is also used as part of *state synchronization* and *delegation*.

A state report is a message sent by a PCC to a PCE reporting on the state of one or more TE tunnels. This allows the PCE to stay abreast of changes as they occur. Reports are triggered when the PCE needs to be informed of state. These occur when:

- State synchronization happens
- The PCC attempts to delegate control of a tunnel to a PCE
- The PCC revokes control of a tunnel from a PCE
- The PCC deletes a tunnel
- A signalling error occurs on a tunnel
- Reportable information about a tunnel changes

Stateful PCE State Synchronization

Synchronization refers to a procedure that occurs after a PCEP session is established between a PCE and a PCC. The purpose of state synchronization is to download the current LSP database of the PCC to a PCE. This is done through a set of state reports which are marked as *synchronizations*. This is the first communication to occur after the session is brought up. A full re-send of state reports can also be avoided when the PCE already has an up-to-date version of the LSP database as the version number can be indicated by the PCE during PCEP session establishment.

Stateful PCE Delegation

Delegation is the action by which control of a state is granted to a PCE by the PCC. A PCE to which control was delegated can alter attributes of the LSP. Control is only delegated to one PCE at a time.

- Delegation of control can be revoked from a PCE by the PCC.
- Delegation of control can also be returned to the PCC by the PCE.

Stateful PCE State Updating

State updating refers to the PCE sending information to a PCC to alter the attributes of an LSP. A state update is a message sent by a PCE to a PCC to alter the state of one or more TE tunnels. State updating is allowed only if the PCE has previously been delegated control of the LSP. State updating is also used to return delegated control.

Stateful PCE Creation of LSPs

Creation (or instantiation) of an LSP is a procedure by which a PCE instructs a PCC to create an LSP respecting certain attributes. For LSPs created in this manner, the PCE is delegated control automatically. Stateful PCE procedures enable a PCE to instruct a PCC to create a locally sourced tunnel.

Delegation of PCC Initiated Tunnels

The delegation of path computation client (PCC) initiated tunnels feature enables the ability to control PCC initiated tunnels through stateful path computation element (PCE).

When a PCC is connected to multiple PCEs, use the **precedence** command to select stateful PCEs for delegating LSPs. Precedence can take any value between 0 and 255. The default precedence value is 255. When there are multiple stateful PCEs with active PCEP sessions, PCC selects the PCE with the lowest precedence value. If multiple PCEs have the same precedence, PCC selects a PCE with the lowest IP address. A PCC considers only the PCEs with active PCEP session for delegating LSPs.

When a PCEP session over which tunnels have been delegated is terminated, the PCC waits till the re-delegation timer expires before re-delegating tunnels. If a PCEP session comes back up within re-delegation timer expiration, tunnels will be delegated back to the same PCE.

For information on PCC, see Path Computation Element, on page 218.

Stateful PCE Enhancements

These topics describe the enhancements made to the stateful path computation element (PCE):

Fast Repair

Fast repair feature minimizes the tunnel down time by allowing the path computation client (headend) to determine a new optimal path for delegated tunnels that went down, or are under fast reroute (FRR) or soft-preemption. Previously, Path Computation Client (PCC) was not designated to take any action on delegated tunnels. To configure the fast repair feature, use the **fast-repair** command under PCE stateful client in MPLS-TE configuration.

PCE is still the primary controller, but the time taken to notify the PCE and the wait till the PCE takes an action, amounts to considerable time. This disadvantage is overcome by the fast repair feature.

Automatic Bandwidth Backoff

Automatic bandwidth backoff is enabled automatically, if the tunnel's current bandwidth is different from the requested bandwidth due to automatic bandwidth update.

In cases where automatic bandwidth is enabled for a tunnel, fast repair tries to determine a path with:

1. Current signaled bandwidth

2. If option (1) fails and the configured bandwidth has a lower value than the current bandwidth, second attempt is made with the average bandwidth value: (current bandwidth + configured bandwidth)/2

Note If configured bandwidth is equal to or higher than the current bandwidth, fast repair fails at this point.

3. If option (2) fails, PCC tries to find a path with the configured bandwidth value
4. If option (3) fails, fast repair is unsuccessful and the tunnel is at the discretion of the PCE

For detailed configuration steps, see Configuring Fast Repair, on page 301.

Optional Vendor Specific PCEP Extension

An optional vendor specific Path Computation Element Protocol (PCEP) extension, *cisco-tlv* is added in this IOS XR release. The vendor information TLV (Type-Length-Variable) is used to carry vendor specific information that applies to a specific PCEP object by including the TLV in the object.

Vendor specific PCEP extension (cisco-tlv) in not sent in PC report (PCReport), or accepted in PC update (PCUpdate) or PC initiate (PCInitiate) by default, for compatibility reasons. This helps in interoperability with PCE implementation which does not understand or support Cisco specific information.

Vendor specific PCEP extension is optional and can be enabled using the **cisco-extension** command under PCE stateful client in MPLS-TE configuration.

For detailed steps to enable vendor specific PCEP extension, see Enabling PCEP Cisco Extension, on page 302.

Automatic Bandwidth Support for Delegated Tunnels

Automatic bandwidth feature allows a tunnel to automatically and dynamically adjust its reserved bandwidth over time, without network operator intervention. The automatic bandwidth feature support has been extended to delegated tunnels. Previously, tunnels configured with automatic bandwidth were switched to *collect-only* mode upon delegation.

New Style Affinities

Affinity is MPLS traffic engineering (TE) tunnel's requirements on the attributes of the links it will cross. The tunnel's affinity bits and affinity mask bits must match the attribute bits of the various links carrying the tunnel.

A new style of affinity reporting support is added in this IOS XR release. Even though TE ignores any affinities from the PCE, the new style affinities in PC update (PCUpdate) or PC initiate (PCInitiate) override the existing tunnel affinities. Previously, only old style affinities (value + mask) were reported. The new affinity mapping has PCEP affinities on the left and IOS XR affinities on the right.

- Lspa.exclude_any = AFFINITY_NEWSTYLE_EXCLUDE **OR** AFFINITY_NEWSTYLE_EXCLUDE_ALL
- Lspa.include_all = AFFINITY_NEWSTYLE_INCLUDE_STRICT
- Lspa.include_any = AFFINITY_NEWSTYLE_INCLUDE_STRICT **OR** AFFINITY_NEWSTYLE_INCLUDE

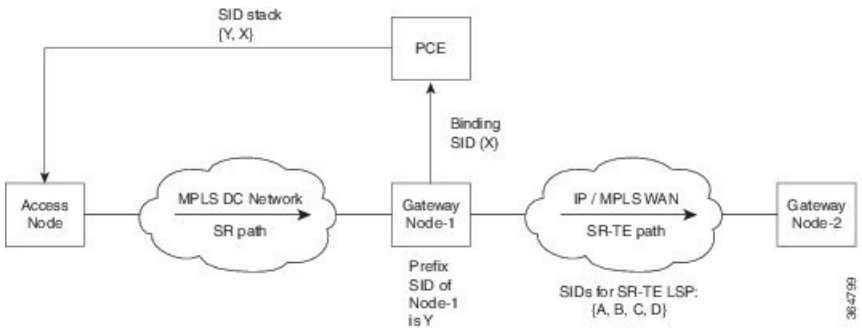
Binding Segment-ID

A binding Segment-ID (SID) can be used to enforce traffic engineering (TE) policy using RSVP-TE or SR-TE label switching path (LSP) tunnel. If the topmost label of an incoming packet is the binding SID, the packet is steered to the appropriate LSP tunnel. As such, a SID can be used by an upstream router to steer traffic originating from a downstream router into the appropriate TE path. If an LSP tunnel is PCE controlled, that is, either initiated by PCE or delegated to PCE, or simply reported (without delegation) to a PCE, the router allocates binding label and reports it to the PCE.

Use Case Scenario

A sample use case for binding SID is illustrated in the following diagram.

Figure 26: Sample Use of Binding SID



1. In the MPLS Data Center (DC) network, an SR LSP (without traffic engineering) is established using a prefix SID advertised by BGP.
2. In IP/MPLS WAN, an SR-TE LSP is setup using the PCE. The list of SIDs of the SR-TE LSP is {A, B, C, D}.
3. The gateway node 1 (which is the PCC) allocates a binding SID X and reports it to the PCE.
4. In order for the access node to steer the traffic over the SR-TE LSP, the PCE passes the SID stack {Y, X} where Y is the prefix SID of the gateway node 1 to the access node. In the absence of the binding SID X, the PCE passes the SID stack {Y, A, B, C, D} to the access node.

This example also illustrates the additional benefit of using the binding SID to reduce the number of SIDs imposed on the access nodes with a limited forwarding capacity.

MPLS TE Usability Enhancements

MPLS traffic engineering command line interface and logging output messages are enhanced as follows:

- The **show mpls traffic engineering** commands display **signaled-name** and supports **signaled-name** filter.
- Ability to allow immediate teardown of all labelled switched paths (LSPs) of the specified tunnel and to create new LSPs.
- Default behavior when affinity check fails at head-end is to reoptimize all LSP types.
- Logging output messages include MPLS TE tunnel signaled name.

- Logging of path change events and available bandwidth on the new for all auto-bandwidth operations.
- Auto-bandwidth logging output includes signaled name.

MPLS TE IPv6 Autoroute

The MPLS TE IPv6 Autoroute feature enables the use of IPv4 MPLS TE tunnels for IPv6 routing. The routing protocol IGP (IS-IS) considers the IPv4 MPLS TE tunnel for IPv6 routing path calculation only if the tunnel is advertised to carry IPv6 traffic. To advertise the tunnel, either IPv6 autoroute announce (AA) configuration or IPv6 forwarding adjacency (FA) configuration should be made on the tunnel. Also, the IPv6 has to be enabled on the tunnel so that the tunnel can handle IPv6 traffic.

For more information on MPLS TE IPv6 Autoroute, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on MPLS TE IPv6 Autoroute commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

MPLS TE IPv6 Autoroute Restrictions

- IGP support is only for IS-IS.
- IS-IS IPv4 and IPv6 must be configured under the same IS-IS instance.
- Unequal load balancing (UELB) does not apply to IPv6 traffic. While it may still be configured and used for IPv4 traffic, IPv6 traffic does not acknowledge the UELB configuration. However, equal loadsharing works for IPv6.
- Policy-based tunnel selection (PBTS) does not apply for IPv6 traffic. While it may still be configured and used for IPv4 traffic, IPv6 traffic does not acknowledge the PBTS configuration.
- MPLS auto tunnels do not support IPv6 autoroute announce and IPv6 forwarding adjacency configurations.

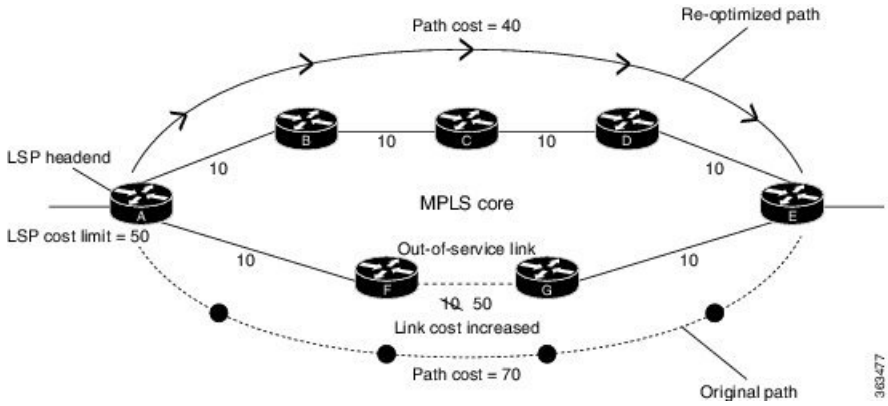
MPLS TE Path Cost Limit

The MPLS TE path cost limit feature enables graceful migration of TE label switched paths (LSPs) away from a link without affecting the traffic. This is useful when a link is scheduled to be decommissioned or brought down for maintenance.

In order to take a link out of service and gracefully migrate the LSPs away from it, the cost assigned to the link is to be set higher than the path cost limit (path aggregate admin-weight) assigned at the LSP headend. The cost of the tunnel is equal to the aggregate cost of the links through which the tunnel passes. The headend routers recalculate the total path costs at the time of periodic path verification. At this stage, the headend routers automatically check if the path limit is crossed and reroute the LSPs away from the out-of-service link.

This sample illustration explains the TE path cost limit application:

Figure 27: MPLS TE path cost limit application



Here, the path cost limit for the LSP is set at 50. To move the LSP away from the link between F and G, the link cost is increased to 50.

For more information on MPLS TE Path Cost Limit, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on MPLS TE Path Cost Limit commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Soft-preemption over FRR Backup Tunnels

The soft-preemption over FRR backup tunnels feature enables to move LSP traffic over the backup tunnels when the LSP is soft- preempted. MPLS TE tunnel soft-preemption allows removal of extra TE traffic in a graceful manner, by giving the preempted LSP a grace period to move away from the link. Though this mechanism saves the traffic of the preempted LSP from being dropped, this might cause traffic drops due to congestion as more bandwidth is reserved on the link than what is available. When the soft-preemption over FRR backup tunnel is enabled, the traffic of the preempted LSP is moved onto the FRR backup, if it is available and ready. This way, the capacity of the backup tunnel is used to remove the potential congestion that might be caused by soft-preemption.

For more information on Soft-Preemption over FRR Backup, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on Soft-Preemption over FRR Backup commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

MPLS TE Auto-tunnel Mesh One-hop

The MPLS TE Auto-tunnel primary one-hop feature allows automatic creation of tunnels over TE enabled interfaces to next hop neighbors. The Auto-tunnel primary one-hop is configurable under the MPLS TE Auto-tunnel mesh group mode and for each mesh group. The Auto-tunnel primary one-hop configuration automatically creates one-hop tunnels to next hop neighbors. A router that becomes a next hop neighbor will have a set of one-hop tunnels created automatically.

For more information on MPLS TE Auto-tunnel Primary One-hop, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information on MPLS TE Auto-tunnel Primary One-hop commands, see the *MPLS Traffic Engineering Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Inter-area Traffic Engineering with Dynamic ABR Discovery

The inter-area traffic engineering with dynamic ABR discovery feature adds support for inter-area point-to-point (P2P) and point-to-multi-point (P2MP) traffic engineering with dynamic ABR discovery. With this feature, there is no need to specify transit ABR addresses in the explicit paths to allow for dynamic/best path computation for inter-area tunnels.

For more information on Inter-area Traffic Engineering with Dynamic ABR Discovery, see the *Implementing MPLS Traffic Engineering* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*.

Named Tunnel

The Named Tunnel feature provides a simplified and flexible means of naming MPLS-TE tunnels.

In the traditional TE tunnel naming scheme, the tunnels are configured with IDs, where an ID is a 16-bit number. With increased TE tunnel scale in the network, and with the 64K limit, there is scarcity of unique tunnel IDs.

The Named Tunnel feature lets you name the TE tunnels in the network with unique tunnel IDs, which lets you manage the network more efficiently. This feature allows you to provision TE tunnels using STRING names.

For example: TUNNEL-NY-TO-LA

Named Path Option

For a given tunnel, you can configure one or more path options - each identified by a unique name. The path option expresses the preference for the path; lower numbers have a higher preference, with 1 having the highest preference. You can also configure the computation method for the path.

RSVP-TE Bandwidth Accounting

The total interface bandwidth utilization in the data plane, excluding RSVP-TE bandwidth, is called dark bandwidth. A network may have dark bandwidth due to IP, LDP, or segment routing traffic flowing in the network. Dark bandwidth effectively reduces the link bandwidth available to RSVP-TE LSPs.

When segment routing is enabled on the network, you should be aware of the segment routing traffic over the links so that RSVP-TE bandwidth reservations can avoid overbooking the links in the network. The RSVP-TE bandwidth accounting feature allows you to perform proper accounting of the traffic.

You can enable RSVP-TE bandwidth accounting, and start dark bandwidth advertisement based on accounting samples, for all MPLS-TE enabled links using the **bandwidth-accounting** command in MPLS-TE configuration mode.

Computing the Effective Maximum Reservable Bandwidth

The statistics collector process (statsD) is responsible for returning statistics counters for each feature. For each traffic engineering (TE)-enabled interface, the TE process collects new RSVP-TE bandwidth rate statistics (samples) from the statsD process, within a specified sampling interval. These samples are collected over a period of time called an application interval.

After each application interval, the average value of the collected rate samples is used to compute the dark bandwidth rate and the effective maximum reservable bandwidth (Max-Reservable-BW) rate.

The dark bandwidth rate is calculated as total rate - RSVP rate:

- The total rate includes IPv4 , IPv6, and MPLS rate (MPLS includes RSVP/LDP/BGP label packets)
- The RSVP rate includes IPv4/IPv6 encapsulation over tunnel, and MPLS label packet counters for RSVP-TE tunnels

The following example shows how the effective maximum reservable bandwidth (Effective-Max-Reservable-BW) is computed (assuming a link capacity of 10Gbps and a configured RSVP bandwidth of 90%):

- Link capacity = 10Gbps
- Max-reservable-bw = RSVP percentage of link capacity = 9Gbps
- Total rate (from statsD) = 5Gpbs
- RSVP rate (from statsD) = 3Gpbs
- Dark-bw = Total rate - RSVP rate = 2Gpbs
- Effective-Max-Reservable-BW = max-reservable-bw (9Gbps) - dark-bw (2Gbps) = 7Gbps

In this example, the bandwidth available for RSVP-TE LSP admission is 7Gbps. This value is flooded in the network if the flooding threshold is crossed.



Note When you change the RSVP bandwidth percentage configuration or when the bundle capacity changes due to bundle-member state change, TE accounts for the dark bandwidth when new bandwidth values are advertised.



Note The measured dark bandwidth can be increased or decreased based on a configurable adjustment factor.

When the computed dark bandwidth increases for a link, it will lower the max-reservable-bw of that link, which might trigger preemption of the RSVP-TE LSPs. Preemption consists of freeing the resources of an established LSP, and assigning them to a new LSP. The freeing of resources causes a traffic disruption to the LSP that is being preempted.



Note SR-TE LSPs at the head-end are treated with the highest priority and cannot be preempted.

You can apply measured rates immediately using the **bandwidth-accounting apply all** command. When you apply measured rates immediately, the RSVP-TE bandwidth-accounting might flood the updated bandwidth values immediately. Applying measured rates immediately does not affect the periodic application of the bandwidth.

How to Implement Traffic Engineering

Traffic engineering requires coordination among several global neighbor routers, creating traffic engineering tunnels, setting up forwarding across traffic engineering tunnels, setting up FRR, and creating differential service.

These procedures are used to implement MPLS-TE:

Building MPLS-TE Topology

Perform this task to configure MPLS-TE topology (required for traffic engineering tunnel operations).

Before you begin

Before you start to build the MPLS-TE topology, you must have enabled:

- IGP such as OSPF or IS-IS for MPLS-TE.
- MPLS Label Distribution Protocol (LDP).
- RSVP on the port interface.
- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.
- If you are going to use nondefault holdtime or intervals, you must decide the values to which they are set.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **exit**
5. **exit**
6. **router ospf** *process-name*
7. **area** *area-id*
8. **exit**
9. **mpls traffic-eng router-id** *ip-address*
10. **commit**
11. (Optional) **show mpls traffic-eng topology**
12. (Optional) **show mpls traffic-eng link-management advertisements**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**mpls traffic-eng**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Enters MPLS-TE configuration mode.

Step 3	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te)#interface POS0/6/0/0`
	`RP/0/RSP0/CPU0:router(config-mpls-te-if)#`
		Enables traffic engineering on a particular interface on the originating node and enters MPLS-TE interface configuration mode.

Step 4	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te-if)# exit`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Exits the current configuration mode.

Step 5	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Exits the current configuration mode.

Step 6	**router ospf** *process-name* **Example:** `RP/0/RSP0/CPU0:router(config)# router ospf 1`	Enters a name for the OSPF process.
Step 7	**area** *area-id* **Example:** `RP/0/RSP0/CPU0:router(config-router)# area 0`	Configures an area for the OSPF process. • Backbone areas have an area ID of 0. • Non-backbone areas have a non-zero area ID.
Step 8	**exit** **Example:**	Exits the current configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-ospf-ar)# exit` `RP/0/RSP0/CPU0:router(config-ospf)#`	
Step 9	**mpls traffic-eng router-id** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# mpls traffic-eng router-id 192.168.70.1`	Sets the MPLS-TE loopback interface.
Step 10	**commit**	
Step 11	(Optional) **show mpls traffic-eng topology** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng topology`	Verifies the traffic engineering topology.
Step 12	(Optional) **show mpls traffic-eng link-management advertisements** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng link-management advertisements`	Displays all the link-management advertisements for the links on this node.

Related Topics

How MPLS-TE Works, on page 203
Build MPLS-TE Topology and Tunnels: Example, on page 387

Creating an MPLS-TE Tunnel

Creating an MPLS-TE tunnel is a process of customizing the traffic engineering to fit your network topology.

Perform this task to create an MPLS-TE tunnel after you have built the traffic engineering topology.

Before you begin

The following prerequisites are required to create an MPLS-TE tunnel:

- You must have a router ID for the neighboring router.
- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.
- If you are going to use nondefault holdtime or intervals, you must decide the values to which they are set.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **destination** *ip-address*
4. **ipv4 unnumbered** *type interface-path-id*
5. **path-option** *preference - priority* **dynamic**
6. **signalled- bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*}
7. **commit**
8. (Optional) **show mpls traffic-eng tunnels**
9. (Optional) **show ipv4 interface brief**
10. (Optional) **show mpls traffic-eng link-management admission-control**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router# interface tunnel-te 1`	Configures an MPLS-TE tunnel interface.
Step 3	**destination** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-if)# destination 192.168.92.125`	Assigns a destination address on the new tunnel. The destination address is the remote node's MPLS-TE router ID.
Step 4	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered Loopback0`	Assigns a source address so that forwarding can be performed on the new tunnel. Loopback is commonly used as the interface type.
Step 5	**path-option** *preference - priority* **dynamic** **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 1 dynamic`	Sets the path option to dynamic and assigns the path ID.

	Command or Action	Purpose
Step 6	**signalled- bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*} **Example:** `RP/0/RSP0/CPU0:router(config-if)# signalled-bandwidth 100`	Sets the CT0 bandwidth required on this interface. Because the default tunnel priority is 7, tunnels use the default TE class map (namely, class-type 1, priority 7).
Step 7	**commit**	
Step 8	(Optional) **show mpls traffic-eng tunnels** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels`	Verifies that the tunnel is connected (in the UP state) and displays all configured TE tunnels.
Step 9	(Optional) **show ipv4 interface brief** **Example:** `RP/0/RSP0/CPU0:router# show ipv4 interface brief`	Displays all TE tunnel interfaces.
Step 10	(Optional) **show mpls traffic-eng link-management admission-control** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng link-management admission-control`	Displays all the tunnels on this node.

Related Topics

How MPLS-TE Works, on page 203
Build MPLS-TE Topology and Tunnels: Example, on page 387
Building MPLS-TE Topology, on page 260

Teardown and Reestablishment of RSVP-TE Tunnels

Table 10: Feature History Table

Feature Name	Release Information	Feature Description
Teardown and Reestablishment of RSVP-TE Tunnels	Release 7.11.1	You can now teardown and reestablish the existing tunnels of headend, midend, or tailend router tunnels of an MPLS network for optimized distribution of the traffic across MPLS and RSVP-TE to improve network performance and enhance resource utilization. Previously, you could reestablish tunnels only at the headend router using the mpls traffic-eng resetup command. The feature introduces these changes: **CLI**: mpls traffic-eng teardown **YANG Data Model**: Cisco-IOS-XR-mpls-te-act.yang (see GitHub, YANG Data Models Navigator)

In an MPLS-TE network which is configured with RSVP-TE, the headend, midend, and tailend router work together to establish and maintain tunnels or adjacencies for traffic engineering purposes. When the headend router boots up, it plays a critical role in MPLS-TE tunnel establishment using RSVP-TE signaling along the computed path with the tailend router.

During a system reboot, if a tailend router comes up first, the Interior Gateway Protocol (IGP) adjacency establishes a path for the tailend with the adjacent network devices. However, if the headend router comes up and starts creating tunnels during this tailend path creation, it may result in a poor distribution of tunnels at the tailend. In such cases, it's necessary to tear down all the tunnels and recreate them to ensure optimal distribution and functioning of the RSVP-TE as per the network conditions.

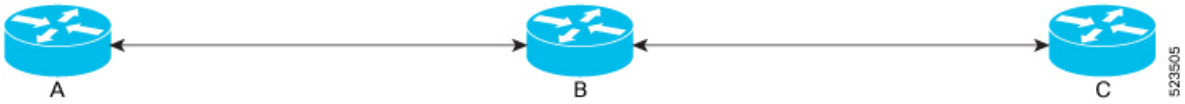
From Release 7.11.1, you can teardown and reestablish tunnels across all headend, midend, and tailend routers using the **mpls traffic-eng teardown** command with **all, head, mid, tail** parameters.

Table 11: Network Routers and Description

Router Name	Router Function	Tunnel Tear-Down and Reestablish Command
Headend Router	The headend router is responsible for determining the tunnel's path. It initiates the signaling process, specifying the tunnel's parameters and requirements. It sets up and manages the MPLS-TE tunnels.	**mpls traffic-eng teardown head**
Midend Router	The midend router, or an intermediate router or network device, is located between the headend and the tailend along the tunnel's path. It's involved in the signaling process and ensures the proper forwarding of traffic along the established tunnel.	**mpls traffic-eng teardown mid**

Router Name	Router Function	Tunnel Tear-Down and Reestablish Command
Tailend Router	The tailend router is the terminating router or network device located at the other end of the tunnel. It receives and processes the traffic that traverses through the tunnel and ensures proper traffic delivery to the destination.	**mpls traffic-eng teardown tail**

Figure 28: RSVP-TE tunnel Teardown and Reestablishment Topology



When RSVP-TE tunnel teardown message is triggered and:

- Router B is configured as tailend and Router A is configured as headend: A **ResvTear upstream** message is sent to the headend router. This message informs the headend router to tear down the RSVP-TE tunnel and release the resources associated with the tunnel.
- Router B is configured as headend and Router C as tailend: A **PathTear downstream** message is sent to the tailend router. A headend router triggers the process of recomputing the tunnels. The headend router (Router B) initiates the process of recomputing the tunnels, which involves recalculating the path and parameters for establishing new tunnels.
- Router B is configured as midend where Router A and Router B as headend and tailend respectively: A **ResvTear upstream** message is sent to the headend router and a **PathTear downstream** message is sent to the tailend router. These messages inform the respective routers to tear down the RSVP-TE tunnel and release the associated resources.

You can tear down and set up all types of tunnels including, P2P, P2MP, numbered, named, flex LSPs, and auto tunnels.

Limitations

- A maximum 90 seconds are required for the tunnels to get reestablished once they are torn.
- Use the **mpls traffic-eng resetup** command to reestablish the tunnels only at the headend router.

Configure Tear down and Reestablishment of RSVP-TE Tunnels

Configuration Example

Use the **mpls traffic-eng teardown all** command to tear down and reestablish all the RSVP-TE tunnels in a network node. This command must be executed in XR EXEC mode.

```
Router# mpls traffic-eng teardown all
```

Use the **mpls traffic-eng teardown head** command to tear down and reestablish the RSVP-TE tunnels at the headend router. This command must be executed in XR EXEC mode.

```
Router# mpls traffic-eng teardown head
```

Note You can also use the **mpls traffic-eng resetup** command to reestablish tunnels only at the headend router in XR EXEC mode.

Use the **mpls traffic-eng teardown mid** command to tear down and reestablish the RSVP-TE tunnels at the midend router. This command must be executed in XR EXEC mode.

```
Router# mpls traffic-eng teardown mid
```

Use the **mpls traffic-eng teardown tail** command to tear down and reestablish the RSVP-TE tunnels at the tailend router. This command must be executed in XR EXEC mode.

```
Router# mpls traffic-eng teardown tail
```

Use the **show mpls traffic-eng tunnels summary** command to check RSVP-TE tunnel status after you run the teardown command.

```
Router# show mpls traffic-eng tunnels summary
Output received:
Thu Sep 14 10:48:45.007 UTC

        Path Selection Tiebreaker:  Min-fill (default)
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 2806 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 9 seconds
      Periodic auto-bw collection:  5 minute(s) (disabled)

Signalling Summary:
    Head: 14006 interfaces, 14006 active signalling attempts, 14006 established
          14006 explicit, 0 dynamic
          14006 activations, 0 deactivations
          0 recovering, 0 recovered
    Mids: 2000
    Tails: 4003

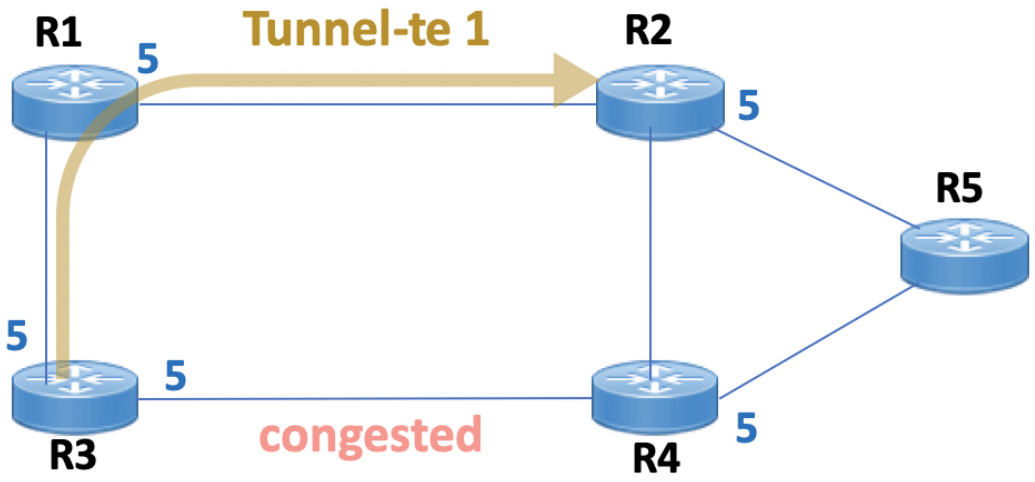
Fast ReRoute Summary:
    Head:     14000 FRR tunnels, 14000 protected, 0 rerouted
    Mid:      2000 FRR tunnels, 2000 protected, 0 rerouted
    Summary:  16000 protected, 13500 link protected, 2500 node protected, 0 bw protected
    Backup:   6 tunnels, 4 assigned
    Interface: 10 protected, 0 rerouted

Bidirectional Tunnel Summary:
    Tunnel Head: 0 total, 0 connected, 0 associated, 0 co-routed
    Tunnel Tail: 0 total, 0 connected, 0 associated, 0 co-routed
    LSPs Head:   0 established, 0 proceeding, 0 associated, 0 standby
    LSPs Mid:    0 established, 0 proceeding, 0 associated, 0 standby
    LSPs Tail:   0 established, 0 proceeding, 0 associated, 0 standby
```

Automatic Modification Of An MPLS-TE Tunnel's Metric

If the IGP calculation on a router results in an equal cost multipath (ECMP) scenario where next-hop interfaces are a mix of MPLS-TE tunnels and physical interfaces, you may want to ensure that a TE tunnel is preferred. Consider this topology:

Figure 29: MPLS-TE Tunnel



1. All links in the network have a metric of 5.
2. To offload a congested link between R3 and R4, an MPLS-TE tunnel is created from R3 to R2.
3. If the metric of the tunnel is also 5, traffic from R3 to R5 is load-balanced between the tunnel and the physical R3-R4 link.

To ensure that the MPLS-TE tunnel is preferred in such scenarios, configure the **autoroute metric** command on the tunnel interface. The modified metric is applied in the routing information base (RIB), and the tunnel is preferred over the physical path of the same metric. Sample configuration:

```
Router# configure
Router(config)# interface tunnel-te 1
Router(config-if)# autoroute metric relative -1
```

The **autoroute metric** command syntax is **autoroute metric** {**absolute**|**relative**} *value*

- **absolute** enables the absolute metric mode, for a metric range between 1 and 2147483647.
- **relative** enables the relative metric mode, for a metric range between -10 and 10, including zero.

Note Since the **relative** metric is not saved in the IGP database, the advertised metric of the MPLS-TE tunnel remains 5, and doesn't affect SPF calculation outcomes on other nodes.

Configuring Forwarding over the MPLS-TE Tunnel

Perform this task to configure forwarding over the MPLS-TE tunnel created in the previous task . This task allows MPLS packets to be forwarded on the link between network neighbors.

Before you begin

The following prerequisites are required to configure forwarding over the MPLS-TE tunnel:

- You must have a router ID for the neighboring router.
- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.



Note From the 7.1.1 release, IS-IS autoroute announce function is enhanced to redirect traffic from a source IP address prefix to a matching IP address assigned to an MPLS-TE tunnel destination interface.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **ipv4 unnumbered** *type interface-path-id*
4. **autoroute announce**
5. **exit**
6. **router static address-family ipv4 unicast** *prefix mask ip-address interface type*
7. **commit**
8. (Optional) **ping** {*ip-address* | *hostname*}
9. (Optional) **show mpls traffic-eng autoroute**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1`	Enters MPLS-TE interface configuration mode.
Step 3	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered Loopback0`	Assigns a source address so that forwarding can be performed on the new tunnel.

	Command or Action	Purpose
Step 4	**autoroute announce** **Example:** `RP/0/RSP0/CPU0:router(config-if)# autoroute announce`	Enables messages that notify the neighbor nodes about the routes that are forwarding.
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if)# exit`	Exits the current configuration mode.
Step 6	**router static address-family ipv4 unicast** *prefix mask ip-address interface type* **Example:** `RP/0/RSP0/CPU0:router(config)# router static address-family ipv4 unicast 172.16.0.1/32 tunnel-te 1`	Enables a route using IP version 4 addressing, identifies the destination address and the tunnel where forwarding is enabled. This configuration is used for static routes when the **autoroute announce** command is not used.
Step 7	**commit**	
Step 8	(Optional) **ping** {*ip-address* | *hostname*} **Example:** `RP/0/RSP0/CPU0:router# ping 192.168.12.52`	Checks for connectivity to a particular IP address or host name.
Step 9	(Optional) **show mpls traffic-eng autoroute** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng autoroute`	Verifies forwarding by displaying what is advertised to IGP for the TE tunnel.

Related Topics

Overview of MPLS Traffic Engineering, on page 201
Creating an MPLS-TE Tunnel, on page 262

Protecting MPLS Tunnels with Fast Reroute

Perform this task to protect MPLS-TE tunnels, as created in the previous task.

Note Although this task is similar to the previous task, its importance makes it necessary to present as part of the tasks required for traffic engineering on Cisco IOS XR software.

Before you begin

The following prerequisites are required to protect MPLS-TE tunnels:

- You must have a router ID for the neighboring router.
- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.
- You must first configure a primary tunnel.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **fast-reroute**
4. **exit**
5. **mpls traffic-eng**
6. **interface** *type interface-path-id*
7. **backup-path tunnel-te** *tunnel-number*
8. **exit**
9. **exit**
10. **interface tunnel-te** *tunnel-id*
11. **backup-bw** {*backup bandwidth* | **sub-pool** {*bandwidth* | **unlimited**} | **global-pool** {*bandwidth* | **unlimited**} }
12. **ipv4 unnumbered** *type interface-path-id*
13. **path-option** *preference-priority* {**explicit name** *explicit-path-name*}
14. **destination** *ip-address*
15. **commit**
16. (Optional) **show mpls traffic-eng tunnels backup**
17. (Optional) **show mpls traffic-eng tunnels protection frr**
18. (Optional) **show mpls traffic-eng fast-reroute database**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router# interface tunnel-te 1`	Configures an MPLS-TE tunnel interface.
Step 3	**fast-reroute** **Example:**	Enables fast reroute.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-if)# fast-reroute`	
Step 4	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if)# exit`	Exits the current configuration mode.

Step 5	**mpls traffic-eng**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Enters MPLS-TE configuration mode.

Step 6	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te)# interface pos0/6/0/0`
	`RP/0/RSP0/CPU0:router(config-mpls-te-if)#`
		Enables traffic engineering on a particular interface on the originating node.

Step 7	**backup-path tunnel-te** *tunnel-number* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# backup-path tunnel-te 2`	Sets the backup path to the backup tunnel.

Step 8	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te-if)# exit`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Exits the current configuration mode.

Step 9	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Exits the current configuration mode.

Step 10	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 2`	Configures an MPLS-TE tunnel interface.

	Command or Action	Purpose
Step 11	**backup-bw** {*backup bandwidth* | **sub-pool** {*bandwidth* | **unlimited**} | **global-pool** {*bandwidth* | **unlimited**} } **Example:** `RP/0/RSP0/CPU0:router(config-if)#backup-bw global-pool 5000`	Sets the CT0 bandwidth required on this interface. **Note** Because the default tunnel priority is 7, tunnels use the default TE class map.
Step 12	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered Loopback0`	Assigns a source address to set up forwarding on the new tunnel.
Step 13	**path-option** *preference-priority* {**explicit name** *explicit-path-name*} **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 1 explicit name backup-path`	Sets the path option to explicit with a given name (previously configured) and assigns the path ID.
Step 14	**destination** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-if)# destination 192.168.92.125`	Assigns a destination address on the new tunnel. • Destination address is the remote node's MPLS-TE router ID. • Destination address is the merge point between backup and protected tunnels. **Note** When you configure TE tunnel with multiple protection on its path and merge point is the same node for more than one protection, you must configure record-route for that tunnel.
Step 15	**commit**	
Step 16	(Optional) **show mpls traffic-eng tunnels backup** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels backup`	Displays the backup tunnel information.
Step 17	(Optional) **show mpls traffic-eng tunnels protection frr** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng`	Displays the tunnel protection information for Fast-Reroute (FRR).

	Command or Action	Purpose
	`tunnels protection frr`	
Step 18	(Optional) **show mpls traffic-eng fast-reroute database** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng fast-reroute database`	Displays the protected tunnel state (for example, the tunnel's current ready or active state).

Related Topics

Fast Reroute, on page 211
Fast Reroute Node Protection, on page 216
Creating an MPLS-TE Tunnel, on page 262
Configuring Forwarding over the MPLS-TE Tunnel, on page 268

Configuring Auto-bandwidth Bundle TE++

Table 12: Feature History Table

Feature Name	Release Information	Feature Description
MPLS-TE++ Support Over Numbered Tunnel-TE Interfaces	Release 7.10.1	We have optimized network performance and enabled efficient utilization of resources for numbered tunnels based on real-time traffic by automatically adding or removing tunnels between two endpoints. This is made possible because this release introduces support for auto-bandwidth TE++ for numbered tunnels, expanding upon the previous support for only named tunnels, letting you define explicit paths and allocate the bandwidth to each tunnel. The feature introduces these changes: • **CLI:** The **auto-capacity** keyword is added to the **interface tunnel-te** command. • **YANG Data Model:** New XPaths for `Cisco-IOS-XR-mpls-te-cfg.yang` (see GitHub, YANG Data Models Navigator)

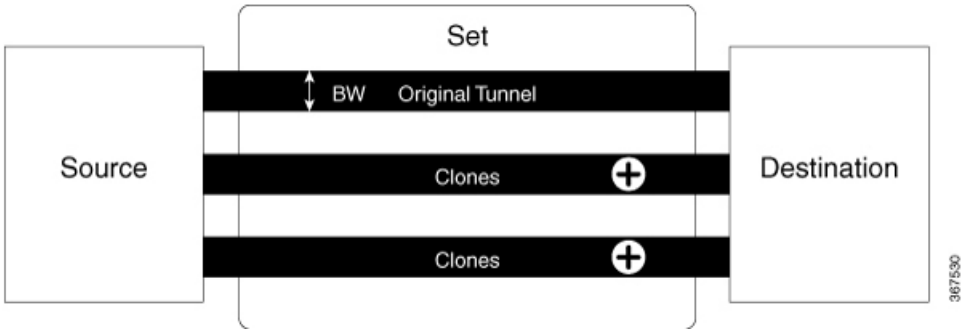
MPLS-TE tunnels are used to set up labeled connectivity and to provide dynamic bandwidth capacity between endpoints. The auto-bandwidth feature addresses the dynamic bandwidth capacity demands by dynamically resizing the MPLS-TE tunnels based on the measured traffic loads. However, many customers require multiple auto-bandwidth tunnels between endpoints for load balancing and redundancy. When the aggregate bandwidth demand increases between two endpoints, you can either configure auto-bandwidth feature to resize the tunnels or create new tunnels and load balance the overall demand over all the tunnels between two endpoints. Similarly, when the aggregate bandwidth demand decreases between two endpoints you can either configure the auto-bandwidth feature to decrease the sizes of the tunnel or delete the new tunnels and load balance the traffic over the remaining tunnels between the endpoints. The autobandwidth bundle TE++ feature is an extension of the auto-bandwidth feature and allows you to automatically increase or decrease the number of MPLS-TE tunnels to a destination based on real time traffic needs.

Tunnels that are automatically created as a response to the increasing bandwidth demands are called clones. The cloned tunnels inherit properties of the main configured tunnel. However, user configured load interval

cannot be inherited. The original tunnel and its clones are collectively called a set. You can specify an upper limit and lower limit on the number of clones that can be created for the original tunnel.

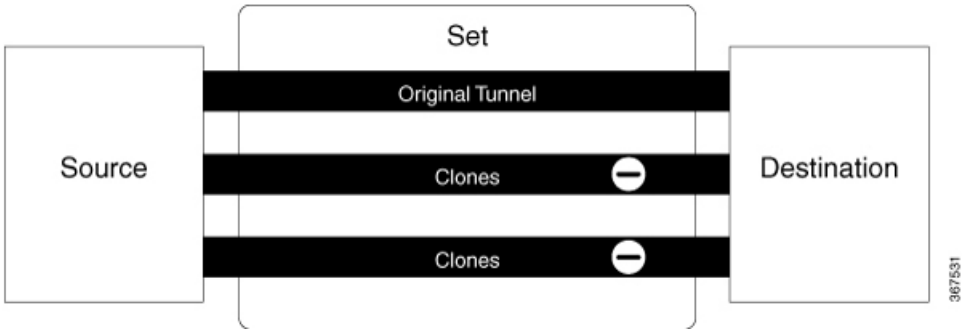
Splitting is the process of cloning a new tunnel when there is a demand for bandwidth increase. When the size of any of the tunnels in the set crosses a configured split bandwidth, then splitting is initiated and clone tunnels are created.

The following figure explains creating clone tunnels when the split bandwidth is exceeded.



Merging is the process of removing a clone tunnel when the bandwidth demand decreases. If the bandwidth goes below the configured merge bandwidth in any one of the tunnels in the set, clone tunnels are removed.

The following figure explains removing clone tunnels to merge with the original tunnel when the bandwidth falls below the merge bandwidth.



There are multiple ways to equally load-share the aggregate bandwidth demand among the tunnels in the set. This means that an algorithm is needed to choose the pair which satisfies the aggregate bandwidth requirements. You can configure a nominal bandwidth to guide the algorithm to determine the average bandwidths of the tunnels. If nominal bandwidth is not configured, TE uses the average of split and merge bandwidth as nominal bandwidth.

Restrictions and Usage Guidelines

The following usage guidelines apply for the autobandwidth bundle TE++ feature.

- This feature is only supported for the named tunnels and not supported on tunnel-te interfaces.
- The range for the lower limit on the number of clones is 0 to 63 and the default value for the lower limit on the number of clones is 0.
- The range for the upper limit on the number of clones is 1 to 63 and the default value for the upper limit on the number of clones is 63.

Configuration Example

This example shows how to configure the autobandwidth bundle TE++ feature for a named MPLS-TE traffic tunnel. You should configure the following values for this feature to work:

- min-clones: Specifies the minimum number of clone tunnels that the original tunnel can create.
- max-clones: Specifies the maximum number of clone tunnels that the original tunnel can create.
- nominal-bandwidth: Specifies the average bandwidth for computing the number of tunnels to satisfy the overall demand.
- split-bandwidth: Specifies the bandwidth value for splitting the original tunnel. If the tunnel bandwidth exceeds the configured split bandwidth, clone tunnels are created.
- merge-bandwidth: Specifies the bandwidth for merging clones with the original tunnel. If the bandwidth goes below the configured merge bandwidth, clone tunnels are removed.

In this example, the lower limit on the number of clones is configured as two and the upper limit on the number of clones is configured as four. The bandwidth size for splitting and merging is configured as 200 and 100 kbps.

```
Router(config)# mpls traffic-eng
Router(config-mpls-te)# named-tunnels
Router(config-te-named-tunnels)# tunnel-te xyz
Router(config-te-tun-name)# auto-bw
Router(config-mpls-te-tun-autobw)# auto-capacity
Router(config-te-tun-autocapacity)# min-clones 2
Router(config-te-tun-autocapacity)# max-clones 4
Router(config-te-tun-autocapacity)# nominal-bandwidth 5
Router(config-te-tun-autocapacity)# split-bandwidth 200
Router(config-te-tun-autocapacity)# merge-bandwidth 100
```

Enabling an AutoTunnel Backup

Perform this task to configure the AutoTunnel Backup feature. By default, this feature is disabled. You can configure the AutoTunnel Backup feature for each interface. It has to be explicitly enabled for each interface or link.

SUMMARY STEPS

1. **configure**
2. **ipv4 unnumbered mpls traffic-eng Loopback** *0*
3. **mpls traffic-eng**
4. **auto-tunnel backup timers removal unused** *frequency*
5. **auto-tunnel backup tunnel-id min** *min***max** *max*
6. **commit**
7. **show mpls traffic-eng auto-tunnel backup summary**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv4 unnumbered mpls traffic-eng Loopback** *0* **Example:** `RP/0/RSP0/CPU0:router(config)#ipv4 unnumbered mpls traffic-eng Loopback 0`	Configures the globally configured IPv4 address that can be used by the AutoTunnel Backup Tunnels. **Note** Loopback 0 is the router ID. The AutoTunnel Backup tunnels will not come up until a global IPv4 address is configured.
Step 3	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 4	**auto-tunnel backup timers removal unused** *frequency* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# auto-tunnel backup timers removal unused 20`	Configures how frequently a timer scans the backup automatic tunnels and removes tunnels that are not in use. • Use the frequency argument to scan the backup automatic tunnel. Range is 0 to 10080. **Note** You can also configure the auto-tunnel backup command at mpls traffic-eng interface mode.
Step 5	**auto-tunnel backup tunnel-id min** *min***max** *max* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# auto-tunnel backup tunnel-id min 6000 max 6500`	Configures the range of tunnel interface numbers to be used for automatic backup tunnels. Range is 0 to 65535.
Step 6	**commit**	
Step 7	**show mpls traffic-eng auto-tunnel backup summary** **Example:** RP/0/RSP0/CPU0:router# show mpls traffic-eng auto-tunnel backup summary	Displays information about configured MPLS-TE backup autotunnels.

Related Topics

Backup AutoTunnels, on page 204
Configure the MPLS-TE Auto-Tunnel Backup: Example, on page 401

Removing an AutoTunnel Backup

To remove all the backup autotunnels, perform this task to remove the AutoTunnel Backup feature.

SUMMARY STEPS

1. **clear mpls traffic-eng auto-tunnel backup unused** { **all** | **tunnel-te***number*}
2. **commit**
3. **show mpls traffic-eng auto-tunnel summary**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**clear mpls traffic-eng auto-tunnel backup unused** { **all** | **tunnel-te***number*} **Example:** `RP/0/RSP0/CPU0:router#  clear mpls traffic-eng auto-tunnel backup unused all`	Clears all MPLS-TE automatic backup tunnels from the EXEC mode. You can also remove the automatic backup tunnel marked with specific tunnel-te, provided it is currently unused.
Step 2	**commit**	
Step 3	**show mpls traffic-eng auto-tunnel summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng auto-tunnel summary`	Displays information about MPLS-TE autotunnels including the ones removed.

Related Topics

Backup AutoTunnels, on page 204
Configure the MPLS-TE Auto-Tunnel Backup: Example, on page 401

Establishing MPLS Backup AutoTunnels to Protect Fast Reroutable TE LSPs

To establish an MPLS backup autotunnel to protect fast reroutable TE LSPs, perform these steps:

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **auto-tunnel backup**
5. **attribute-set** *attribute-set-name*
6. **commit**
7. **show mpls traffic-eng auto-tunnel backup summary**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# interface POS 0/6/0/0`	Enables traffic engineering on a specific interface on the originating node.
Step 4	**auto-tunnel backup** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# auto-tunnel backup`	Enables an auto-tunnel backup feature for the specified interface. **Note** You cannot configure the static backup on the similar link.
Step 5	**attribute-set** *attribute-set-name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if-auto-backup)#attribute-set ab`	Configures attribute-set template for auto-tunnel backup tunnels.
Step 6	**commit**	
Step 7	**show mpls traffic-eng auto-tunnel backup summary** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic auto-tunnel backup summary`	Displays information about configured MPLS-TE backup autotunnels.

Related Topics

Backup AutoTunnels, on page 204
Configure the MPLS-TE Auto-Tunnel Backup: Example, on page 401

Establishing Next-Hop Tunnels with Link Protection

To establish a next-hop tunnel and link protection on the primary tunnel, perform these steps:

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **auto-tunnel backup nhop-only**

5. **auto-tunnel backup exclude srlg** [preferred]
6. **attribute-set** *attribute-set-name*
7. **commit**
8. **show mpls traffic-eng tunnels** *number* **detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# interface POS 0/6/0/0`	Enables traffic engineering on a specific interface on the originating node.
Step 4	**auto-tunnel backup nhop-only** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# auto-tunnel backup nhop-only`	Enables the creation of dynamic NHOP backup tunnels. By default, both NHOP and NNHOP protection are enabled. **Note** Using this nhop-only option, only link protection is provided.
Step 5	**auto-tunnel backup exclude srlg** [preferred] **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# auto-tunnel backup exclude srlg preferred`	Enables the exclusion of SRLG values on a given link for the AutoTunnel backup associated with a given interface. The preferred option allows the AutoTunnel Backup tunnels to come up even if no path excluding all SRLG is found.
Step 6	**attribute-set** *attribute-set-name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if-auto-backup)#attribute-set ab`	Configures attribute-set template for auto-tunnel backup tunnels.
Step 7	**commit**	
Step 8	**show mpls traffic-eng tunnels** *number* **detail** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels 1 detail`	Displays information about configured NHOP tunnels and SRLG information.

Related Topics

Backup AutoTunnels, on page 204
Configure the MPLS-TE Auto-Tunnel Backup: Example, on page 401

Configuring a Prestandard DS-TE Tunnel

Perform this task to configure a Prestandard DS-TE tunnel.

Before you begin

The following prerequisites are required to configure a Prestandard DS-TE tunnel:

- You must have a router ID for the neighboring router.
- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.

SUMMARY STEPS

1. **configure**
2. **rsvp interface** *type interface-path-id*
3. **bandwidth** [*total reservable bandwidth*] [**bc0** *bandwidth*] [**global-pool** *bandwidth*] [**sub-pool** *reservable-bw*]
4. **exit**
5. **exit**
6. **interface tunnel-te** *tunnel-id*
7. **signalled-bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*}
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp interface pos0/6/0/0`	Enters RSVP configuration mode and selects an RSVP interface.
Step 3	**bandwidth** [*total reservable bandwidth*] [**bc0** *bandwidth*] [**global-pool** *bandwidth*] [**sub-pool** *reservable-bw*] **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if)# bandwidth 100 150 sub-pool 50`	Sets the reserved RSVP bandwidth available on this interface by using the prestandard DS-TE mode. The range for the *total reserve bandwidth* argument is 0 to 4294967295. Physical interface bandwidth is not used by MPLS-TE.
Step 4	**exit** **Example:**	Exits the current configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# exit` `RP/0/RSP0/CPU0:router(config-rsvp)#`	

Step 5	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Exits the current configuration mode.

Step 6	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 2`	Configures an MPLS-TE tunnel interface.

Step 7	**signalled-bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*}
	Example:
	`RP/0/RSP0/CPU0:router(config-if)#`
	`signalled-bandwidth sub-pool 10`
		Sets the bandwidth required on this interface. Because the default tunnel priority is 7, tunnels use the default TE class map (namely, class-type 1, priority 7).

Step 8	**commit**	

Related Topics

Configuring Traffic Engineering Tunnel Bandwidth, on page 157
Prestandard DS-TE Mode, on page 208
Configure IETF DS-TE Tunnels: Example, on page 388

Configuring an IETF DS-TE Tunnel Using RDM

Perform this task to create an IETF mode DS-TE tunnel using RDM.

Before you begin

The following prerequisites are required to create an IETF mode DS-TE tunnel using RDM:

- You must have a router ID for the neighboring router.
- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.

SUMMARY STEPS

1. **configure**

2. **rsvp interface** *type interface-path-id*
3. **bandwidth rdm** {*total-reservable-bw* | **bc0** | **global-pool**} {**sub-pool** | **bc1** *reservable-bw*}
4. **exit**
5. **exit**
6. **mpls traffic-eng**
7. **ds-te mode ietf**
8. **exit**
9. **interface tunnel-te** *tunnel-id*
10. **signalled-bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*}
11. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp interface pos0/6/0/0`	Enters RSVP configuration mode and selects an RSVP interface.
Step 3	**bandwidth rdm** {*total-reservable-bw*	**bc0**	**global-pool**} {**sub-pool**	**bc1** *reservable-bw*} **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if)# bandwidth rdm 100 150`	Sets the reserved RSVP bandwidth available on this interface by using the Russian Doll Model (RDM) bandwidth constraints model. The range for the *total reserve bandwidth* argument is 0 to 4294967295. **Note** Physical interface bandwidth is not used by MPLS-TE.

Step 4	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# exit`
	`RP/0/RSP0/CPU0:router(config-rsvp)`
		Exits the current configuration mode.

Step 5	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp) exit`
	`RP/0/RSP0/CPU0:router(config)`
		Exits the current configuration mode.

Step 6	**mpls traffic-eng** **Example:**	Enters MPLS-TE configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng` `RP/0/RSP0/CPU0:router(config-mpls-te)#`	
Step 7	**ds-te mode ietf** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# ds-te mode ietf`	Enables IETF DS-TE mode and default TE class map. IETF DS-TE mode is configured on all network nodes.
Step 8	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# exit`	Exits the current configuration mode.

Step 9	**interface tunnel-te** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface tunnel-te 4`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Configures an MPLS-TE tunnel interface.

Step 10	**signalled-bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*}
	Example:
	`RP/0/RSP0/CPU0:router(config-if)#`
	`signalled-bandwidth 10 class-type 1`
		Configures the bandwidth required for an MPLS TE tunnel. Because the default tunnel priority is 7, tunnels use the default TE class map (namely, class-type 1, priority 7).

Step 11	**commit**	

Related Topics

Configuring Traffic Engineering Tunnel Bandwidth, on page 157
Russian Doll Bandwidth Constraint Model, on page 209

Configuring an IETF DS-TE Tunnel Using MAM

Perform this task to configure an IETF mode differentiated services traffic engineering tunnel using the Maximum Allocation Model (MAM) bandwidth constraint model.

Before you begin

The following prerequisites are required to configure an IETF mode differentiated services traffic engineering tunnel using the MAM bandwidth constraint model:

- You must have a router ID for the neighboring router.

- Stable router ID is required at either end of the link to ensure that the link is successful. If you do not assign a router ID to the routers, the system defaults to the global router ID. Default router IDs are subject to change, which can result in an unstable link.

SUMMARY STEPS

1. **configure**
2. **rsvp interface** *type interface-path-id*
3. **bandwidth mam** {*total reservable bandwidth* | **max-reservable-bw** *maximum-reservable-bw*} [**bc0** *reservable bandwidth*] [**bc1** *reservable bandwidth*]
4. **exit**
5. **exit**
6. **mpls traffic-eng**
7. **ds-te mode ietf**
8. **ds-te bc-model mam**
9. **exit**
10. **interface tunnel-te** *tunnel-id*
11. **signalled-bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*}
12. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp interface pos0/6/0/0`	Enters RSVP configuration mode and selects the RSVP interface.
Step 3	**bandwidth mam** {*total reservable bandwidth*	**max-reservable-bw** *maximum-reservable-bw*} [**bc0** *reservable bandwidth*] [**bc1** *reservable bandwidth*] **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if)# bandwidth mam max-reservable-bw 400 bc0 300 bc1 200`	Sets the reserved RSVP bandwidth available on this interface. **Note** Physical interface bandwidth is not used by MPLS-TE.

Step 4	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp-if)# exit`
	`RP/0/RSP0/CPU0:router(config-rsvp)#`
		Exits the current configuration mode.

	Command or Action	Purpose

Step 5	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-rsvp)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Exits the current configuration mode.

Step 6	**mpls traffic-eng**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Enters MPLS-TE configuration mode.

Step 7	**ds-te mode ietf** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# ds-te mode ietf`	Enables IETF DS-TE mode and default TE class map. Configure IETF DS-TE mode on all nodes in the network.
Step 8	**ds-te bc-model mam** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# ds-te bc-model mam`	Enables the MAM bandwidth constraint model globally.
Step 9	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# exit`	Exits the current configuration mode.

Step 10	**interface tunnel-te** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface tunnel-te 4`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Configures an MPLS-TE tunnel interface.

Step 11	**signalled-bandwidth** {*bandwidth* [**class-type** *ct*] | **sub-pool** *bandwidth*} **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-if)# signalled-bandwidth 10 class-type 1`	Configures the bandwidth required for an MPLS TE tunnel. Because the default tunnel priority is 7, tunnels use the default TE class map (namely, class-type 1, priority 7).

	Command or Action	Purpose
Step 12	**commit**	

Related Topics

Configuring Traffic Engineering Tunnel Bandwidth, on page 157
Maximum Allocation Bandwidth Constraint Model, on page 209

Configuring MPLS -TE and Fast-Reroute on OSPF

Perform this task to configure MPLS-TE and Fast Reroute (FRR) on OSPF.

Before you begin

Note Only point-to-point (P2P) interfaces are supported for OSPF multiple adjacencies. These may be either native P2P interfaces or broadcast interfaces on which the **OSPF P2P configuration** command is applied to force them to behave as P2P interfaces as far as OSPF is concerned. This restriction does not apply to IS-IS.

The tunnel-te interface is not supported under IS-IS.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **path-option** [**protecting**] *preference-priority* {**dynamic** [**pce** [**address ipv4** *address*] | **explicit** {**name** *pathname* | **identifier** *path-number* } } [**isis** *instance name* {**level** *level*}] [**ospf** *instance name* {**area** *area ID*}]] [**verbatim**] [**lockdown**]
4. Repeat Step 3 as many times as needed.
5. **commit**
6. **show mpls traffic-eng tunnels** [*tunnel-number*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**interface tunnel-te** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Configures an MPLS-TE tunnel interface. The range for the tunnel ID number is 0 to 65535.

	Command or Action	Purpose
Step 3	**path-option** [**protecting**] *preference-priority* {**dynamic** [**pce** [**address ipv4** *address*] | **explicit** {**name** *pathname* | **identifier** *path-number* } } [**isis** *instance name* {**level** *level*}] [**ospf** *instance name* {**area** *area ID*}]] [**verbatim**] [**lockdown**] **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 1 explicit identifier 6 ospf green area 0`	Configures an explicit path option for an MPLS-TE tunnel. OSPF is limited to a single OSPF instance and area.
Step 4	Repeat Step 3 as many times as needed. **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 2 explicit name 234 ospf 3 area 7 verbatim`	Configures another explicit path option.
Step 5	**commit**	
Step 6	**show mpls traffic-eng tunnels** [*tunnel-number*] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels 1`	Displays information about MPLS-TE tunnels.

Configuring the Ignore Integrated IS-IS Overload Bit Setting in MPLS-TE

Perform this task to configure an overload node avoidance in MPLS-TE. When the overload bit is enabled, tunnels are brought down when the overload node is found in the tunnel path.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **path-selection ignore overload {head | mid | tail}**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose

Step 2	**mpls traffic-eng**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Enters MPLS-TE configuration mode.

Step 3	**path-selection ignore overload {head | mid | tail}**
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
	`path-selection ignore overload head`
		Ignores the Intermediate System-to-Intermediate System (IS-IS) overload bit setting for MPLS-TE.
		If **set-overload-bit** is set by IS-IS on the head router, the tunnels stay up.

Step 4	**commit**	

Related Topics

Ignore Intermediate System-to-Intermediate System Overload Bit Setting in MPLS-TE, on page 212
Configure the Ignore IS-IS Overload Bit Setting in MPLS-TE: Example, on page 389

Configuring Flexible Name-based Tunnel Constraints

To fully configure MPLS-TE flexible name-based tunnel constraints, you must complete these high-level tasks in order:

1. Assigning Color Names to Numeric Values, on page 290
2. Associating Affinity-Names with TE Links, on page 291
3. Associating Affinity Constraints for TE Tunnels, on page 292

Assigning Color Names to Numeric Values

The first task in enabling the new coloring scheme is to assign a numerical value (in hexadecimal) to each value (color).

Note An affinity color name cannot exceed 64 characters. An affinity value cannot exceed a single digit. For example, magenta1.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **affinity-map** *affinity name* {*affinity value* | **bit-position** *value*}
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**mpls traffic-eng**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Enters MPLS-TE configuration mode.

Step 3	**affinity-map** *affinity name* {*affinity value* | **bit-position** *value*} **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# affinity-map red 1`	Enters an affinity name and a map value by using a color name (repeat this command to assign multiple colors up to a maximum of 64 colors). An affinity color name cannot exceed 64 characters. The value you assign to a color name must be a single digit.
Step 4	**commit**	

Related Topics

Flexible Name-based Tunnel Constraints, on page 213
Configure Flexible Name-based Tunnel Constraints: Example, on page 390

Associating Affinity-Names with TE Links

The next step in the configuration of MPLS-TE Flexible Name-based Tunnel Constraints is to assign affinity names and values to TE links. You can assign up to a maximum of 32 colors. Before you assign a color to a link, you must define the name-to-value mapping for each color.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **attribute-names** *attribute name*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose

Step 2	**mpls traffic-eng**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Enters MPLS-TE configuration mode.

Step 3	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te)# interface tunnel-te 2`
	`RP/0/RSP0/CPU0:router(config-mpls-te-if)#`
		Enables MPLS-TE on an interface and enters MPLS-TE interface configuration mode.

Step 4	**attribute-names** *attribute name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# attribute-names red`	Assigns colors to TE links over the selected interface.
Step 5	**commit**	

Related Topics

Flexible Name-based Tunnel Constraints, on page 213
Configure Flexible Name-based Tunnel Constraints: Example, on page 390
Assigning Color Names to Numeric Values, on page 290

Associating Affinity Constraints for TE Tunnels

The final step in the configuration of MPLS-TE Flexible Name-based Tunnel Constraints requires that you associate a tunnel with affinity constraints.

Using this model, there are no masks. Instead, there is support for four types of affinity constraints:

- include
- include-strict
- exclude
- exclude-all

Note For the affinity constraints above, all but the exclude-all constraint may be associated with up to 10 colors.

SUMMARY STEPS

1. **configure**

2. **interface tunnel-te** *tunnel-id*
3. **affinity** {*affinity-value* **mask** *mask-value* | **exclude** *name* | **exclude -all** | **include** *name* | **include-strict** *name*}
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1`	Configures an MPLS-TE tunnel interface.
Step 3	**affinity** {*affinity-value* **mask** *mask-value* | **exclude** *name* | **exclude -all** | **include** *name* | **include-strict** *name*} **Example:** `RP/0/RSP0/CPU0:router(config-if)# affinity include red`	Configures link attributes for links comprising a tunnel. You can have up to ten colors. Multiple include statements can be specified under tunnel configuration. With this configuration, a link is eligible for CSPF if it has at least a red color or has at least a green color. Thus, a link with red and any other colors as well as a link with green and any additional colors meet the above constraint.
Step 4	**commit**	

Related Topics

Flexible Name-based Tunnel Constraints, on page 213
Configure Flexible Name-based Tunnel Constraints: Example, on page 390

Configuring IS-IS to Flood MPLS-TE Link Information

Perform this task to configure a router running the Intermediate System-to-Intermediate System (IS-IS) protocol to flood MPLS-TE link information into multiple IS-IS levels.

This procedure shows how to enable MPLS-TE in both IS-IS Level 1 and Level 2.

SUMMARY STEPS

1. **configure**
2. **router isis** *instance-id*
3. **net** *network-entity-title*
4. **address-family** {**ipv4** | **ipv6**} {**unicast**}
5. **mpls traffic-eng tunnel restricted**
6. **metric-style wide**

7. **mpls traffic-eng** *level*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router isis** *instance-id* **Example:** `RP/0/RSP0/CPU0:router(config)# router isis 1`	Enters an IS-IS instance.
Step 3	**net** *network-entity-title* **Example:** `RP/0/RSP0/CPU0:router(config-isis)# net 47.0001.0000.0000.0002.00`	Enters an IS-IS network entity title (NET) for the routing process.
Step 4	**address-family** {**ipv4** | **ipv6**} {**unicast**} **Example:** `RP/0/RSP0/CPU0:router(config-isis)# address-family ipv4 unicast`	Enters address family configuration mode for configuring IS-IS routing that uses IPv4 and IPv6 address prefixes.
Step 5	**mpls traffic-eng tunnel restricted** **Example:** `RP/0/RSP0/CPU0:router(config-isis-af)# mpls traffic-eng tunnel restricted`	(Optional) Steers traffic from MPLS-TE tunnel source IP address prefixes towards matching IP addresses assigned on MPLS-TE tunnel destination interfaces.
Step 6	**metric-style wide** **Example:** `RP/0/RSP0/CPU0:router(config-isis-af)# metric-style wide`	Enters the new-style type, length, and value (TLV) objects.
Step 7	**mpls traffic-eng** *level* **Example:** `RP/0/RSP0/CPU0:router(config-isis-af)# mpls traffic-eng level-1-2`	Enters the required MPLS-TE level or levels.

	Command or Action	Purpose
Step 8	**commit**	

Configuring an OSPF Area of MPLS-TE

Perform this task to configure an OSPF area for MPLS-TE in both the OSPF backbone area 0 and area 1.

SUMMARY STEPS

1. **configure**
2. **router ospf** *process-name*
3. **mpls traffic-eng router-id** *ip-address*
4. **area** *area-id*
5. **interface** *type interface-path-id*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**router ospf** *process-name* **Example:** `RP/0/RSP0/CPU0:router(config)# router ospf 100`	Enters a name that uniquely identifies an OSPF routing process. ***process-name*** Any alphanumeric string no longer than 40 characters without spaces.
Step 3	**mpls traffic-eng router-id** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# mpls traffic-eng router-id 192.168.70.1`	Enters the MPLS interface type. For more information, use the question mark (?) online help function.
Step 4	**area** *area-id* **Example:** `RP/0/RSP0/CPU0:router(config-ospf)# area 0`	Enters an OSPF area identifier. ***area-id*** Either a decimal value or an IP address.
Step 5	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-ospf-ar)# interface`	Identifies an interface ID. For more information, use the question mark (?) online help function.

	Command or Action	Purpose
	`POS 0/2/0/0`	
Step 6	**commit**	

Configuring Explicit Paths with ABRs Configured as Loose Addresses

Perform this task to specify an IPv4 explicit path with ABRs configured as loose addresses.

SUMMARY STEPS

1. **configure**
2. **explicit-path name** *name*
3. **index** *index-id* **next-address** [**loose**] **ipv4 unicast** *ip-address*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**explicit-path name** *name* **Example:** `RP/0/RSP0/CPU0:router(config)# explicit-path name interarea1`	Enters a name for the explicit path.
Step 3	**index** *index-id* **next-address** [**loose**] **ipv4 unicast** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-expl-path)# index 1 next-address loose ipv4 unicast 10.10.10.10`	Includes an address in an IP explicit path of a tunnel.
Step 4	**commit**	

Configuring MPLS-TE Forwarding Adjacency

Perform this task to configure forwarding adjacency on a specific tunnel-te interface.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*

3. **forwarding-adjacency holdtime** *value*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1`	Enters MPLS-TE interface configuration mode.
Step 3	**forwarding-adjacency holdtime** *value* **Example:** `RP/0/RSP0/CPU0:router(config-if)# forwarding-adjacency holdtime 60`	Configures forwarding adjacency using an optional specific holdtime value. By default, this value is 0 (milliseconds).
Step 4	**commit**	

Related Topics

MPLS-TE Forwarding Adjacency Benefits, on page 217
Configure Forwarding Adjacency: Example, on page 392

Configuring a Path Computation Client and Element

Perform these tasks to configure Path Comptation Client (PCC) and Path Computation Element (PCE):

- Configuring a Path Computation Client, on page 297
- Configuring a Path Computation Element Address, on page 298
- Configuring PCE Parameters, on page 299

Configuring a Path Computation Client

Perform this task to configure a TE tunnel as a PCC.

Note Only one TE-enabled IGP instance can be used at a time.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **path-option** *preference-priority* **dynamic pce**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 6`	Enters MPLS-TE interface configuration mode and enables traffic engineering on a particular interface on the originating node.
Step 3	**path-option** *preference-priority* **dynamic pce** **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 1 dynamic pce`	Configures a TE tunnel as a PCC.
Step 4	**commit**	

Related Topics

Path Computation Element, on page 218
Configure PCE: Example, on page 392

Configuring a Path Computation Element Address

Perform this task to configure a PCE address.

Note Only one TE-enabled IGP instance can be used at a time.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **pce address ipv4** *address*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters the MPLS-TE configuration mode.
Step 3	**pce address ipv4** *address* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce address ipv4 10.1.1.1`	Configures a PCE IPv4 address.
Step 4	**commit**	

Related Topics

Path Computation Element, on page 218
Configure PCE: Example, on page 392

Configuring PCE Parameters

Perform this task to configure PCE parameters, including a static PCE peer, periodic reoptimization timer values, and request timeout values.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **pce address ipv4** *address*
4. **pce peer ipv4** *address*
5. **pce keepalive** *interval*
6. **pce deadtimer** *value*
7. **pce reoptimize** *value*
8. **pce request-timeout** *value*
9. **pce tolerance keepalive** *value*
10. **commit**
11. **show mpls traffic-eng pce peer** [*address* | **all**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**pce address ipv4** *address* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce address ipv4 10.1.1.1`	Configures a PCE IPv4 address.
Step 4	**pce peer ipv4** *address* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce peer address ipv4 10.1.1.1`	Configures a static PCE peer address. PCE peers are also discovered dynamically through OSPF or ISIS.
Step 5	**pce keepalive** *interval* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce keepalive 10`	Configures a PCEP keepalive interval. The range is from 0 to 255 seconds. When the keepalive interval is 0, the LSR does not send keepalive messages.
Step 6	**pce deadtimer** *value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce deadtimer 50`	Configures a PCE deadtimer value. The range is from 0 to 255 seconds. When the dead interval is 0, the LSR does not timeout a PCEP session to a remote peer.
Step 7	**pce reoptimize** *value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce reoptimize 200`	Configures a periodic reoptimization timer value. The range is from 60 to 604800 seconds. When the dead interval is 0, the LSR does not timeout a PCEP session to a remote peer.

	Command or Action	Purpose
Step 8	**pce request-timeout** *value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce request-timeout 10`	Configures a PCE request-timeout. Range is from 5 to 100 seconds. PCC or PCE keeps a pending path request only for the request-timeout period.
Step 9	**pce tolerance keepalive** *value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# pce tolerance keepalive 10`	Configures a PCE tolerance keepalive value (which is the minimum acceptable peer proposed keepalive).
Step 10	**commit**	
Step 11	**show mpls traffic-eng pce peer** [*address* | **all**] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng pce peer`	Displays the PCE peer address and state.

Related Topics

Path Computation Element, on page 218
Configure PCE: Example, on page 392

Configuring Fast Repair

Perform this task to configure fast repair to minimize the tunnel down time.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **pce**
4. **stateful-client**
5. **fast-repair**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)#mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**pce** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)#pce`	Enters PCE configuration mode.
Step 4	**stateful-client** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-pce)#stateful-client`	Enters stateful PCE client configuration mode. When the stateful-client configuration is added to the node, it will close all existing PCEP peer connections, and add the stateful capabilities TLV to the OPEN object it exchanges during the PCEP session establishment. When the stateful-client configuration is removed from the node, it will delete all PCE instantiated tunnels, close all existing PCEP connections, and no longer add the stateful capabilities TLV to the OPEN object it exchanges during the PCEP session establishment.
Step 5	**fast-repair** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-pce-stateful)#fast-repair`	Configures fast repair.
Step 6	**commit**	

Enabling PCEP Cisco Extension

Perform this task to enable PCEP Cisco extension.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **pce**
4. **stateful-client**
5. **cisco-extension**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)#mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**pce** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)#pce`	Enters PCE configuration mode.
Step 4	**stateful-client** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-pce)#stateful-client`	Enters stateful PCE client configuration mode. When the stateful-client configuration is added to the node, it will close all existing PCEP peer connections, and add the stateful capabilities TLV to the OPEN object it exchanges during the PCEP session establishment. When the stateful-client configuration is removed from the node, it will delete all PCE instantiated tunnels, close all existing PCEP connections, and no longer add the stateful capabilities TLV to the OPEN object it exchanges during the PCEP session establishment.
Step 5	**cisco-extension** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-pce-stateful)#cisco-extension`	Enables PCEP Cisco extension.
Step 6	**commit**	

Configuring MPLS-TE LSP Timers

Table 13: Feature History Table

Feature Name	Release Information	Feature Description
MPLS-TE: Backoff Timer	Release 7.3.2	In case of an LSP error on a head-end router, this feature introduces the flexibility to either set a timer for the router to retry sending traffic, or resend traffic across a different LSP without a waiting period. New command: • **mpls traffic-eng timers backoff-timer**

When an LSP path error occurs, the head-end router attempts to send traffic over the LSP after a 3-second interval. The router continues these attempts, with the time interval doubled between each attempt, till the total time from the first path error is 300 seconds. This timer function is the *MPLS-TE backoff timer*. You can update the default initial and final time duration (3 seconds and 300 seconds, respectively) using the **mpls traffic-eng timers backoff-timer** command.

Backoff Timer Configuration

```
Router# configure
Router (config)# mpls traffic-eng timers backoff-timer initial-interval 3 final-interval
600
Router (config)# commit
```

To enable MPLS-TE to send traffic over a different LSP immediately after a path error occurs, set the initial and final backoff timer values to 0, as shown below.

```
Router# configure
Router (config)# mpls traffic-eng timers backoff-timer initial-interval 0 final-interval 0
Router (config)# commit
```

Running Configuration

```
Router# show run mpls traffic-eng

mpls traffic-eng
 timers backoff-timer initial-interval 10 final-interval 400
!
```

Configuring Forwarding Path

Perform this task to configure forwarding path in the MPLS-TE interface.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*

3. **forward-class** *forward-class*
4. **exit**
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1`	Enters MPLS-TE configuration mode.
Step 3	**forward-class** *forward-class* **Example:** `RP/0/RSP0/CPU0:router(config-if)# forward-class 1`	Defines forwarding path in the MPLS-TE interface.

Step 4	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# exit`
	`RP/0/RSP0/CPU0:router(config)#`
		Exits the current configuration mode.

Step 5	**commit**	

Related Topics

Policy-Based Tunnel Selection Functions, on page 220
Policy-Based Tunnel Selection, on page 219

Configuring Path Protection on MPLS-TE

These tasks show how to configure path protection on MPLS-TE:

Enabling Path Protection for an Interface

Perform this task to enable path protection for a given tunnel interface.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*

3. **path-protection**
4. **commit**
5. **show mpls traffic-eng tunnels** [*tunnel-number*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 6`	Configures an MPLS-TE tunnel interface and enables traffic engineering on a particular interface on the originating node.
Step 3	**path-protection** **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-protection`	Enables path protection on the tunnel-te interface.
Step 4	**commit**	
Step 5	**show mpls traffic-eng tunnels** [*tunnel-number*] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels 6`	Displays information that path protection is enabled on the tunnel-te interface for tunnel number 6.

Related Topics

Path Protection, on page 228
Pre-requisites for Path Protection, on page 229
Restrictions for Path Protection, on page 229
Configure Tunnels for Path Protection: Example, on page 396

Assigning a Dynamic Path Option to a Tunnel

Perform this task to assign a secondary path option in case there is a link or node failure along a path and all interfaces in your network are not protected.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **path-option** *preference-priority* **dynamic**

4. **commit**
5. **show mpls traffic-eng tunnels** [*tunnel-number*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 6`	Configures an MPLS-TE tunnel interface and enables traffic engineering on a particular interface on the originating node.
Step 3	**path-option** *preference-priority* **dynamic** **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 10 dynamic`	Configures a secondary path option for an MPLS-TE tunnel.
Step 4	**commit**	
Step 5	**show mpls traffic-eng tunnels** [*tunnel-number*] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels 6`	Displays information about the secondary path option that on the tunnel-te interface for tunnel number 6.

Related Topics

Path Protection, on page 228
Pre-requisites for Path Protection, on page 229
Restrictions for Path Protection, on page 229
Configure Tunnels for Path Protection: Example, on page 396

Forcing a Manual Switchover on a Path-Protected Tunnel

Perform this task to force a manual switchover on a path-protected tunnel.

SUMMARY STEPS

1. **mpls traffic-eng path-protection switchover tunnel-te** *tunnel-ID*
2. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**mpls traffic-eng path-protection switchover tunnel-te** *tunnel-ID* **Example:** `RP/0/RSP0/CPU0:router# mpls traffic-eng path-protection switchover tunnel-te 6`	Forces the path protection switchover of the Point-to-Point (P2P) tunnel on the tunnel-te interface.
Step 2	**commit**	

Related Topics

Path Protection, on page 228
Pre-requisites for Path Protection, on page 229
Restrictions for Path Protection, on page 229
Configure Tunnels for Path Protection: Example, on page 396

Configuring the Delay the Tunnel Takes Before Reoptimization

Perform this task to configure the time between when a path-protection switchover event is effected on a tunnel head to when a reoptimization is performed on that tunnel. This timer affects only the required reoptimization that is attempted due to a switchover and does not override the global reoptimization timer.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **reoptimize timers delay path-protection** *seconds*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router# mpls traffic-eng`	Enters MPLS-TE configuration mode.

	Command or Action	Purpose
Step 3	**reoptimize timers delay path-protection** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# reoptimize timers delay path-protection 180`	Adjusts the number of seconds that the tunnel takes before triggering reoptimization after switchover has happened. **Note** The restriction is that at least one dynamic path-option must be configured for a standby LSP to come up. The strict (explicit) path option is not supported for the standby LSP.
Step 4	**commit**	

Related Topics

Path Protection, on page 228
Pre-requisites for Path Protection, on page 229
Restrictions for Path Protection, on page 229
Configure Tunnels for Path Protection: Example, on page 396

Configuring the Automatic Bandwidth

Perform these tasks to configure the automatic bandwidth:

Configuring the Collection Frequency

Perform this task to configure the collection frequency. You can configure only one global collection frequency.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **auto-bw collect frequency** *minutes*
4. **commit**
5. **show mpls traffic-eng tunnels** [**auto-bw**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**mpls traffic-eng**
	Example:
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`
	`RP/0/RSP0/CPU0:router(config-mpls-te)#`
		Enters MPLS-TE configuration mode.

	Command or Action	Purpose
Step 3	**auto-bw collect frequency** *minutes* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# auto-bw collect frequency 1`	Configures the automatic bandwidth collection frequency, and controls the manner in which the bandwidth for a tunnel collects output rate information; but does not adjust the tunnel bandwidth. ***minutes*** Configures the interval between automatic bandwidth adjustments in minutes. Range is from 1 to 10080.
Step 4	**commit**	
Step 5	**show mpls traffic-eng tunnels** [**auto-bw**] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic tunnels auto-bw`	Displays information about MPLS-TE tunnels for the automatic bandwidth. The globally configured collection frequency is displayed.

Related Topics

MPLS-TE Automatic Bandwidth Overview, on page 230
Configure Automatic Bandwidth: Example, on page 397

Forcing the Current Application Period to Expire Immediately

Perform this task to force the current application period to expire immediately on the specified tunnel. The highest bandwidth is applied on the tunnel before waiting for the application period to end on its own.

SUMMARY STEPS

1. **mpls traffic-eng auto-bw apply** {**all** | **tunnel-te** *tunnel-number*}
2. **commit**
3. **show mpls traffic-eng tunnels** [**auto-bw**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**mpls traffic-eng auto-bw apply** {**all**	**tunnel-te** *tunnel-number*} **Example:** `RP/0/RSP0/CPU0:router# mpls traffic-eng auto-bw apply tunnel-te 1`	Configures the highest bandwidth available on a tunnel without waiting for the current application period to end. **all** Configures the highest bandwidth available instantly on all the tunnels. **tunnel-te** Configures the highest bandwidth instantly to the specified tunnel. Range is from 0 to 65535.

	Command or Action	Purpose
Step 2	**commit**	
Step 3	**show mpls traffic-eng tunnels** [**auto-bw**] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels auto-bw`	Displays information about MPLS-TE tunnels for the automatic bandwidth.

Configuring the Automatic Bandwidth Functions

Perform this task to configure the following automatic bandwidth functions:

Application frequency

Configures the application frequency in which a tunnel bandwidth is updated by the automatic bandwidth.

Bandwidth collection

Configures only the bandwidth collection.

Bandwidth parameters

Configures the minimum and maximum automatic bandwidth to set on a tunnel.

Adjustment threshold

Configures the adjustment threshold for each tunnel.

Overflow detection

Configures the overflow detection for each tunnel.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **auto-bw**
4. **application** *minutes*
5. **bw-limit** {**min** *bandwidth* } {**max** *bandwidth*}
6. **adjustment-threshold** *percentage* [**min** *minimum-bandwidth*]
7. **overflow threshold** *percentage* [**min** *bandwidth*] **limit** *limit*
8. **commit**
9. **show mpls traffic-eng tunnels** [**auto-bw**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose

Step 2	**interface tunnel-te** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface tunnel-te 6`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Configures an MPLS-TE tunnel interface and enables traffic engineering on a particular interface on the originating node.

Step 3	**auto-bw**
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# auto-bw`
	`RP/0/RSP0/CPU0:router(config-if-tunte-autobw)#`
		Configures automatic bandwidth on a tunnel interface and enters MPLS-TE automatic bandwidth interface configuration mode.

Step 4	**application** *minutes* **Example:** `RP/0/RSP0/CPU0:router(config-if-tunte-autobw)# application 1000`	Configures the application frequency in minutes for the applicable tunnel. ***minutes*** Frequency in minutes for the automatic bandwidth application. Range is from 5 to 10080 (7 days). The default value is 1440 (24 hours).
Step 5	**bw-limit** {**min** *bandwidth* } {**max** *bandwidth*} **Example:** `RP/0/RSP0/CPU0:router(config-if-tunte-autobw)# bw-limit min 30 max 80`	Configures the minimum and maximum automatic bandwidth set on a tunnel. **min** Applies the minimum automatic bandwidth in kbps on a tunnel. Range is from 0 to 4294967295. **max** Applies the maximum automatic bandwidth in kbps on a tunnel. Range is from 0 to 4294967295.
Step 6	**adjustment-threshold** *percentage* [**min** *minimum-bandwidth*] **Example:** `RP/0/RSP0/CPU0:router(config-if-tunte-autobw)# adjustment-threshold 50 min 800`	Configures the tunnel bandwidth change threshold to trigger an adjustment. ***percentage*** Bandwidth change percent threshold to trigger an adjustment if the largest sample percentage is higher or lower than the current tunnel bandwidth. Range is from 1 to 100 percent. The default value is 5 percent. **min** Configures the bandwidth change value to trigger an adjustment. The tunnel bandwidth is changed only if the largest sample is higher or lower than the current tunnel bandwidth. Range is from 10 to 4294967295 kilobits per second (kbps). The default value is 10 kbps.

	Command or Action	Purpose
Step 7	**overflow threshold** *percentage* [**min** *bandwidth*] **limit** *limit* **Example:** `RP/0/RSP0/CPU0:router(config-if-tunte-autobw)# overflow threshold 100 limit 1`	Configures the tunnel overflow detection. ***percentage*** Bandwidth change percent to trigger an overflow. Range is from 1 to 100 percent. **limit** Configures the number of consecutive collection intervals that exceeds the threshold. The bandwidth overflow triggers an early tunnel bandwidth update. Range is from 1 to 10 collection periods. The default value is none. **min** Configures the bandwidth change value in kbps to trigger an overflow. Range is from 10 to 4294967295. The default value is 10.
Step 8	**commit**	
Step 9	**show mpls traffic-eng tunnels** [**auto-bw**] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels auto-bw`	Displays the MPLS-TE tunnel information only for tunnels in which the automatic bandwidth is enabled.

Related Topics

MPLS-TE Automatic Bandwidth Overview, on page 230
Configure Automatic Bandwidth: Example, on page 397

Configuring the Shared Risk Link Groups

To activate the MPLS traffic engineering SRLG feature, you must configure the SRLG value of each link that has a shared risk with another link.

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link

Perform this task to configure the SRLG value for each link that has a shared risk with another link.

Note You can configure up to 30 SRLGs per interface.

SUMMARY STEPS

1. **configure**
2. **srlg**

3. **interface** *type interface-path-id*
4. **value** *value*
5. **commit**
6. **show srlg interface** *type interface-path-id*
7. **show srlg**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**srlg** **Example:** `RP/0/RSP0/CPU0:router(config)# srlg`	Configures SRLG configuration commands on a specific interface configuration mode and assigns this SRLG a value.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-srlg)# interface POS 0/6/0/0`	Configures an interface type and path ID to be associated with an SRLG and enters SRLG interface configuration mode.

Step 4	**value** *value*
	Example:
	`RP/0/RSP0/CPU0:router(config-srlg-if)# value 100`
	`RP/0/RSP0/CPU0:router (config-srlg-if)# value 200`
	`RP/0/RSP0/CPU0:router(config-srlg-if)# value 300`
		Configures SRLG network values for a specific interface. Range is 0 to 4294967295.
		Note
		You can also set SRLG values on multiple interfaces including bundle interface.

Step 5	**commit**	
Step 6	**show srlg interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router# show srlg interface POS 0/6/0/0`	(Optional) Displays the SRLG values configured for a specific interface.
Step 7	**show srlg** **Example:** `RP/0/RSP0/CPU0:router# show srlg`	(Optional) Displays the SRLG values for all the configured interfaces. **Note** You can configure up to 250 interfaces.

Related Topics

MPLS Traffic Engineering Shared Risk Link Groups, on page 237
Explicit Path, on page 238
Fast ReRoute with SRLG Constraints, on page 239
Importance of Protection, on page 240
Delivery of Packets During a Failure, on page 241

Multiple Backup Tunnels Protecting the Same Interface, on page 241
Weighted-SRLG Auto-backup Path Computation, on page 241
SRLG Limitations, on page 242
MPLS TE SRLG Scale Enhancements, on page 242
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Creating an Explicit Path With Exclude SRLG

Perform this task to create an explicit path with the exclude SRLG option.

SUMMARY STEPS

1. **configure**
2. **explicit-path {identifier number [disable | index]}{ name** *explicit-path-name*}
3. **index 1 exclude-address** 192.168.92.1
4. **index 2 exclude-srlg** *192.168.92.2*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**explicit-path {identifier number [disable | index]}{ name** *explicit-path-name*} **Example:** `RP/0/RSP0/CPU0:router(config)# explicit-path name backup-srlg`	Enters the explicit path configuration mode. Identifer range is 1 to 65535.
Step 3	**index 1 exclude-address** 192.168.92.1 **Example:** `RP/0/RSP0/CPU0:router router(config-expl-path)# index 1 exclude-address 192.168.92.1`	Specifies the IP address to be excluded from the explicit path.
Step 4	**index 2 exclude-srlg** *192.168.92.2* **Example:** `RP/0/RSP0/CPU0:router(config-expl-path)# index 2 exclude-srlg 192.168.192.2`	Specifies the IP address to extract SRLGs to be excluded from the explicit path.
Step 5	**commit**	

Related Topics

MPLS Traffic Engineering Shared Risk Link Groups, on page 237
Explicit Path, on page 238
Fast ReRoute with SRLG Constraints, on page 239
Importance of Protection, on page 240

Delivery of Packets During a Failure, on page 241
Multiple Backup Tunnels Protecting the Same Interface, on page 241
Weighted-SRLG Auto-backup Path Computation, on page 241
SRLG Limitations, on page 242
MPLS TE SRLG Scale Enhancements, on page 242
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Using Explicit Path With Exclude SRLG

Perform this task to use an explicit path with the exclude SRLG option on the static backup tunnel.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **backup-path tunnel-te** *tunnel-number*
5. **exit**
6. **exit**
7. **interface tunnel-te***tunnel-id*
8. **ipv4 unnumbered** *type interface-path-id*
9. **path-option** *preference-priority*{ **dynamic** | **explicit {identifier** | **name** *explicit-path-name*}}
10. **destination** *ip-address*
11. **exit**
12. **commit**
13. **show run explicit-path name** *name*
14. **show mpls traffic-eng topology path destination** *name* **explicit-path** *name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# interface POS 0/6/0/0`	Enables traffic engineering on a specific interface on the originating node.
Step 4	**backup-path tunnel-te** *tunnel-number* **Example:**	Configures an MPLS TE backup path for a specific interface.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-mpls-te)# backup-path tunnel-te 2`	
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# exit`	Exits the current configuration mode.
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# exit`	Exits the current configuration mode.
Step 7	**interface tunnel-te***tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 2`	Configures an MPLS-TE tunnel interface.
Step 8	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered Loopback0`	Assigns a source address to set up forwarding on the new tunnel.
Step 9	**path-option** *preference-priority*{ **dynamic | explicit {identifier | name** *explicit-path-name*}} **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option l explicit name backup-srlg`	Sets the path option to explicit with a given name (previously configured) and assigns the path ID. **Note** You can use the dynamic option to dynamically assign a path.
Step 10	**destination** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-if)# destination 192.168.92.125`	Assigns a destination address on the new tunnel. • Destination address is the remote node's MPLS-TE router ID. • Destination address is the merge point between backup and protected tunnels. **Note** When you configure TE tunnel with multiple protection on its path and merge point is the same node for more than one protection, you must configure record-route for that tunnel.
Step 11	**exit** **Example:** RP/0/RSP0/CPU0:router(config-if)# exit	Exits the current configuration mode.
Step 12	**commit**	

	Command or Action	Purpose
Step 13	**show run explicit-path name** *name* **Example:** `RP/0/RSP0/CPU0:router# show run explicit-path name backup-srlg`	Displays the SRLG values that are configured for the link.
Step 14	**show mpls traffic-eng topology path destination** *name* **explicit-path** *name* **Example:** `RP/0/RSP0/CPU0:router#show mpls traffic-eng topology path destination 192.168.92.125 explicit-path backup-srlg`	Displays the SRLG values that are configured for the link.

Related Topics

MPLS Traffic Engineering Shared Risk Link Groups, on page 237
Explicit Path, on page 238
Fast ReRoute with SRLG Constraints, on page 239
Importance of Protection, on page 240
Delivery of Packets During a Failure, on page 241
Multiple Backup Tunnels Protecting the Same Interface, on page 241
Weighted-SRLG Auto-backup Path Computation, on page 241
SRLG Limitations, on page 242
MPLS TE SRLG Scale Enhancements, on page 242
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Creating a Link Protection on Backup Tunnel with SRLG Constraint

Perform this task to create an explicit path with the exclude SRLG option on the static backup tunnel.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **backup-path tunnel-te** *tunnel-number*
5. **exit**
6. **exit**
7. **interface tunnel-te***tunnel-id*
8. **ipv4 unnumbered** *type interface-path-id*
9. **path-option** *preference-priority*{ **dynamic** | **explicit {identifier** | **name** *explicit-path-name*}}
10. **destination** *ip-address*
11. **exit**
12. **explicit-path {identifier number [disable** | **index]}{ name** *explicit-path-name*}
13. **index 1 exclude-srlg** 192.168.92.2
14. **commit**
15. **show mpls traffic-eng tunnels***tunnel-number* **detail**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# interface POS 0/6/0/0`	Enables traffic engineering on a particular interface on the originating node.
Step 4	**backup-path tunnel-te** *tunnel-number* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# backup-path tunnel-te 2`	Sets the backup path to the primary tunnel outgoing interface.
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# exit`	Exits the current configuration mode.
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# exit`	Exits the current configuration mode.
Step 7	**interface tunnel-te***tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 2`	Configures an MPLS-TE tunnel interface.
Step 8	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered Loopback0`	Assigns a source address to set up forwarding on the new tunnel.
Step 9	**path-option** *preference-priority*{ **dynamic | explicit {identifier | name** *explicit-path-name*}} **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 1 explicit name backup-srlg`	Sets the path option to explicit with a given name (previously configured) and assigns the path ID. Identifier range is from 1 to 4294967295. **Note** You can use the dynamic option to dynamically assign a path.
Step 10	**destination** *ip-address*	Assigns a destination address on the new tunnel.

	Command or Action	Purpose
	Example: `RP/0/RSP0/CPU0:router(config-if)# destination 192.168.92.125`	• Destination address is the remote node's MPLS-TE router ID. • Destination address is the merge point between backup and protected tunnels. **Note** When you configure TE tunnel with multiple protection on its path and merge point is the same node for more than one protection, you must configure record-route for that tunnel.
Step 11	**exit** **Example:** RP/0/RSP0/CPU0:router(config-if)# exit	Exits the current configuration mode.
Step 12	**explicit-path {identifier number [disable | index]}{ name** *explicit-path-name*} **Example:** `RP/0/RSP0/CPU0:router(config)# explicit-path name backup-srlg-nodep`	Enters the explicit path configuration mode. Identifer range is 1 to 65535.
Step 13	**index 1 exclude-srlg** 192.168.92.2 **Example:** `RP/0/RSP0/CPU0:router:router(config-if)# index 1 exclude-srlg 192.168.192.2`	Specifies the protected link IP address to get SRLGs to be excluded from the explicit path.
Step 14	**commit**	
Step 15	**show mpls traffic-eng tunnels***tunnel-number* **detail** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels 2 detail`	Display the tunnel details with SRLG values that are configured for the link.

Related Topics

MPLS Traffic Engineering Shared Risk Link Groups, on page 237
Explicit Path, on page 238
Fast ReRoute with SRLG Constraints, on page 239
Importance of Protection, on page 240
Delivery of Packets During a Failure, on page 241
Multiple Backup Tunnels Protecting the Same Interface, on page 241
Weighted-SRLG Auto-backup Path Computation, on page 241
SRLG Limitations, on page 242
MPLS TE SRLG Scale Enhancements, on page 242
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Creating a Node Protection on Backup Tunnel with SRLG Constraint

Perform this task to configure node protection on backup tunnel with SRLG constraint.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **backup-path tunnel-te** *tunnel-number*
5. **exit**
6. **exit**
7. **interface tunnel-te***tunnel-id*
8. **ipv4 unnumbered** *type interface-path-id*
9. **path-option** *preference-priority*{ **dynamic | explicit {identifier | name** *explicit-path-name*}}
10. **destination** *ip-address*
11. **exit**
12. **explicit-path {identifier number [disable | index]}{ name** *explicit-path-name*}
13. **index 1 exclude-address** 192.168.92.1
14. **index 2 exclude-srlg** *192.168.92.2*
15. **commit**
16. **show mpls traffic-eng tunnels topology path destination** *ip-address* **explicit-path-name** *name*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# interface POS 0/6/0/0`	Enables traffic engineering on a particular interface on the originating node.
Step 4	**backup-path tunnel-te** *tunnel-number* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# backup-path tunnel-te 2`	Sets the backup path for the primary tunnel outgoing interface.
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# exit`	Exits the current configuration mode.

	Command or Action	Purpose
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# exit`	Exits the current configuration mode.
Step 7	**interface tunnel-te***tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-te 2`	Configures an MPLS-TE tunnel interface.
Step 8	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered Loopback0`	Assigns a source address to set up forwarding on the new tunnel.
Step 9	**path-option** *preference-priority*{ **dynamic | explicit {identifier | name** *explicit-path-name*}} **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 1 explicit name backup-srlg`	Sets the path option to explicit with a given name (previously configured) and assigns the path ID. Identifier range is 1 to 4294967295. **Note** You can use the dynamic option to dynamically assign path.
Step 10	**destination** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-if)# destination 192.168.92.125`	Assigns a destination address on the new tunnel. • Destination address is the remote node's MPLS-TE router ID. • Destination address is the merge point between backup and protected tunnels. **Note** When you configure TE tunnel with multiple protection on its path and merge point is the same node for more than one protection, you must configure record-route for that tunnel.
Step 11	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if)# exit`	Exits the current configuration mode.
Step 12	**explicit-path {identifier number [disable | index]}{ name** *explicit-path-name*} **Example:** `RP/0/RSP0/CPU0:router(config)# explicit-path name backup-srlg-nodep`	Enters the explicit path configuration mode. Identifer range is 1 to 65535.
Step 13	**index 1 exclude-address** 192.168.92.1 **Example:**	Specifies the protected node IP address to be excluded from the explicit path.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router:router(config-if)# index 1 exclude-address 192.168.92.1`	
Step 14	**index 2 exclude-srlg** *192.168.92.2* **Example:** `RP/0/RSP0/CPU0:router(config-if)# index 2 exclude-srlg 192.168.192.2`	Specifies the protected link IP address to get SRLGs to be excluded from the explicit path.
Step 15	**commit**	
Step 16	**show mpls traffic-eng tunnels topology path destination** *ip-address* **explicit-path-name** *name* **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels topology path destination 192.168.92.125 explicit-path-name backup-srlg-nodep`	Displays the path to the destination with the constraint specified in the explicit path.

Related Topics

MPLS Traffic Engineering Shared Risk Link Groups, on page 237
Explicit Path, on page 238
Fast ReRoute with SRLG Constraints, on page 239
Importance of Protection, on page 240
Delivery of Packets During a Failure, on page 241
Multiple Backup Tunnels Protecting the Same Interface, on page 241
Weighted-SRLG Auto-backup Path Computation, on page 241
SRLG Limitations, on page 242
MPLS TE SRLG Scale Enhancements, on page 242
Configure the MPLS-TE Shared Risk Link Groups: Example, on page 397

Configuring Default Admin Weight

Perform this task to configure a default admin weight to apply to all SRLG values if a specific admin weight is not configured under the SRLG value configuration mode.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng srlg**
3. **admin-weight** *weight*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**mpls traffic-eng srlg** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng srlg`	Enters MPLS TE SRLG configuration mode.
Step 3	**admin-weight** *weight* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-srlg)# admin-weight 10`	Configures default admin-weight for all the SRLG values. Range is from 0-4294967295. Default is 1. The example shows how to configure an admin-weight of 10 for all the SRLG values.
Step 4	**commit**	

Configuring Static SRLG Value to Topology Link

Perform this task to assign static SRLG value to a topology link based on its IP address. Use this command for platforms that do not support SRLG flooding, so that the local node auto-tunnel backup diverse path calculation is based on static SRLG.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng srlg**
3. **value** *srlg-value*
4. **static ipv4 address** *ip-address* **next-hop ipv4 address** *next-hop-ip-address*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng srlg** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng srlg`	Enters MPLS TE SRLG configuration mode.
Step 3	**value** *srlg-value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-srlg)# value 5`	Enters MPLS TE SRLG value configuration mode and configures SRLG value. The example shows how to enter MPLS TE SRLG value configuration mode and configure a SRLG value of 5.
Step 4	**static ipv4 address** *ip-address* **next-hop ipv4 address** *next-hop-ip-address* **Example:**	Configures static SRLG value to a topology link. The example shows how to configure static SRLG value for a topology link with source IP address of 10.0.0.1 and next-hop IP address of 10.1.1.2.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-mpls-te-srlg)# static ipv4 address 10.0.0.1 next-hop ipv4 address 10.1.1.2`	
Step 5	**commit**	

Configuring Admin-Weight Associated with an SRLG Value

Perform this task to configure admin-weight associated with an SRLG value. This admin-weight will be added to the link admin weight during SRLG aware path calculation when the link matches the SRLG value of the protected link. The admin-weight configured in the MPLS TE SRLG value configuration mode overwrites the admin-weight configured in the MPLS TE SRLG configuration mode.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng srlg**
3. **value** *srlg-value*
4. **admin-weight** *weight*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng srlg** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng srlg`	Enters MPLS TE SRLG configuration mode.
Step 3	**value** *srlg-value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-srlg)# value 150`	Enters MPLS TE SRLG value configuration mode and configures SRLG value. The example shows how to enter MPLS TE SRLG value configuration mode and configure a SRLG value of 150.
Step 4	**admin-weight** *weight* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-srlg)# admin-weight 100`	Configures admin-weight for SRLG value. Range is from 0-4294967295. Default is 1. The example shows how to configure an admin-weight of 100 for the SRLG value of 150.
Step 5	**commit**	

Configuring Point-to-Multipoint TE

You must enable multicast routing on the edge router before performing Point-to-Multipoint (P2MP) TE configurations. To configure Point-to-Multipoint TE, perform these procedures:

Enabling Multicast Routing on the Router

Perform this task to enable multicast routing on the router to configure P2MP tunnels.

Before you begin

- To configure Point-to-Multipoint (P2MP) tunnels, you must enable multicast routing on the router.
- The customer-facing interface must enable multicast.

SUMMARY STEPS

1. **configure**
2. **multicast-routing**
3. **address-family** {**ipv4** | **ipv6** }
4. **interface tunnel-mte** *tunnel-id*
5. **enable**
6. **exit**
7. **interface** *type interface-path-id*
8. **enable**
9. **commit**
10. **show pim ipv6 interface** *type interface-path-id*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**multicast-routing**
	Example:
	`RP/0/RSP0/CPU0:router(config)# multicast-routing`
	`RP/0/RSP0/CPU0:router(config-mcast)#`
		Enters multicast routing configuration mode.

Step 3	**address-family** {**ipv4**	**ipv6** }
		Example:
		`RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv6`
		`RP/0/RSP0/CPU0:router(config-mcast-default-ipv6)#`
			Configures the available IPv4 or IPv6 address prefixes to enable multicast routing and forwarding on all router interfaces.

	Command or Action	Purpose

Step 4	**interface tunnel-mte** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-mcast-default-ipv6)# interface tunnel-mte 1`
	`RP/0/RSP0/CPU0:router(config-mcast-default-ipv6-if)#`
		Configures an MPLS-TE P2MP tunnel interface.

Step 5	**enable** **Example:** `RP/0/RSP0/CPU0:router(config-mcast-default-ipv6-if)# enable`	Enables multicast routing on the tunnel-mte interface.

Step 6	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-mcast-default-ipv6-if)# exit`
	`RP/0/RSP0/CPU0:router(config-mcast-default-ipv6)#`
		Exits the current configuration mode.

Step 7	**interface** *type interface-path-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-mcast-default-ipv6)# interface GigabitEthernet0/2/0/3`
	`RP/0/RSP0/CPU0:router(config-mcast-default-ipv6-if)#`
		Configures multicast routing on the GigabitEthernet interface.

Step 8	**enable** **Example:** `RP/0/RSP0/CPU0:router(config-mcast-default-ipv6-if)# enable`	Enables multicast routing on the GigabitEthernet interface.
Step 9	**commit**	
Step 10	**show pim ipv6 interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router# show pim ipv6 interface tunnel-mte 1`	Displays the output for the P2MP-TE tunnel interface that has IPv6 multicast enabled.

Related Topics

Configuring the Static Group for the Point-to-Multipoint Interface, on page 328

Configuring the Static Group for the Point-to-Multipoint Interface

Perform this task to configure the static group on the Point-to-Multipoint (P2MP) interface to forward specified multicast traffic over P2MP LSP.

SUMMARY STEPS

1. **configure**
2. **router mld**
3. **vrf** *vrf-name*
4. **interface tunnel-mte** *tunnel-id*
5. **static-group** *group-address*
6. **commit**
7. **show mrib ipv6 route** *source-address*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**router mld**
	Example:
	`RP/0/RSP0/CPU0:router(config)# router mld`
	`RP/0/RSP0/CPU0:router(config-mld)#`
		Enters router MLD configuration mode.

Step 3	**vrf** *vrf-name*
	Example:
	`RP/0/RSP0/CPU0:router(config-mld)#vrf default`
	`RP/0/RSP0/CPU0:router(config-mld-default)#`
		Configures a virtual private network (VRF) instance.

Step 4	**interface tunnel-mte** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config-mld-default)#interface tunnel-mte 1`
	`RP/0/RSP0/CPU0:router(config-mld-default-if)#`
		Configures an MPLS-TE P2MP tunnel interface.

	Command or Action	Purpose
Step 5	**static-group** *group-address* **Example:** `RP/0/RSP0/CPU0:router(config-mld-default-if)# static-group ff35::1 2000::1`	Configures the multicast group address in the Source-Specific Multicast (SSM) address range (ff35::/16) for the IPv6 address prefix.
Step 6	**commit**	
Step 7	**show mrib ipv6 route** *source-address* **Example:** `RP/0/RSP0/CPU0:router# show mrib ipv6 route ff35::1`	Verifies the multicast static mapping.

Related Topics

Enabling Multicast Routing on the Router, on page 326

Configuring Destinations for the Tunnel Interface

Perform this task to configure three destinations for the tunnel interface for Point-to-Multipoint (P2MP).

These variations are listed to ensure that the destination and path option configurations are separate from the tunnel interface.

- Different path option is used for different destinations. This task shows three destinations.
- Explicit path option is based on an ID or a name.
- Default path option is similar to the Point-to-Point (P2P) LSP.

Before you begin

These prerequisites are required to configure destinations for the tunnel interface.

- Multicast routing must be enabled on both the tunnel-mte interface and customer-facing interface from the source.
- Static-group must be configured on the tunnel-mte interface to forward specified multicast traffic over P2MP LSP.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-mte** *tunnel-id*
3. **destination** *ip-address*
4. **path-option** *preference-priority* **explicit identifier** *path-number*
5. **path-option** *preference-priority* **dynamic**
6. **exit**
7. **destination** *ip-address*
8. **path-option** *preference-priority* **explicit name** *pathname*

9. **path-option** *preference-priority* **dynamic**
10. **exit**
11. **destination** *ip-address*
12. **path-option** *preference-priority* **explicit name** *pathname* [**verbatim**]
13. **commit**
14. **show mpls traffic-eng tunnels** [**brief**] [**p2mp** *tunnel-number*]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**interface tunnel-mte** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface tunnel-mte 10`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Configures an MPLS-TE P2MP tunnel interface.

Step 3	**destination** *ip-address*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# destination 172.16.255.1`
	`RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#`
		Sets the destination address for tunnel-mte 10 to 172.16.255.1. This destination uses the explicit path identified by explicit path ID 10. If destination 172.16.255.1 cannot come with explicit path ID 10, the fall back path option is dynamic.

Step 4	**path-option** *preference-priority* **explicit identifier** *path-number* **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# path-option 1 explicit identifier 10`	Configures the path number of the IP explicit path.
Step 5	**path-option** *preference-priority* **dynamic** **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# path-option 2 dynamic`	Specifies that label switched paths (LSP) are dynamically calculated.
Step 6	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# exit`	Exits the current configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-if)#`	

Step 7	**destination** *ip-address*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# destination 172.16.255.2`
	`RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#`
		Sets the destination address for tunnel-mte 10 to 172.16.255.2.

Step 8	**path-option** *preference-priority* **explicit name** *pathname* **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# path-option 1 explicit name how-to-get-to-172.16.255.2`	Specifies the path name of the IP explicit path. Destination 172.16.255.2 uses the explicit path that is identified by the explicit path name "how-to-get-to-172.16.255.2."
Step 9	**path-option** *preference-priority* **dynamic** **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# path-option 2 dynamic`	Sets the fall back path option as dynamic when the destination cannot come to the explicit path.

Step 10	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# exit`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Exits the current configuration mode.

Step 11	**destination** *ip-address*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# destination 172.16.255.3`
	`RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#`
		Specifies that destination 172.16.255.3 uses only the dynamically computed path.

Step 12	**path-option** *preference-priority* **explicit name** *pathname* [**verbatim**] **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# path-option 1 explicit name how-to-get-to-172.16.255.3 verbatim`	Specifies that destination 172.16.255.3 uses the explicit path identified by the explicit path name "how-to-get-to-172.16.255.3" in verbatim mode.
Step 13	**commit**	

	Command or Action	Purpose
Step 14	**show mpls traffic-eng tunnels** [**brief**] [**p2mp** *tunnel-number*] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels brief p2mp 10`	Displays the brief summary of the P2MP tunnel status and configuration.

Related Topics

Enabling Multicast Routing on the Router, on page 326
Configuring the Static Group for the Point-to-Multipoint Interface, on page 328

Disabling Destinations

Perform this task to disable the given destination for the Point-to-Multipoint (P2MP) tunnel interface.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-mte** *tunnel-id*
3. **ipv4 unnumbered** *type interface-path-id*
4. **destination** *ip-address*
5. **disable**
6. **path-option** *preference-priority* **dynamic**
7. **path-option** *preference-priority* **explicit name** *pathname*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**interface tunnel-mte** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface tunnel-mte 101`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Configures an MPLS-TE P2MP tunnel interface.

Step 3	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered`	Assigns a source address so that forwarding can be performed on the new tunnel. Loopback is commonly used as the interface type.

	Command or Action	Purpose
	`Loopback0`	

Step 4	**destination** *ip-address*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# destination 140.140.140.140`
	`RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#`
		Sets the destination address for tunnel-mte 10 to 140.140.140.140.

Step 5	**disable** **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#disable`	Disables destination 140.140.140.140 for tunnel-mte 10.
Step 6	**path-option** *preference-priority* **dynamic** **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#path-option 1 dynamic`	Specifies that label switched paths (LSP) are dynamically calculated.
Step 7	**path-option** *preference-priority* **explicit name** *pathname* **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#path-option 2 explicit name to4`	Specifies that destination 140.140.140.140 uses the explicit path identified by the explicit path name "to4."
Step 8	**commit**	

Logging Per Destinations for Point-to-Multipoint

Perform this task to log destinations for Point-to-Multipoint (P2MP).

SUMMARY STEPS

1. **configure**
2. **interface tunnel-mte** *tunnel-id*
3. **ipv4 unnumbered** *type interface-path-id*
4. **destination** *ip-address*
5. **logging events lsp-status state**
6. **logging events lsp-status reroute**
7. **path-option** *preference-priority* **explicit name** *pathname*
8. **exit**
9. **fast-reroute**
10. **commit**

11. **show mpls traffic-eng tunnels** [**p2mp**]

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**interface tunnel-mte** *tunnel-id*
	Example:
	`RP/0/RSP0/CPU0:router(config)# interface tunnel-mte 1000`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Configures an MPLS-TE P2MP tunnel interface.

Step 3	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered loopback0`	Configures the MPLS-TE tunnel to use the IPv4 address on loopback interface 0.

Step 4	**destination** *ip-address*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)# destination 100.0.0.3`
	`RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#`
		Sets the destination address for tunnel-mte from 1000 to 100.0.0.3.

Step 5	**logging events lsp-status state** **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# logging events lsp-status state`	Sends out the log message when the tunnel LSP goes up or down when the software is enabled.
Step 6	**logging events lsp-status reroute** **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# logging events lsp-status reroute`	Sends out the log message when the tunnel LSP is rerouted due to an FRR event when the software is enabled.
Step 7	**path-option** *preference-priority* **explicit name** *pathname* **Example:** `RP/0/RSP0/CPU0:router(config-if-p2mp-dest)#`	Specifies the path name of the IP explicit path. Destination 100.0.0.3 uses the explicit path that is identified by the explicit path name "path123."

	Command or Action	Purpose
	`path-option 1 explicit name path123`	

Step 8	**exit**
	Example:
	`RP/0/RSP0/CPU0:router(config-if-p2mp-dest)# exit`
	`RP/0/RSP0/CPU0:router(config-if)#`
		Exits the current configuration mode.

Step 9	**fast-reroute** **Example:** `RP/0/RSP0/CPU0:router(config-if)# fast-reroute`	Enables fast-reroute (FRR) protection for a P2MP TE tunnel.
Step 10	**commit**	
Step 11	**show mpls traffic-eng tunnels** [**p2mp**] **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels p2mp`	Displays the information for all P2MP tunnels.

Enabling Soft-Preemption on a Node

Perform this task to enable the soft-preemption feature in the MPLS TE configuration mode. By default, this feature is disabled. You can configure the soft-preemption feature for each node. It has to be explicitly enabled for each node.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **soft-preemption**
4. **timeout** *seconds*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:**	Enters MPLS-TE configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	
Step 3	**soft-preemption** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# soft-preemption`	Enables soft-preemption on a node. **Note** If soft-preemption is enabled, the head-end node tracks whether an LSP desires the soft-preemption treatment. However, when a soft-preemption feature is disabled on a node, this node continues to track all LSPs desiring soft-preemption. This is needed in a case when soft-preemption is re-enabled, TE will have the property of the existing LSPs without any re-signaling.
Step 4	**timeout** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-soft-preemption)# timeout 20`	Specifies the timeout for the soft-preempted LSP, in seconds. The range is from 1 to 300.
Step 5	**commit**	

Related Topics

Soft-Preemption, on page 242

Enabling Soft-Preemption on a Tunnel

Perform this task to enable the soft-preemption feature on a MPLS TE tunnel. By default, this feature is disabled. It has to be explicitly enabled.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **soft-preemption**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router# interface tunnel-te 10`	Configures an MPLS-TE tunnel interface.
Step 3	**soft-preemption**	Enables soft-preemption on a tunnel.

	Command or Action	Purpose
	Example: `RP/0/RSP0/CPU0:router(config-if)# soft-preemption`	When soft preemption is enabled on a tunnel, these actions occur: • A path-modify message is sent for the current LSP with the **soft preemption desired** property. • A path-modify message is sent for the reopt LSP with the **soft preemption desired** property. • A path-modify message is sent for the path protection LSP with the **soft preemption desired** property. • A path-modify message is sent for the current LSP in FRR active state with the **soft preemption desired** property. **Note** The soft-preemption is not available in the interface tunnel-mte and interface tunnel-gte configuration modes.
Step 4	**commit**	

Related Topics

Soft-Preemption, on page 242

Configuring Attributes within a Path-Option Attribute

Perform this task to configure attributes within a path option attribute-set template.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **attribute-set path-option** *attribute-set-name*
4. **affinity** *affinity-value* **mask** *mask-value*
5. **signalled-bandwidth** *kbps* **class-type** *class-type number*
6. **commit**
7. **show mpls traffic-eng attribute-set**
8. **show mpls traffic-eng tunnels***detail*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**attribute-set path-option** *attribute-set-name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# attribute-set path-option myset`	Enters attribute-set path option configuration mode. **Note** The configuration at the **path-option** level takes precedence over the values configured at the level of the tunnel, and therefore is applied.
Step 4	**affinity** *affinity-value* **mask** *mask-value* **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# affinity 0xBEEF mask 0xBEEF`	Configures affinity attribute under a path option attribute-set. The attribute values that are required for links to carry this tunnel.
Step 5	**signalled-bandwidth** *kbps* **class-type** *class-type number* **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# signalled-bandwidth 1000 class-type 0`	Configures the bandwidth attribute required for an MPLS-TE tunnel under a path option attribute-set. **Note** You can configure the class type of the tunnel bandwidth request. The class-type 0 is strictly equivalent to **global-pool** and class-type 1 is strictly equivalent to **subpool.**
Step 6	**commit**	
Step 7	**show mpls traffic-eng attribute-set** **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng attribute-set`	Displays the attributes that are defined in the attribute-set for the link.
Step 8	**show mpls traffic-eng tunnels***detail* **Example:** `RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels detail`	Displays the attribute-set path option information on a specific tunnel.

Related Topics

Path Option Attributes, on page 243
Configuration Hierarchy of Path Option Attributes, on page 243
Traffic Engineering Bandwidth and Bandwidth Pools, on page 244
Path Option Switchover, on page 244
Path Option and Path Protection, on page 245

Configuring Auto-Tunnel Mesh Tunnel ID

Perform this activity to configure the tunnel ID range that can be allocated to Auto-tunnel mesh tunnels.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **auto-tunnel mesh**
4. **tunnel-id min** *value* **max** *value*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS TE configuration mode.
Step 3	**auto-tunnel mesh** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# auto-tunnel mesh`	Enters auto-tunnel mesh configuration mode. You can configure auto-tunnel mesh related options from this mode.
Step 4	**tunnel-id min** *value* **max** *value* **Example:** `RP/0/RSP0/CPU0:router(config-te-auto-mesh)# tunnel-id min 10 max 50`	Specifies the minimum and maximum number of auto-tunnel mesh tunnels that can be created on this router. The range of tunnel ID is from 0 to 65535.
Step 5	**commit**	

Related Topics

Auto-Tunnel Mesh, on page 245
Destination List (Prefix-List), on page 246

Configuring Auto-tunnel Mesh Unused Timeout

Perform this task to configure a global timer to remove unused auto-mesh tunnels.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **auto-tunnel mesh**
4. **timer removal unused** *timeout*

5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**auto-tunnel mesh** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# auto-tunnel mesh`	Enables auto-tunnel mesh groups globally.
Step 4	**timer removal unused** *timeout* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-auto-mesh)# timers removal unused 10`	Specifies a timer, in minutes, after which a down auto-tunnel mesh gets deleted whose destination was not in TE topology. The default value for this timer is 60. The timer gets started when these conditions are met: • Tunnel destination node is removed from the topology • Tunnel is in down state **Note** The unused timer runs per tunnel because the same destination in different mesh-groups may have different tunnels created.
Step 5	**commit**	

Related Topics

Auto-Tunnel Mesh, on page 245
Destination List (Prefix-List), on page 246

Configuring Auto-Tunnel Mesh Group

Perform this task to configure an auto-tunnel mesh group globally on the router.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **auto-tunnel mesh**

4. **group** *value*
5. **disable**
6. **attribute-set***name*
7. **destination-list**
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**auto-tunnel mesh** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# auto-tunnel mesh`	Enables auto-tunnel mesh groups globally.
Step 4	**group** *value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-auto-mesh)# group 65`	Specifies the membership of auto-tunnel mesh. The range is from 0 to 4294967295. **Note** When the destination-list is not supplied, head-end will automatically build destination list belonging for the given mesh-group membership using TE topology.
Step 5	**disable** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-auto-mesh-group)# disable`	Disables the meshgroup and deletes all tunnels created for this meshgroup.
Step 6	**attribute-set***name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-auto-mesh-group)# attribute-set am-65`	Specifies the attributes used for all tunnels created for the meshgroup. If it is not defined, this meshgroup does not create any tunnel.
Step 7	**destination-list** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-auto-mesh-group)# destination-list dl-65`	This is a mandatory configuration under a meshgroup. If a given destination-list is not defined as a prefix-list, this meshgroup create tunnels to all nodes available in TE topology.

	Command or Action	Purpose
Step 8	**commit**	

Related Topics

Auto-Tunnel Mesh, on page 245
Destination List (Prefix-List), on page 246

Configuring Tunnel Attribute-Set Templates

Perform this task to define attribute-set templates for auto-mesh tunnels.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **attribute-set auto-mesh** *attribute-set-name*
4. **affinity** *value* **mask** *mask-value*
5. **signalled-bandwidth** *kbps* **class-type** *class-type number*
6. **autoroute announce**
7. **fast-reroute protect bandwidth node**
8. **auto-bw collect-bw-only**
9. **logging events lsp-status {state | insufficient-bandwidth | reoptimize | reroute** }
10. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**attribute-set auto-mesh** *attribute-set-name* **Example:** `RP/0/RSP0/CPU0:router(config-te)# attribute-set auto-mesh attribute-set-mesh`	Specifies name of the attribute-set of auto-mesh type.
Step 4	**affinity** *value* **mask** *mask-value* **Example:** `RP/0/RSP0/CPU0:router(config-te)# affinity 0101 mask 320`	Configures the affinity properties the tunnel requires in its links for an MPLS-TE tunnel under an auto-mesh attribute-set.

	Command or Action	Purpose
Step 5	**signalled-bandwidth** *kbps* **class-type** *class-type number* **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# signalled-bandwidth 1000 class-type 0`	Configures the bandwidth attribute required for an MPLS-TE tunnel under an auto-mesh attribute-set. Because the default tunnel priority is 7, tunnels use the default TE class map (namely, class-type 0, priority 7). **Note** You can configure the class type of the tunnel bandwidth request. The class-type 0 is strictly equivalent to **global-pool** and class-type 1 is strictly equivalent to **subpool**.
Step 6	**autoroute announce** **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# autoroute announce`	Enables parameters for IGP routing over tunnel.
Step 7	**fast-reroute protect bandwidth node** **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# fast-reroute`	Enables fast-reroute bandwidth protection and node protection for auto-mesh tunnels.
Step 8	**auto-bw collect-bw-only** **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# auto-bw collect-bw-only`	Enables automatic bandwidth collection frequency, and controls the manner in which the bandwidth for a tunnel collects output rate information, but does not adjust the tunnel bandwidth.
Step 9	**logging events lsp-status {state | insufficient-bandwidth | reoptimize | reroute** } **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# logging events lsp-status state`	Sends out the log message when the tunnel LSP goes up or down when the software is enabled. Sends out the log message when the tunnel LSP undergoes setup or reoptimize failure due to bandwidth issues. Sends out the log message for the LSP reoptimize change alarms. Sends out the log message for the LSP reroute change alarms.
Step 10	**commit**	

Related Topics

Auto-Tunnel Mesh, on page 245
Destination List (Prefix-List), on page 246

Enabling LDP on Auto-Tunnel Mesh

Perform this task to enable LDP on auto-tunnel mesh group.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **traffic-eng auto-tunnel mesh**
4. **group***id***all**
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls ldp** **Example:** `RP/0/RSP0/CPU0:router(config-ldp)# mpls ldp`	Enters MPLS LDP configuration mode.
Step 3	**traffic-eng auto-tunnel mesh** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-te-auto-mesh)# traffic-eng auto-tunnel mesh`	Enters auto-tunnel mesh configuration mode. You can configure TE auto-tunnel mesh groups from this mode.
Step 4	**group***id***all** **Example:** `RP/0/RSP0/CPU0:router(config-ldp-te-auto-mesh)# group all`	Configures an auto-tunnel mesh group of interfaces in LDP. You can enable LDP on all TE meshgroup interfaces or you can specify the TE mesh group ID on which the LDP is enabled. The range of group ID is from 0 to 4294967295.
Step 5	**commit**	

Related Topics

Auto-Tunnel Mesh, on page 245
Destination List (Prefix-List), on page 246

Configuring P2MP TE Auto-tunnels

Perform these tasks to enable P2MP TE Auto-tunnels. These steps configure the tunnel ID range to be allocated to P2MP auto-tunnels and determine the maximum number of P2MP auto-tunnels that can be created.

Before you begin

The P2MP TE Auto-tunnel configuration is disabled by default.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **auto-tunnel p2mp**
4. **tunnel-id min** *number* **max** *value*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)#mpls traffic-eng`	Enables MPLS traffic engineering (TE) configuration mode.
Step 3	**auto-tunnel p2mp** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)#auto-tunnel p2mp`	Enables automatically created tunnel configuration and enters the auto-tunnel P2MP configuration mode.
Step 4	**tunnel-id min** *number* **max** *value* **Example:** `RP/0/RSP0/CPU0:router(config-te-auto-p2mp)#tunnel-id min 10000 max 11000`	Configures the tunnel ID range that can be allocated to P2MP auto-tunnels and determines the maximum number of P2MP auto-tunnels that can be created.
Step 5	**commit**	

Related Topics

P2MP-TE Auto-tunnels, on page 246

Enabling Stateful PCE Client

Perform these steps to enable stateful PCE client.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **pce**
4. **stateful-client**
5. **capabilities** { **instantiation** | **update** }
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)#mpls traffic-eng`	Enters MPLS TE configuration mode.
Step 3	**pce** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)#pce`	Enters PCE configuration mode.
Step 4	**stateful-client** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-pce)#stateful-client`	Enters stateful PCE client configuration mode. When the stateful-client configuration is added to the node, it will close all existing PCEP peer connections, and add the stateful capabilities TLV to the OPEN object it exchanges during the PCEP session establishment. When the stateful-client configuration is removed from the node, it will delete all PCE instantiated tunnels, close all existing PCEP connections, and no longer add the stateful capabilities TLV to the OPEN object it exchanges during the PCEP session establishment.
Step 5	**capabilities** { **instantiation** | **update** } **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-pce-stateful)#capabilities instantiation`	Enables stateful client capabilities. • **instantiation**—enables stateful instantiate capability • **update**—enables stateful update capability
Step 6	**commit**	

Configuring VRF Redirection

Perform these steps to configure VRF redirection by installing multiple routes in the routing information base (RIB) per MPLS TE tunnel:

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **autoroute destination** *ip-address*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)#interface tunnel-te 10`	Configures an MPLS-TE tunnel interface.

Step 3	**autoroute destination** *ip-address*
	Example:
	`RP/0/RSP0/CPU0:router(config-if)#autoroute destination 192.168.1.2`
	`RP/0/RSP0/CPU0:router(config-if)#autoroute destination 192.168.2.2`
	`RP/0/RSP0/CPU0:router(config-if)#autoroute destination 192.168.3.2`
	`RP/0/RSP0/CPU0:router(config-if)#autoroute destination 192.168.4.2`
		Adds a route (ip-address) in RIB with TE tunnel as outgoing interface. to the tunnel destination.

Step 4	**commit**	

Example

This example shows how to configure installing four autoroute destination routes into the RIB along with the default route:

```
interface tunnel-te10
 autoroute destination 192.168.1.2
 autoroute destination 192.168.2.2
 autoroute destination 192.168.3.2
 autoroute destination 192.168.4.2
```

Configure IPv6 routing over IPv4 MPLS-TE tunnels

Perform these steps to configure IPv6 routing over IPv4 MPLS-TE tunnels:

Procedure

Step 1 **configure**

Step 2 **interface tunnel-te** *tunnel-id*

Example:

```
RP/0/RSP0/CPU0:router# interface tunnel-te 1
```

Configures an MPLS-TE tunnel interface.

Step 3 **ipv4 unnumbered** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-if)#ipv4 unnumbered Loopback 0
```

Assigns a source address so that forwarding can be performed on the new tunnel. Loopback is the commonly-used interface type.

Step 4 **ipv6 enable**

Example:

```
RP/0/RSP0/CPU0:router(config-if)#ipv6 enable
```

Enables IPv6 on interface.

Step 5 **signalled-bandwidth** *bandwidth*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# signalled-bandwidth 10
```

Sets the tunnel bandwidth requirement to be signalled in Kbps.

Step 6 **destination** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-if)#destination 192.168.0.1
```

Specifies the IPv4 destination address.

Step 7 Use one of these options:

- **autoroute announce include-ipv6**
- **forwarding-adjacency include-ipv6**

Example:

```
RP/0/RSP0/CPU0:router(config-if)#autoroute announce include-ipv6
```

Or

```
RP/0/RSP0/CPU0:router(config-if)#forwarding-adjacency include-ipv6
```

Announces the tunnel as an IPv6 autoroute or an IPv6 forwarding adjacency.

Step 8 **path-option** *preference-priority* **dynamic**

Example:

```
RP/0/RSP0/CPU0:router(config-if)#path-option 1 dynamic
```

Sets the path option to dynamic and assigns the path ID.

Step 9 **commit**

Step 10 (Optional) **show mpls traffic-eng autoroute**

Example:

```
RP/0/RSP0/CPU0:router#show mpls traffic-eng autoroute
```

```
  Destination 192.168.0.2 has 1 tunnels in IS-IS ring level 1
    tunnel-te1 (traffic share 0, nexthop 192.168.0.2)
               (IPv4 unicast)
               (IPv6 unicast)
```

Verifies that the tunnel announces IPv6 autoroute information.

Step 11 (Optional) **show mpls traffic-eng forwarding-adjacency**

Example:

```
RP/0/RSP0/CPU0:router#show mpls traffic-eng forwarding-adjacency

 destination 192.168.0.1 has 1 tunnels

              tunnel-te10    (traffic share 0, next-hop 192.168.0.1)
                             (Adjacency Announced: yes, holdtime 0)
                             (IS-IS 100, IPv4 unicast)
                             (IS-IS 100, IPv6 unicast)
```

Verifies that the tunnel announces IPv6 forwarding adjacency information.

Configure IPv6 routing over IPv6 MPLS-TE tunnels

Perform these steps to configure IPv6 routing over IPv6 MPLS-TE tunnels:

Procedure

Step 1 **configure**

Step 2 **interface tunnel-te** *tunnel-id*

Example:

```
RP/0/RSP0/CPU0:router# interface tunnel-te 1
```

Configures an MPLS-TE tunnel interface.

Step 3 **ipv4 unnumbered** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-if)#ipv4 unnumbered Loopback 0
```

Assigns a source address so that forwarding can be performed on the new tunnel. Loopback is the commonly-used interface type.

Step 4 **ipv6 enable**

Example:

```
RP/0/RSP0/CPU0:router(config-if)#ipv6 enable
```

Enables IPv6 on interface.

Step 5 **signalled-bandwidth** *bandwidth*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# signalled-bandwidth 10
```

Sets the tunnel bandwidth requirement to be signalled in Kbps.

Step 6 Use one of these options:

- **autoroute announce include-ipv6**
- **forwarding-adjacency include-ipv6**

Example:

```
RP/0/RSP0/CPU0:router(config-if)#autoroute announce include-ipv6
```

Or

```
RP/0/RSP0/CPU0:router(config-if)#forwarding-adjacency include-ipv6
```

Announces the tunnel as an IPv6 autoroute or an IPv6 forwarding adjacency.

Step 7 **destination ipv6** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-if)#destination ipv6 2000::1
```

Specifies the IPv6 destination address.

Step 8 **path-option** *preference-priority* **dynamic**

Example:

```
RP/0/RSP0/CPU0:router(config-if)#path-option 1 dynamic
```

Sets the path option to dynamic and assigns the path ID.

Step 9 **commit**

Step 10 (Optional) **show mpls traffic-eng autoroute**

Example:

```
RP/0/RSP0/CPU0:router#show mpls traffic-eng autoroute

  Destination 192.168.0.2 has 1 tunnels in IS-IS ring level 1
    tunnel-te1 (traffic share 0, nexthop 192.168.0.2)
               (IPv4 unicast)
               (IPv6 unicast)
```

Verifies that the tunnel announces IPv6 autoroute information.

Step 11 (Optional) **show mpls traffic-eng forwarding-adjacency**

Example:

```
RP/0/RSP0/CPU0:router#show mpls traffic-eng forwarding-adjacency

 destination 192.168.0.1 has 1 tunnels

              tunnel-te10    (traffic share 0, next-hop 192.168.0.1)
                             (Adjacency Announced: yes, holdtime 0)
                             (IS-IS 100, IPv4 unicast)
                             (IS-IS 100, IPv6 unicast)
```

Verifies that the tunnel announces IPv6 forwarding adjacency information.

Using ePBR for MPLS Packets on Subscriber Interfaces

The enhanced policy based routing (ePBR) match/redirect MPLS packets on subscriber interfaces feature enables the capability to match MPLS labeled packets and redirect those to an external server by re-writing the source and destination IP addresses of the packets. This feature is applicable when the DNS server (an external server) is hidden in the MPLS cloud.

The traffic that is entering the MPLS cloud will be matched for a specific destination address and based on it, the new destination will be set. When the packet returns from the DNS server, the source address is changed back to the original source address.

For information on the commands used for configuring Enhanced Policy Based Routing Match/Redirect MPLS Packets on Subscriber Interfaces, see *MPLS Traffic Engineering Commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Use Case: Using ePBR for MPLS Packets on Subscriber Interfaces

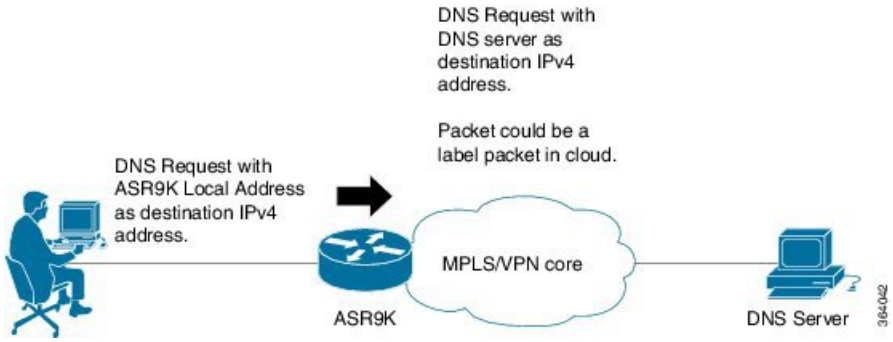
The ePBR match/redirect MPLS packets on subscriber Interfaces feature is applicable when a packet arrives at an interface with a destination address of a known server. This feature changes the known destination address to a required address that is hidden in the DNS cloud. For example, when the packet reaches a known interface with a specific IP address, say 10.0.0.1, it can to be redirected to a new IP address, say 172.16.0.1 , that is hidden in the cloud.

For subscriber to core DNS packets, the sequence for match and redirect is:

- Match the incoming packet for the known DNS server. This address could be a local address on the Cisco ASR 9000 Series Router, which the subscriber uses as DNS server address.
- Set the destination address to a new IP address to which the packet has to be redirected.

This figure explains the match and redirect sequence for subscriber to core DNS packets.

Figure 30: Subscriber to core DNS packets

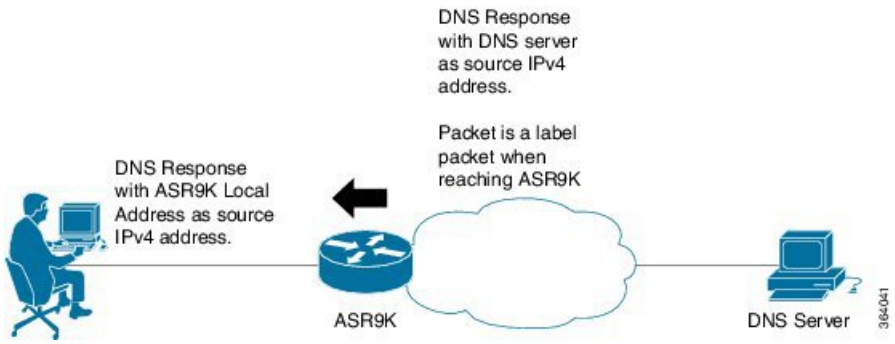


For core to subscriber DNS packets, the sequence for match and redirect is :

- Match the incoming labeled DNS packet's source IP address from the core.
- Set the source address to a local address, which the subscriber uses as DNS server address. The packet would be forwarded based on label + destination IP address, which is the subscriber address.

This figure explains the match and redirect sequence for core to subscriber DNS packets.

Figure 31: Core to subscriber DNS packets



Configuring ePBR-Based MPLS Redirection

These examples show how to configure ePBR-based MPLS match/redirect configuration.

Match configuration for IPv4 packets:

```
policy-map type pbr policy_mpls_src_test
class type traffic class_mpls_src_test
  set source-address ipv4 17.17.18.18
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0#show running-config class-map type traffic class_mpls_src_test
Wed Sep  3 02:52:31.411 UTC
class-map type traffic match-any class_mpls_src_test
match mpls disposition access-group ipv4 ACL_MPLS_SRC
 end-class-map
!

show running-config ipv4 access-list ACL_MPLS_SRC
Wed Sep  3 02:53:40.918 UTC
ipv4 access-list ACL_MPLS_SRC
10 permit ipv4 30.1.1.1/24 112.112.0.1/24
!
```

Match configuration for IPv6 packets:

```
policy-map type pbr policy_mpls_src_test
class type traffic class_mpls_ipv6_src_test
  set source-address ipv4 10.10.10.10
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0# show running-config class-map type traffic class_mpls_ipv6_src_test
Wed Sep  3 02:52:31.411 UTC
class-map type traffic match-any class_mpls_ipv6_src_test
match mpls disposition access-group ipv6 ACL_MPLS_IPV6__SRC
 end-class-map
!
```

```
show running-config ipv6 access-list ACL_MPLS_IPV6_SRC
Wed Sep  3 02:53:40.918 UTC
Ipv6 access-list ACL_MPLS_IPV6_SRC
10 permit ipv6 any any
!
```

Set destination configuration:

```
show running-config policy-map type pbr pbr_prec_exp
Wed Sep  3 03:11:16.000 UTC
policy-map type pbr pbr_prec_exp
class type traffic class_prec_exp
  set destination-address ipv4 192.168.0.1
!
class type traffic class-default
 !
end-policy-map
!

RP/0/RSP0/CPU0:ASR9K-0#show running-config class-map type traffic class_prec_e$
Wed Sep  3 03:11:30.339 UTC
class-map type traffic match-all class_prec_exp
match mpls experimental topmost 2
 match mpls disposition access-group ipv4 acl2
 end-class-map
!

RP/0/RSP0/CPU0:ASR9K-0# show running-config ipv4 access-list acl2
Wed Sep  3 03:11:47.963 UTC
ipv4 access-list acl2
5 permit ipv4 host 10.10.10.10 any
10 permit ipv4 any any
!
```

Multi Nexthop Tracking

The multi nexthop tracking feature enables the setting of virtual routing and forwarding (VRF) with nexthop and nexthop tracking, for an incoming MPLS or IP packet. When a MPLS/IP packet reaches an interface, a new VRF or a new nexthop is set. This feature enables the capability of matching the packet and redirecting to a new VRF or IP. This is extremely useful in cases of DNS redirect or HTTP redirect. If an incoming packet is redirected to an IP without specifying the VRF, it refers to the default VRF.

The multi nexthop tracking feature sets the nexthop by matching an incoming packet on the current VRF and then sets the VRF to the new value. The matching of the packets can also be based on the length of the packets.

A maximum number of three nexthops can be configured. The first nexthop configured has the highest priority as compared to the last nexthop, which has the least priority. The nexthops configured must be either IPv4 or IPv6. For a given nexthop, a VRF name, an IPv4/IPv6 address or both can be configured. When VRF is not configured, it is presumed to be an ingress interface VRF.

For the nexthop policy based routing (PBR) action, the available highest priority nexthop is chosen when setting the policy based route nexthop, though this may not be the highest priority configured nexthop. When a higher priority route comes up, it replaces the programmed nexthop.

Configuring Multi Nexthop Tracking for IPv4

Perform this task to configure multi nexthop tracking on a VRF for IPv4.

SUMMARY STEPS

1. **configure**
2. **policy-map type pbr** *policy-map name*
3. **class type traffic** *class name*
4. **redirect ipv4 nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address*
5. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**policy-map type pbr** *policy-map name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type pbr multi-vrf`	Enters policy-map configuration mode.
Step 3	**class type traffic** *class name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class_all`	Specifies a traffic class previously created with the class-map command.
Step 4	**redirect ipv4 nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# redirect ipv4 nexthop vrf vpn1 3.2.1.2 nexthop vrf vpn2 3.2.3.2 nexthop vrf vpn3 3.2.4.2`	Configures a maximum of three nexthops for VRFs and IPv4 addresses specified. **Note** The first nexthop will have the highest priority and the last nexthop will have the least priority.

Step 5	**end** or **commit**
	Example:
	`RP/0/RSP0/CPU0:router(config-pmap-c)# end`
	or
	`RP/0/RSP0/CPU0:router(config-pmap-c)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.

	Command or Action	Purpose
		- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes. - Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Configuring Multi Nexthop Tracking for IPv6

Perform this task to configure multi nexthop tracking on a VRF for IPv6.

SUMMARY STEPS

1. **configure**
2. **policy-map type pbr** *policy-map name*
3. **class type traffic** *class name*
4. **redirect ipv6 nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address*
5. **end** or **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**policy-map type pbr** *policy-map name* **Example:** `RP/0/RSP0/CPU0:router(config)# policy-map type pbr multi-vrf`	Enters policy-map configuration mode.
Step 3	**class type traffic** *class name* **Example:** `RP/0/RSP0/CPU0:router(config-pmap)# class type traffic class_all`	Specifies a traffic class previously created with the class-map command.

	Command or Action	Purpose
Step 4	**redirect ipv6 nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address* **nexthop vrf** *vrf-name nexthop address* **Example:** `RP/0/RSP0/CPU0:router(config-pmap-c)# redirect ipv6 nexthop vrf vpn1 3.2.1.2 nexthop vrf vpn2 3.2.3.2 nexthop vrf vpn3 3.2.4.2`	Configures a maximum of three nexthops for VRFs and IPv6 addresses specified. **Note** The first nexthop will have the highest priority and the last nexthop will have the least priority.

Step 5	**end** or **commit**
	Example:
	`RP/0/RSP0/CPU0:router(config-pmap-c)# end`
	or
	`RP/0/RSP0/CPU0:router(config-pmap-c)# commit`
		Saves configuration changes.
		• When you issue the **end** command, the system prompts you to commit changes:
		`Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:`
		- Entering **yes** saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode.
		- Entering **no** exits the configuration session and returns the router to EXEC mode without committing the configuration changes.
		- Entering **cancel** leaves the router in the current configuration session without exiting or committing the configuration changes.
		• Use the **commit** command to save the configuration changes to the running configuration file and remain within the configuration session.

Verifying Multi Nexthop Tracking Configuration

Use the **show running-config policy-map type pbr multi-vrf** command to verify the multi nexthop tracking configuration. The following example shows sample output for the command:

```
show running-config policy-map type pbr multi-vrf

policy-map type pbr multi-vrf
 class type traffic class_all
  redirect ipv4 nexthop vrf vpn1 3.2.1.2 nexthop vrf vpn3 3.2.3.2 nexthop vrf vpn4 3.2.4.2

 !
class type traffic class-default
 !
end-policy-map
!
```

Configuring Path-selection Cost Limit

Apply the path-selection cost-limit configuration to set the upper limit on the path aggregate admin-weight when computing paths for MPLS-TE LSPs. Once the path-selection cost is configured, the periodic path verification will check if the cost-limit is crossed. Path-selection cost limit can be configured at global MPLS TE, per interface tunnel, and per path-option attribute set. The path-selection cost limit per path-option attribute set takes the highest priority, followed by per interface and MPLS TE global path-selection cost limit values.

Configuring Global Path-selection Cost Limit on MPLS TE Tunnels

Perform these steps to configure path-selection cost limit globally for MPLS TE tunnels:

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **path-selection cost-limit** *cost-limit*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**path-selection cost-limit** *cost-limit* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# path-selection cost-limit 3`	Sets the upper limit on the path aggregate admin-weight when computing paths for MPLS TE LSPs.
Step 4	**commit**	

Configuring Path-selection Cost Limit per TE Tunnel

Perform these steps to configure path-selection cost limit per MPLS TE tunnel:

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **path-selection cost-limit** *cost-limit*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router(config)#interface tunnel-te 1`	Configures an MPLS-TE tunnel interface.
Step 3	**path-selection cost-limit** *cost-limit* **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-selection cost-limit 2`	Sets the upper limit on the path aggregate admin-weight when computing paths for MPLS TE LSPs for the specified MPLS TE tunnel.
Step 4	**commit**	

Configuring Path-selection Cost Limit per Path-option Attribute-set

Perform these steps to configure path-selection cost limit per path-option attribute-set:

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **attribute-set path-option** *attribute-set-name*
4. **path-selection cost-limit** *3*

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**attribute-set path-option** *attribute-set-name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# attribute-set path-option PO3AttrSet`	Enters attribute-set path option configuration mode. **Note** The configuration at the **attribute-set path-option** level takes precedence over the values configured at global and interface tunnel level.

	Command or Action	Purpose
Step 4	**path-selection cost-limit** *3* **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# path-selection cost-limit 3`	Sets the upper limit on the path aggregate admin-weight when computing paths for MPLS TE LSPs per path-option attribute set.

Enabling Soft-preemption over FRR Backup Tunnels

Perform these tasks to enable LSP traffic to be moved over the backup tunnel when the LSP is soft-preempted. With this configuration, when there is a soft-preemption, the MPLS TE process triggers a rewrite to move the traffic on the backup tunnel, if the backup tunnel is ready. The rest of the soft-preemption process remains unchanged.

Before you begin

Ensure that the following configurations are enabled before enabling soft-preemption over FRR backup:

- Soft-preemption enabled.
- Fast-reroute (FRR) backup tunnel is activated.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **soft-preemption frr-rewrite**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)#mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**soft-preemption frr-rewrite** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)#soft-preemption frr-rewrite`	Moves FRR LSP traffic over the backup tunnel, when LSP is soft-preempted.
Step 4	**commit**	

Enabling Auto-onehop Tunnels to Next-hop Neighbors

Perform these tasks to enable automatic creation of one-hop tunnels over MPLS traffic-engineering enabled interfaces to nexthop neighbors. A router that becomes a next hop neighbor will have a set of one-hop tunnels created automatically.

Before you begin

The **ipv4 unnumbered mpls traffic-eng Loopback** *Number* configuration must be applied at the global configuration level.

SUMMARY STEPS

1. **configure**
2. **ipv4 unnumbered mpls traffic-eng Loopback** *N*
3. **mpls traffic-eng**
4. **auto-tunnel mesh**
5. **tunne-id min** *value* **max** *value*
6. **group** *group-id*
7. **onehop**
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv4 unnumbered mpls traffic-eng Loopback** *N* **Example:** `RP/0/RSP0/CPU0:router(config)#ipv4 unnumbered mpls traffic-eng loopback 0`	Configures the globally configured IPv4 address that can be used by the Auto-tunnel backup tunnels.
Step 3	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)#mpls traffic-eng`	Enters the MPLS-TE submode.
Step 4	**auto-tunnel mesh** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)#auto-tunnel mesh`	Enters the auto-tunnel mesh configuration submode.
Step 5	**tunne-id min** *value* **max** *value* **Example:** `RP/0/0/CPU0:ios(config-te-auto-mesh)# tunnel-id min 4000 max 6000`	Specifies the minimum and maximum number of auto-tunnel mesh tunnels that can be created on this router. The range of tunnel ID is from 0 to 65535.

	Command or Action	Purpose
Step 6	**group** *group-id* **Example:** `RP/0/RSP0/CPU0:router(config-te-auto-mesh)#group 50`	Enters the auto-tunnel mesh group configuration submode and creates a group ID.
Step 7	**onehop** **Example:** `RP/0/RSP0/CPU0:router(config-te-mesh-group)#onehop`	Enables automatic creation of one-hop tunnels to all next hop neighbors. The onehop keyword can be applied to as many mesh groups as desired.
Step 8	**commit**	

Implementing Associated Bidirectional Label Switched Paths

Associated Bidirectional Label Switched Paths are LSP instances where the forward and the reverse direction paths are setup, monitored and protected independently and associated together during signaling. You use a RSVP Association object to bind the two forward and reverse LSPs together to form either a co-routed or non co-routed associated bidirectional TE tunnel.

You can associate a protecting MPLS-TE tunnel with either a working MPLS-TE LSP, protecting MPLS-TE LSP, or both. The working LSP is the primary LSP backed up by the protecting LSP. When a working LSP goes down, the protecting LSP is automatically activated. You can configure a MPLS-TE tunnel to operate without protection as well.

For more information on Associated Bidirectional Co-routed LSPs, see the *Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide, Release 5.2.x*. For information on the commands used for Associated Bidirectional Co-routed LSPs, see the *Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference, Release 5.2.x*.

Signaling Methods and Object Association for Bidirectional LSPs

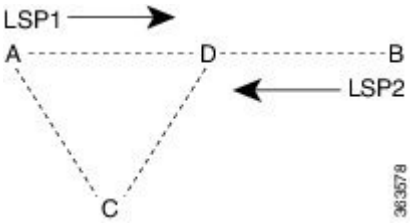
This section provides an overview of the association signaling methods for the bidirectional LSPs. Two unidirectional LSPs can be bound to form an associated bidirectional LSP in the following scenarios:

- No unidirectional LSP exists, and both must be established.
- Both unidirectional LSPs exist, but the association must be established.
- One unidirectional LSP exists, but the reverse associated LSP must be established.

Configuration information regarding the LSPs can be provided at one or both endpoints of the associated bidirectional LSP. Depending on the method chosen, there are two models of creating an associated bidirectional LSP; single-sided provisioning, and double-sided provisioning.

- **Single-sided Provisioning:** For the single-sided provisioning, the TE tunnel is configured only on one side. An LSP for this tunnel is initiated by the initiating endpoint with the Association Object inserted in the Path message. The other endpoint then creates the corresponding reverse TE tunnel and signals the reverse LSP in response to this. Currently, there is no support available for configuring single-sided provisioning.
- **Double-sided Provisioning:** For the double-sided provisioning, two unidirectional TE tunnels are configured independently on both sides. The LSPs for the tunnels are signaled with Association Objects inserted in the Path message by both sides to indicate that the two LSPs are to be associated to form a bidirectional LSP.

Consider this topology (an example of associated bidirectional LSP):



Here, LSP1 from A to B, takes the path A,D,B and LSP2 from B to A takes the path B,D,C,A. These two LSPs, once established and associated, form an associated bidirectional LSP between node A and node B. For the double sided provisioning model, both LSP1 and LSP2 are signaled independently with (Extended) Association Object inserted in the Path message, in which the Association Type indicating double-sided provisioning. In this case, the two unidirectional LSPs are bound together to form an associated bidirectional LSP based on identical Association Objects in the two LSPs' Path messages.

Association Object: An Association Object is used to bind unidirectional LSPs originating from both endpoints. The Association Object takes the following values:

- **Association Type**: In order to bind two reverse unidirectional LSPs to be an associated bidirectional LSP, the Association Type must be set to indicate either single sided or double sided LSPs.
- **Association ID**: For both single sided and double sided provisioning, Association ID must be set to a value assigned by the node that originates the association for the bidirectional LSP. This is set to the Tunnel ID of the bound LSP or the Tunnel ID of the binding LSP.
- **Association Source:** For double sided provisioning, Association Source must be set to an address selected by the node that originates the association for the bidirectional LSP. For single sided provisioning, Association Source must be set to an address assigned to the node that originates the LSP.
- **Global ID**: This is the global ID for the association global source. This must be set to the global ID of the node that originates the association for the bidirectional LSP.

Note You must provide identical values for the content of the Association Object on either end of the participating LSPs to ensure successful binding of the LSPs.

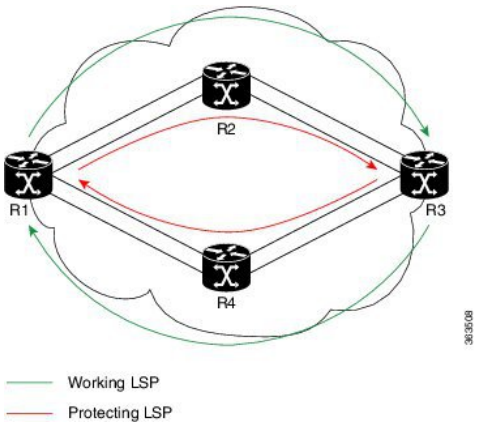
Configure Associated Bidirectional Co-routed LSPs, on page 364 describes the procedure to create associated bidirectional co-routed LSPs.

Associated Bidirectional Non Co-routed and Co-routed LSPs

This section provides an overview of associated bidirectional non co-routed and co-routed LSPs. Establishment of MPLS TE-LSP involves computation of a path between a head-end node to a tail-end node, signaling along the path, and modification of intermediate nodes along the path. The signaling process ensures bandwidth reservation (if signaled bandwidth is lesser than 0 and programming of forwarding entries.

Path computation is performed by the head-end nodes of both the participating LSPs using Constrained Shortest Path First (CSPF). CSPF is the 'shortest path (measured in terms of cost) that satisfies all relevant LSP TE constraints or attributes, such as required bandwidth, priority and so on.

Associated Bidirectional Non Co-routed LSPs: A non co-routed bidirectional TE LSP follows two different paths, that is, the forward direction LSP path is different than the reverse direction LSP path. Here is an illustration.



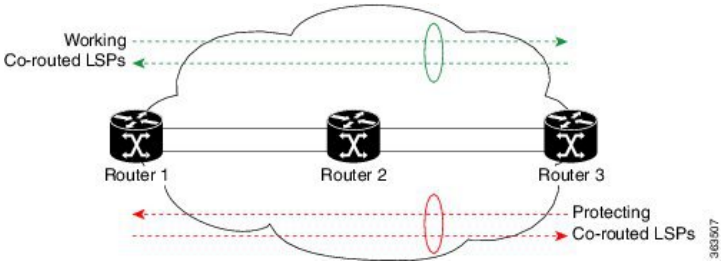
In the above topology:

- The outer paths (in green) are working LSP pairs.
- The inner paths (in red) are protecting LSP pairs.
- Router 1 sets up working LSP to Router 3 and protecting LSP to Router 3 independently.
- Router 3 sets up working LSP to Router 1 and protecting LSP to Router 1 independently.

Non co-routed bidirectional TE LSP is available by default, and no configuration is required.

Note In case of non co-routed LSPs, the head-end nodes relax the constraint on having identical forward and reverse paths. Hence, depending on network state you can have identical forward and reverse paths, though the bidirectional LSP is co-routed.

Associated Bidirectional Co-routed LSPs: A co-routed bidirectional TE LSP denotes a bidirectional tunnel where the forward direction LSP and reverse direction LSP must follow the same path, for example, the same nodes and paths. Here is an illustration.



In the above topology:

- Paths at the top of the figure (in green) indicate working co-routed LSP pairs.
- Paths at the bottom of the figure (in red) indicate protecting co-routed LSP pairs.
- Router 1 sets up working LSP to Router 3 (in red) after performing bidirectional CSPF and sends reverse explicit route object (ERO) to Router 3. Node Router 3 uses the received reverse ERO to set up reverse red working LSP to Router 1.
- Router 3 sets up protecting LSP to Router 1 (in green) after performing bidirectional CSPF and sends reverse ERO to Router 1. Node Router 1 uses the received reverse ERO to set up reverse green protecting LSP to Router 3.

Configure Associated Bidirectional Co-routed LSPs, on page 364 describes the procedure to configure an associated bidirectional co-routed LSP.

Configure Associated Bidirectional Co-routed LSPs

A co-routed bidirectional packet LSP is a combination of two LSPs (one in the forward direction and the other in reverse direction) sharing the same path between a pair of ingress and egress nodes. It is established using the extensions to RSVP-TE. This type of LSP can be used to carry any of the standard types of MPLS-based traffic, including Layer 2 VPNs, Layer 2 circuits, and Layer 3 VPNs. You can configure a single BFD session for the bidirectional LSP (that is, you do not need to configure a BFD session for each LSP in each direction). You can also configure a single standby bidirectional LSP to provide a backup for the primary bidirectional LSP.

Before you begin

- You must have symmetric source and destination TE router IDs in order for bidirectional LSPs to be associated.
- Tunnels attributes must be configured identically on both sides of co-routed bidirectional LSP.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **bidirectional**
4. **association** {**id** <0-65535> | **source-address** <IP address>} [**global-id** <0-4294967295>]
5. **association type co-routed**
6. **commit**
7. **show mpls traffic-eng tunnels bidirectional-associated co-routed**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router# interface tunnel-te 1`	Configures an MPLS-TE tunnel interface.
Step 3	**bidirectional** **Example:** `RP/0/0/CPU0:router(config-if)# bidirectional`	Configure the ingress router for the LSP and include the bidirectional statement to specify that the LSP be established as a bidirectional LSP.
Step 4	**association** {**id** <0-65535> | **source-address** <IP address>} [**global-id** <0-4294967295>] **Example:** `RP/0/0/CPU0:router(config-if-bidir)# association id 1 source-address 11.0.0.1`	Set the association ID that uniquely identifies the association of LSPs, which is the tunnel ID of the bound LSP or the tunnel ID of the binding LSP. Also, set the source address to the tunnel sender address of the bound LSP or the tunnel

	Command or Action	Purpose
		sender address of the binding LSP. Optionally, specify the global ID for association global source. **Note** Association ID, association source and global ID must be configured identically on both the endpoints.
Step 5	**association type co-routed** **Example:** `RP/0/0/CPU0:router(config-if-bidir)#association type co-routed`	Specify that the LSP be established as a associated co-routed bidirectional LSP.
Step 6	**commit**	
Step 7	**show mpls traffic-eng tunnels bidirectional-associated co-routed** **Example:** `RP/0/0/CPU0:router#show mpls traffic-eng tunnels bidirectional-associated co-routed`	Shows details of an associated co-routed bidirectional LSP.

Show output for an associated co-routed bidirectional LSP configuration

This is a sample of the output for the **show mpls traffic-eng tunnels role head** command.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels role head

Name: tunnel-te1  Destination: 49.49.49.2
  Signalled-Name: IMC0_t1
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 1,  type dynamic  (Basis for Setup, path weight 20 (reverse 20))
    path option 1,  type dynamic  (Basis for Standby, path weight 20 (reverse 20))
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Sun May  4 12:09:56 2014 (03:24:11 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    Hop-limit: disabled
    Cost-limit: disabled
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (default)
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Enabled
    Association Type: Single Sided Bidirectional LSPs, Co-routed: YES
    Association ID: 100, Source: 49.49.49.2
    Reverse Bandwidth: 0 kbps (CT0), Standby: 0 kbps (CT0)
    BFD Fast Detection: Enabled
    BFD Parameters: Min-interval 100 ms (default), Multiplier 3 (default)
    BFD Bringup Timeout: Interval 60 seconds (default)
    BFD Initial Dampening: 16000 ms (default)
    BFD Maximum Dampening: 600000 ms (default)
```

```
BFD Secondary Dampening: 20000 ms (default)
Periodic LSP Ping: Interval 120 seconds (default)
Session Down Action: ACTION_REOPTIMIZE, Reopt Timeout: 300
BFD Encap Mode: GAL
Reoptimization after affinity failure: Enabled
Soft Preemption: Disabled
```

Path Protection

Path protection provides an end-to-end failure recovery mechanism (that is, full path protection) for associated bidirectional MPLS-TE LSPs. Associated bidirectional MPLS-TE LSPs support 1:1 path protection. You can configure the working and protecting LSPs as part of configuring the MPLS-TE tunnel. The working LSP is the primary LSP used to route traffic, while the protecting LSP is a backup for a working LSP. If the working LSP fails, traffic is switched to the protecting LSP until the working LSP is restored, at which time traffic forwarding reverts back to the working LSP.

When FRR is not enabled on a tunnel, and when GAL-BFD and/or Fault OAM is enabled on an associated bidirectional co-routed LSP, path-protection is activated by the FIB running on the line card that hosts the working LSP. The failure on the working LSP can be detected using BFD or Fault OAM.

Configure Path Protection for Associated Bidirectional LSPs, on page 366 provides procedural details.

You can use the **show mpls traffic-eng fast-reroute log** command to confirm whether protection switching has been activated by FIB.

Configure Path Protection for Associated Bidirectional LSPs

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **ipv4 unnumbered** *type interface-path-id*
4. **bfd** {fast-detect | encap-mode}
5. **destination** *ip-address*
6. **bidirectional**
7. **bidirectional association** {**id** <0-65535> | **source-address** <IP address>} [**global-id** <0-4294967295>
8. **association type co-routed**
9. **path-protection**
10. **path-option** *preference - priority* **{dynamic | explicit}**
11. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:router# interface tunnel-te 1`	Configures an MPLS-TE tunnel interface.

	Command or Action	Purpose
Step 3	**ipv4 unnumbered** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-if)# ipv4 unnumbered Loopback0`	Assigns a source address so that forwarding can be performed on the new tunnel. Loopback is commonly used as the interface type.

Step 4	**bfd** {fast-detect | encap-mode}
	Example:
	`RP/0/RSP0/CPU0:IMC0(config-if)#bfd`
	`RP/0/RSP0/CPU0:IMC0(config-if-tunte-bfd)#fast-detect`
	`RP/0/RSP0/CPU0:IMC0(config-if-tunte-bfd)#encap-mode gal`
		Specify if you want BFD enabled for the LSP over a Generic Associated Channel (G-ACh) or over a IP channel. IP channel is the default.

Step 5	**destination** *ip-address* **Example:** `RP/0/RSP0/CPU0:router(config-if)# destination 49.49.49.2`	Assigns a destination address on the new tunnel. The destination address is the remote node's MPLS-TE router ID.
Step 6	**bidirectional** **Example:** `Router(config-if)# bidirectional`	Configure the ingress router for the LSP and include the bidirectional statement to specify that the LSP be established as a bidirectional LSP.
Step 7	**bidirectional association** {**id** <0-65535> | **source-address** <IP address>} [**global-id** <0-4294967295>] **Example:** `Router(config-if-bidir)# association id 1 source-address 11.0.0.1`	Set the association ID that uniquely identifies the association of LSPs, which is the tunnel ID of the bound LSP or the tunnel ID of the binding LSP. Also, set the source address to the tunnel sender address of the bound LSP or the tunnel sender address of the binding LSP. Also, set the ID for associating the global source. **Note** Association ID, association source and optional global-id must be configured identically on both the endpoints.
Step 8	**association type co-routed** **Example:** `Router(config-if-bidir)#association type co-routed`	Specify that the LSP be established as a associated co-routed bidirectional LSP.
Step 9	**path-protection** **Example:** `RP/0/RSP0/CPU0:IMC0(config-if-bidir-co-routed)#path-protection`	Enable path protection.
Step 10	**path-option** *preference - priority* **{dynamic | explicit}** **Example:** `RP/0/RSP0/CPU0:router(config-if)# path-option 1`	Sets the path option and assigns the path-option ID. Both sides of the co-routed bidirectional LSPs must use dynamic or matching co-routed strict-hop explicit path-option.

	Command or Action	Purpose
	`dynamic`	
Step 11	**commit**	

Example

Here is a sample configuration with path protection defined for the Associated Bidirectional LSP.

```
RP/0/RSP0/CPU0:IMC0#config
RP/0/RSP0/CPU0:IMC0(config)#interface tunnel-te 1
RP/0/RSP0/CPU0:IMC0(config-if)#ipv4 unnumbered loopback0
RP/0/RSP0/CPU0:IMC0(config-if)#destination 49.49.49.2
RP/0/RSP0/CPU0:IMC0(config-if)#bidirectional
RP/0/RSP0/CPU0:IMC0(config-if-bidir)#association id 100 source-address 49.49.4$
RP/0/RSP0/CPU0:IMC0(config-if-bidir)#association type co-routed
RP/0/RSP0/CPU0:IMC0(config-if-bidir-co-routed)#path-protection
RP/0/RSP0/CPU0:IMC0(config-if)#path-option 1  dynamic
RP/0/RSP0/CPU0:IMC0(config-if)#commit
```

OAM Support for Associated Bidirectional LSPs

You can opt to configure operations, administration and management (OAM) support for Associated Bidirectional LSPs in the following areas:

- **Continuity check:** You can configure bidirectional forwarding detection (BFD) over a Generic Associated Channel (G-ACh) with hardware assist. This allows for BFD Hello packets to be generated and processed in hardware making smaller Hello intervals such as 3.3 ms feasible. For more information on BFD and BFD hardware offload see *Implementing BFD* module in the *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide* .
- **Fault notification:** You can run Fault OAM over associated bidirectional co-routed LSPs to convey fault notification from mid-point to end-point of the LSP. The following fault OAM messages are supported:
  - Link Down Indication (LDI): generated when an interface goes down (for example, to fiber-cut) at mid-point.
  - Lock Report (LKR): generated when an interface is shutdown at mid-point.

  You can configure fault OAM to generate OAM message at mid-point or enable protection switching due to fault OAM at end-point. Generate Fault OAM Messages at Mid-point, on page 368 and Generate Fault OAM Messages at End-point, on page 369provides procedural details.
- **Fault diagnostics:** You can use the ping and traceroute features as a means to check connectivity and isolate failure points for both co-routed and non-co-routed bidirectional TE tunnels. *MPLS Network Management with MPLS LSP Ping and MPLS SP Traceroute* provides details.

Generate Fault OAM Messages at Mid-point

To program all bi-directional LSPs to generate fault OAM message at mid-point use the following steps:

SUMMARY STEPS

1. **configure**

2. **mpls traffic-eng**
3. **fault-oam**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:IMO(config)# mpls traffic-eng`	Configures an MPLS-TE tunnel interface.
Step 3	**fault-oam** **Example:** `RP/0/RSP0/CPU0:IMC0(config-mpls-te)#fault-oam`	Enable fault OAM for an associated bidirectional LSP.
Step 4	**commit**	

Generate Fault OAM Messages at End-point

In order to enable protection switching due to fault OAM at end-point use the following steps:

SUMMARY STEPS

1. **configure**
2. **interface tunnel-te** *tunnel-id*
3. **bidirectional association type co-routed fault-oam**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-te** *tunnel-id* **Example:** `RP/0/RSP0/CPU0:IMC0(config)#interface tunnel-te 1`	Configures an MPLS-TE tunnel interface.
Step 3	**bidirectional association type co-routed fault-oam** **Example:** `RP/0/RSP0/CPU0:IMC0(config-if)#bidirectional association type co-routed fault-oam`	Enable fault OAM for an associated co-routed bidirectional LSP.

	Command or Action	Purpose
Step 4	**commit**	

Pseudowire Call Admission Control

You can use the Pseudowire Call Admission Control (PW CAC) process to check for bandwidth constraints and ensure that once the path is signaled, the links (pseudowires) participating in the bidirectional LSP association have the required bandwidth. Only pseudowires with sufficient bandwidth are admitted in the bidirectional LSP association process. *Configure Pseudowire Bandwidth* in the *Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Configuration Guide* provides procedural details.

Configure Named Tunnel and Named Path Option

Perform this task to uniquely name TE (Traffic Engineering) tunnels in a network and their path options using STRING names.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **named-tunnels**
4. **tunnel-te** *tunnel-name*
5. **destination** *address*
6. **path-option** *path-name*
7. **preference** *value*
8. **computation** { **explicit** *explicit-path-name* | **dynamic** }
9. **root**
10. **ipv4 unnumbered mpls traffic-engloopback** *loopback-number*
11. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters global configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.

	Command or Action	Purpose
Step 3	**named-tunnels** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# named-tunnels`	Enters the named tunnels configuration sub-mode.
Step 4	**tunnel-te** *tunnel-name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-named-tunnels)# tunnel-te FROM-NY-TO-LA`	Specifies the TE tunnel name using STRING characters. The STRING limit is 59.
Step 5	**destination** *address* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tunnel-name)# destination 192.168.0.1`	Assigns a destination address to the new tunnel.
Step 6	**path-option** *path-name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tunnel-name)# path-option VIA_DC`	Specifies the path option name.
Step 7	**preference** *value* **Example:** `RP/0/RSP0/CPU0:router(config-path-option-name)# preference 10`	Specifies the path option preference. The range is from 1 to 4294967295. Lower values have a higher preference.
Step 8	**computation** { **explicit** *explicit-path-name* | **dynamic** } **Example:** `RP/0/RSP0/CPU0:router(config-path-option-name)# computation explicit MY_EXPLICIT_PATH`	Sets the path computation method as explicit (Computation is based on the preconfigured path). **Note** You can use the *dynamic* option as the path computation method, where the path is dynamically calculated.
Step 9	**root**	
Step 10	**ipv4 unnumbered mpls traffic-engloopback** *loopback-number* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv4 unnumbered mpls traffic-eng loopback 0`	Enables IPv4 processing without an explicit address.

	Command or Action	Purpose
Step 11	**commit**	

Verify Named Tunnel and Named Path Option Configuration: Example

Use the **show mpls traffic-eng tunnels name** *tunnel-name* command to verify the named tunnel configuration. The following example shows sample output for this command:

```
show mpls traffic-eng tunnels name FROM-NY-TO-LA

Name: FROM-NY-TO-LA  Destination: 192.168.0.1  Ifhandle:0x580
  Tunnel-ID: 32769
  Status:
    Admin:    up Oper: down   Path: valid   Signalling: connected

    path option VIA_DC, preference 10,  type explicit MY_EXPLICIT_PATH

    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Fri Jun 10 15:32:00 2016 (00:36:10 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (global)
    Path Selection:
      Tiebreaker: Min-fill (default)
    Hop-limit: disabled
    Cost-limit: disabled
    Path-invalidation timeout: 10000 msec (default), Action: Tear (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forward class: 0 (default)
    Forwarding-Adjacency: disabled
    Autoroute Destinations: 0
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    Soft Preemption: Disabled
Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 0 up, 1 down, 0 recovering, 0 recovered head
```

Enable per-application accounting for interfaces

The following configurations helps enable per-application accounting for MPLS RSVP-TE IPv4 traffic and segment routing with MPLS IPv4 traffic on the interfaces respectively.

Example 1: Enable per-application accounting for MPLS RSVP-TE IPv4 traffic on the interfaces

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# accounting
RP/0/RSP0/CPU0:router(config-acct)# interfaces
RP/0/RSP0/CPU0:router(config-acct-if)# mpls
RP/0/RSP0/CPU0:router(config-acct-if-mpls)# ipv4 rspv-te
```

Example 2: Enable per-application accounting for segment routing MPLS IPv4 traffic on the interfaces

```
RP/0/RSP0/CPU0:router# config
RP/0/RSP0/CPU0:router(config)# accounting
RP/0/RSP0/CPU0:router(config-acct)# interfaces
RP/0/RSP0/CPU0:router (config-acct-if)# segment-routing mpls ipv4
```

Configure RSVP-TE bandwidth accounting

Perform these steps to enable RSVP-TE bandwidth accounting and dark bandwidth advertisement for all MPLS-TE enabled links:

Before you begin

Make sure that the traffic accounting feature is enabled on the router.

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters global configuration mode.

Step 2 **mpls traffic-eng**

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls traffic-eng
```

Enters MPLS TE configuration mode.

Step 3 **bandwidth-accounting**

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-te)# bandwidth-accounting
```

Enables RSVP-TE dark bandwidth accounting and enters bandwidth accounting configuration mode.

Step 4 **application interval** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-te-bw-account)# application interval 90
```

Configures the length of the application interval in seconds. At the end of application interval, dark bandwidth rates are computed and applied to all RSVP-TE enabled interfaces.

Note
Model-driven telemetry supports dark bandwidth. The telemetry polling interval is reduced to 10 seconds.

If the interval is reconfigured while the timer is running, the new value is compared to the time remaining for the running timer. The timer is adjusted so that the lower of these two values is used for this interval. The subsequent interval will use the newly configured value.

Note
TE stores sample history for the current and previous application intervals. If the application interval is lowered, TE may discard the sample history.

Range is from 90 to 1800. The default value is 180.

Step 5 **application enforced**

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-te-bw-account)# application enforced
```

Enables enforcement of the calculated effective maximum reservable bandwidth rate. This configuration is mandatory for the dark bandwidth accounting feature to work properly.

Step 6 **adjustment-factor** *percentage*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-te-bw-account)# adjustment-factor 85
```

Configures TE to over-book (>100%) or under-book (<100%) the effective maximum reservable bandwidth. The measured dark-bandwidth will be scaled based on the adjustment factor. Range is from 0 to 200. The default value is 100.

Step 7 **sampling-interval** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-te-bw-account)# sampling-interval 30
```

Configures the length of the sampling interval in seconds. The bandwidth rate is collected from the statistics collector process (statsD) at the end of each sampling interval for each TE link.

If the interval is reconfigured while the timer is running, the new value is compared to the time remaining for the running timer. The timer is adjusted so that the lower of these two values is used for this interval. The subsequent interval will use the newly configured value.

Range is from 30 to 600. The default is 60.

Step 8 **flooding threshold** { **up** | **down** } *percentage*

Example:

```
RP/0/RSP0/CPU0:router(config-mpls-te-bw-account)# flooding threshold up 30 down 30
```

Configures the reserved bandwidth thresholds. When bandwidth crosses one of these thresholds, flooding is triggered. Range is from 0 to 100. The default value is 10.

Step 9 **commit**

Step 10 **show mpls traffic-eng link-management summary**

Example:

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng link-management summary
```

(Optional)

Displays a summary of link management information, including bandwidth accounting information.

Step 11 **show mpls traffic-eng link-management advertisements**

Example:

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng link-management advertisements
```

(Optional)

Displays local link information that MPLS-TE link management is currently flooding into the global TE topology.

Step 12 **show mpls traffic-eng link-management interfaces** [*type interface-path-id*]

Example:

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng link-management interfaces gig0/1/1/1 detail
```

(Optional)

Displays bandwidth accounting and utilization details and link management information.

Autoroute Announce with IS-IS

The autoroute announce feature in an MPLS Traffic Engineering (TE) network is a mechanism that:

- simplifies the integration of MPLS TE tunnels into the Interior Gateway Protocol (IGP) routing process, and
- allows an MPLS TE tunnel to automatically advertise itself as a forwarding adjacency (FA) to the IGP, making the tunnel appear like a regular link in the network topology.

The autoroute announce feature can be used to steer traffic through the MPLS-TE tunnel for optimal network performance and efficient use of resources.

Table 14: Feature History Table

Feature Name	Release	Feature Description
MPLS-TE IPv6-only autoroute announce	Release 25.4.1	This feature allows you to disable IPv4 autoroute announce without turning off autoroute announce entirely. To achieve IPv6-only announcements over MPLS-TE tunnels, use the new **exclude-ipv4** option along with the **include-ipv6** option in the autoroute announce configuration. This feature introduces these changes: **CLI:** A new keyword, **exclude-ipv4**, has been added to the **autoroute announce** command.
Autoroute announce with IPv6 destination address for IS-IS	Release 25.2.1	The autoroute announce feature now allows an MPLS-TE tunnel as the nexthop for IPv6 destinations thus ensuring a seamless IPv6 traffic engineering. IS-IS uses this IPv6 destination address when filtering prefixes. This feature introduces these changes: **CLI:** Two new keywords, **destination** and **ipv6**, were added to the **autoroute announce** command.

Feature Name	Release	Feature Description
Autoroute Announce with IS-IS for Anycast Prefixes	Release 7.5.4	We have enabled seamless migration from autoroute announce (AA) tunnels with OSPF to AA tunnels with IS-IS. This is possible because you can now use AA tunnels with IS-IS to calculate the underlying native IGP metric for anycast prefixes to select the shortest path and then select a tunnel on that shortest path. Previously, autoroute announce tunnels with IS-IS behaved differently as compared to OSPF. IS-IS used the autoroute announce metric whereas, OSPF uses the underlying native IGP cost. With this feature the router uses the same method of cost calculation in autoroute announce in both OSPF and IS-IS. This feature introduces these: • CLI: **anycast-prefer-igp-cost** • YANG Data model: New Xpaths for Cisco-IOS-XR-um-router-isis-cfg.yang and Cisco-IOS-XR-clns-isis-cfg.yang (see GitHub and Yang Data Navigator)

When you configure Autoroute Announce (AA) tunnels, IGP installs the tunnel to the destination in the Routing Information Base (RIB) for the shortest paths. However, the behavior of AA for anycast destination is different from IS-IS compared to OSPF.

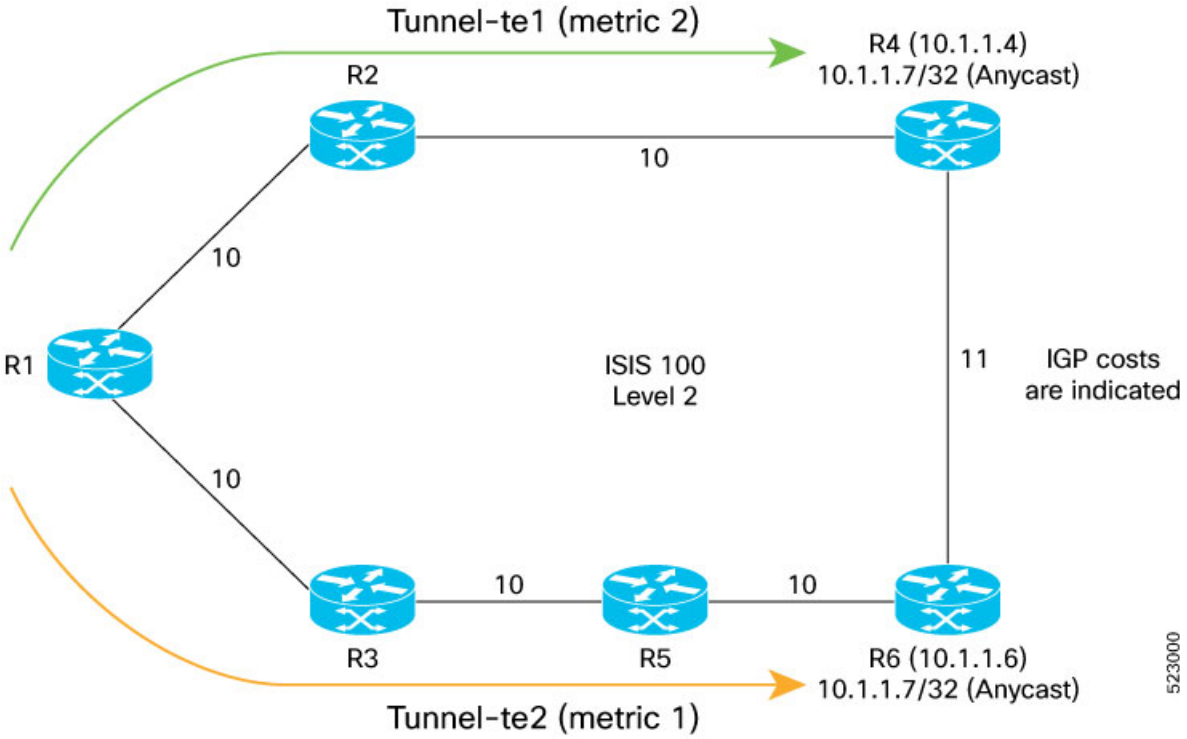
- IS-IS: AA tunnel with IS-IS considers the AA metric to calculate the prefix reachability for the shortest path.
- OSPF: AA with OSPF uses the lowest IGP cost to find the shortest path. And, then use the TE tunnel which is on that shortest path.

We now introduce the **anycast-prefer-igp-cost** command for AA tunnel with IS-IS anycast prefixes to allow the router to choose the shortest IGP path and select the tunnel on that shortest path, similar to OSPF behavior.

Starting from Cisco IOS XR Release 25.4.1, the autoroute announce feature restricts the usage of MPLS-TE tunnels by IGP to IPv6 prefixes. To enable the IPv6-only autoroute announce feature, configure the **autoroute announce exclude-ipv4** and **autoroute announce include-ipv6** commands.

Topology

Using this topology, let's see how the shortest path is chosen based on the IGP cost:



- In this topology, R1 is the headend and has MPLS RSVP-TE tunnels to R2 and R3.
- The tunnel destinations are loopback addresses of R4 and R6, which is 10.1.1.4 and 10.1.1.6.
- R1 uses AA to allow traffic to prefixes advertised by R2 and R3 to go over the MPLS-TE tunnel.
- Two AA tunnels are configured with different metrics and destinations. Tunnel-te1 has a metric value of 2 and tunnel-te2 has a metric value of 1.
- R1 can reach the anycast prefix (10.1.1.7/32) using two paths R1-R2-R4 and R1-R3-R5-R6.
- To reach the anycast prefix, the IGP cost is 20 for the R1-R2-R4 path and it is 30 for the R1-R3-R5-R6 path. Based on the IGP metric, the R1-R2-R4 path is the shortest path.
- With IS-IS, by default, the AA tunnel considers the tunnel metric to forward the traffic. In this topology, tunnel-te2 has a lower metric value when compared to tunnel-te1. As the AA metric is considered and the traffic is forwarded through te-2.
- When this feature is enabled, the IGP cost is first considered for the shortest path like AA with OSPF.

  In this topology, the R1-R2-R4 path is considered as the IGP cost is 20 that lower when compared to tunnel-te2, which is 30. Then the MPLS-TE tunnel on that path is considered, which is tunnel-te1.

Configure IGP Path Selection for Anycast Prefixes using AA with IS-IS

Perform the following tasks to configure IGP Path Selection for Anycast Prefixes using Autoroute Announce with IS-IS:

- Configure MPLS RSVP-TE.
- Enable **anycast-prefer-igp-cost** wish IS-IS.

```
/* Configure MPLS RSVP-TE */
Router(config)#interface tunnel-te1
Router(config-if)#ipv4 unnumbered Loopback0
Router(config-if)#autoroute announce
Router(config-if-tunte-aa)#metric 2
Router(config-if-tunte-aa)#exit
Router(config-if)#destination 10.1.1.4
Router(config-if)#path-option 1 dynamic
Router(config-if)#commit

Router(config)#interface tunnel-te2
Router(config-if)#ipv4 unnumbered Loopback0
Router(config-if)#autoroute announce
Router(config-if-tunte-aa)#metric 1
Router(config-if-tunte-aa)#exit
Router(config-if)#destination 10.1.1.6
Router(config-if)#path-option 1 dynamic
Router(config-if)#exit
Router(config)#commit

/* Enable anycast-prefer-igp-cost with IS-IS */
Router#configure
Router(config)#router isis 100
Router(config-isis)#is-type level-2-only
Router(config-isis)#net 47.2377.50ea.ffff.988a.2d13.00
Router(config-isis)#address-family ipv4 unicast
Router(config-isis-af)#metric-style wide
Router(config-isis-af)#mpls traffic-eng level-2-only
Router(config-isis-af)#mpls traffic-eng router-id Loopback0
Router(config-isis-af)#mpls traffic-eng tunnel anycast-prefer-igp-cost
Router(config-isis-af)#maximum-paths 64
Router(config-isis-af)#commit
```

Running Configuration

```
Router#show running-config
interface tunnel-te1
 ipv4 unnumbered Loopback0
 autoroute announce
  metric 2
 !
 destination 10.1.1.4
 path-option 1 dynamic
!
interface tunnel-te2
 ipv4 unnumbered Loopback0
 autoroute announce
  metric 1
 !
 destination 10.1.1.6
 path-option 1 dynamic
!
router isis 100
 is-type level-2-only
 net 47.2377.50ea.ffff.988a.2d13.00
 address-family ipv4 unicast
  metric-style wide
```

```
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  mpls traffic-eng tunnel anycast-prefer-igp-cost
  maximum-paths 64
 !
!
end
```

Verification

When you enable **anycast-prefer-igp-cost**, the traffic is forwarded through tunnel-te1:

```
Router#show route 10.1.1.7/32
Routing entry for 10.1.1.7/32
  Known via "isis 100", distance 115, metric 12, type level-2
  Installed Nov  3 09:48:39.520 for 00:00:05
  Routing Descriptor Blocks
    10.1.1.4, from 10.1.1.4, via tunnel-te1
      Route metric is 20
```

When you disable **anycast-prefer-igp-cost**, the traffic is forwarded through tunnel-te2:

```
Router#show route 10.1.1.7/32
Routing entry for 10.1.1.7/32
  Known via "isis 100", distance 115, metric 11, type level-2
  Installed Nov  3 09:25:38.162 for 00:18:23
  Routing Descriptor Blocks
    10.1.1.6, from 10.1.1.6, via tunnel-te2
      Route metric is 11
```

Configure autoroute announce

This example shows how to configure IGP to use the tunnel in its enhanced SPF calculation when the tunnel is up:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RSP0/CPU0:router(config-if)# autoroute announce
```

Use the **autoroute announce include-ipv6** to announce the MPLS-TE tunnel to IS-IS IGP for IPv6 routing.

This example shows how an MPLS-TE tunnel can be announced to IS-IS IGP for IPv6 routing:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-te 65534
RP/0/RSP0/CPU0:router(config-if)# autoroute announce
RP/0/RSP0/CPU0:router(config-if-tunte-aa)# include-ipv6
```

This example shows how an MPLS-TE tunnel can be announced to IS-IS IGP for IPv6-only routing:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1
RP/0/RSP0/CPU0:router(config-if)# autoroute announce
RP/0/RSP0/CPU0:router(config-if-tunte-aa)# exclude-ipv4
RP/0/RSP0/CPU0:router(config-if-tunte-aa)# include-ipv6
```

The **autoroute announce metric** configuration allows you to specify the MPLS-TE tunnel metric that the Interior Gateway Protocol (IGP) enhanced Shortest Path First (SPF) calculation uses.

The **autoroute announce metric** configuration overrides the autoroute metric configuration, if present.

Configure IPv6-only autoroute announce over MPLS-TE tunnels

Perform these steps to configure IPv6-only autoroute announce over MPLS-TE tunnels:

Procedure

Step 1 **configure**

Step 2 **interface tunnel-te** *tunnel-id*

Example:

```
RP/0/RSP0/CPU0:router(config)# interface tunnel-te 1
```

Configures an MPLS-TE tunnel interface.

Step 3 **autoroute announce include-ipv6**

Example:

```
RP/0/RSP0/CPU0:router(config-if)# autoroute announce include-ipv6
```

Enables IPv6 autoroute announce.

Step 4 **exclude-ipv4**

Example:

```
RP/0/RSP0/CPU0:router(config-if-tunte-aa)# exclude-ipv4
```

Disables IPv4 autoroute announce.

Step 5 **commit**

Step 6 (Optional) **show mpls traffic-eng autoroute**

Example:

```
RP/0/RSP0/CPU0:router#show mpls traffic-eng autoroute

  Destination 192.168.0.2 has 1 tunnels in IS-IS ring level 1
    T1 (traffic share 0, nexthop 192.168.0.3,  metric 0)
    (IS-IS ring level-1, IPV6 Unicast)
    Signalled-Name: T1
```

Verifies that the tunnel announces IPv6-only autoroute information.

Event history for MPLS-TE tunnels

MPLS-TE tunnel event histories are network diagnostic records that

- chronologically document significant events and actions that occur within MPLS-TE headend tunnels
- enable detailed tracking and analysis of tunnel lifecycle changes, including RSVP signaling events, and
- facilitate monitoring, troubleshooting, and compliance by recording each event with timestamps and associated metadata.

Table 15: Feature History Table

Feature Name	Release	Feature Description
Event history for MPLS-TE headend tunnels	Release 25.4.1	This feature introduces a granular and configurable event tracking mechanism for operational visibility into MPLS-TE tunnels. You can enable event history with the **mpls traffic-eng event-history tunnel** command and set the number of tracked events with the **mpls traffic-eng event-history tunnel event-count** command. This feature introduces these changes: CLI: • Three new keywords, **event-history**, **tunnel**,and **event-count**, are added to the **mpls traffic-eng** command. • Two new keywords, **event-history**, and **tunnels** are added to the **show mpls traffic-eng** command. • A new **clear mpls traffic-eng event-history tunnels** command has been added. • The **show mpls traffic-eng counters global** and **show mpls traffic-eng chunks** commands have been modified to include the event history information.

Cisco IOS XR Release 25.4.1 introduces the tunnel event history for MPLS-TE tunnels to track and analyse the timeline of events in the tunnel lifecycle, including RSVP signaling. This feature enables enhanced operational visibility for MPLS-TE tunnels by providing granular, configurable event tracking.

To enable the MPLS-TE tunnel event history feature, use the **mpls traffic-eng event-history tunnel** command. To set the event count for the tunnel event history, configure the use the **mpls traffic-eng event-history tunnel event-count** command.

Benefits of tunnel event history

You can use the event history feature for MPLS-TE headend tunnels to:

- maintain a familiar workflow with minimal changes,

- log events in dedicated, per-tunnel buffers for fair and isolated event recording,
- flexibly capture and report events with comprehensive argument handling,
- compress duplicate events to minimize log size and clutter, and
- enhance debugging with accessible historical records for troubleshooting.

Restrictions for tunnel event history

The tunnel event history feature is:

- Disabled by default.
- Supported only on MPLS-TE headend tunnels.

Configure tunnel event history and event count

This procedure helps you to configure the tunnel event history and the event count.

Procedure

Step 1 Enable the tunnel event history.

Example:

```
Router# configure
Router(config)# mpls traffic-eng event-history tunnel
Router(config-te-evt-hist)# commit
```

Step 2 Specify the event count.

Example:

```
Router# configure
Router(config)# mpls traffic-eng event-history tunnel event-count 45
Router(config-te-evt-hist)# commit
```

The default number of events is 25. You can set up to 1000 events per tunnel.

Step 3 Verify the tunnel event history configuration.

Example:

This output shows the event history for all tunnels.

```
Router# show mpls traffic-eng event-history tunnel all
Wed Dec 3 14:08:59.529 UTC

Name: tunnel-te1
Event history (oldest first):
ID                   Time               LSP  Event-Type  Rep  Event-Message
01764770758196406124 Dec 3 14:06:05.309   2  Path          0  BW:300 kbps ERO: 10.1.3.103 10.3.5.105
 10.5.6.106 20.1.0.106
01764770758196406128 Dec 3 14:06:05.346   2  Path Err      0  (24,0), Error: routing (24), Suberror:
 none (0), error-node: 10.1.3.103
01764770758196406129 Dec 3 14:06:05.346   2  Path Tear     0
01764770758196406131 Dec 3 14:06:08.349   3  Path          0   BW:300 kbps ERO: 10.1.3.103 10.3.5.105
 10.5.6.106 20.1.0.106
01764770758196406132 Dec 3 14:06:08.449   3  Resv          0   BW:300 kbps RRO:
```

```
01764770758196406134 Dec 3 14:06:08.449   3  Oper State    0   New tunnel state: UP

Name: T10
Event history (oldest first):
ID                   Time               LSP  Event-Type  Rep  Event-Message
01764770758196406125 Dec 3 14:06:05.309   2  Path          0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104
 10.4.6.106 20.1.0.106
01764770758196406126 Dec 3 14:06:05.346   2  Path Err      0  (24,0), Error: routing (24), Suberror:
 none (0), error-node: 10.1.2.102
01764770758196406127 Dec 3 14:06:05.346   2  Path Tear     0
01764770758196406130 Dec 3 14:06:08.346   3  Path          0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104
 10.4.6.106 20.1.0.106
01764770758196406133 Dec 3 14:06:08.449   3  Resv          0  BW:300 kbps RRO:
01764770758196406135 Dec 3 14:06:08.496   3  Oper State    0  New tunnel state: UP

Name: SELFPING-101
 Event history (oldest first):
 ID                   Time                  LSP  Event-Type  Rep  Event-Message
 01769076278173248001  Jan 22 05:30:13.487    2  Path         0  BW:0 kbps ERO: 10.10.10.2 17.17.17.2
 17.17.17.3 22.22.22.3 22.22.22.4 192.168.0.4
 01769076278173248002  Jan 22 05:30:13.546    2  Resv         0  BW:0 kbps RRO:
 01769076278173248003  Jan 22 05:30:23.551    2  Self-Ping    0  Timed-out (started at Jan 22
05:01:30.769)
 01769076278173248004  Jan 22 05:30:23.554    2  Oper State   0  New tunnel state: UP

Name: SELFPING-103
 Event history (oldest first):
 ID                   Time                  LSP  Event-Type  Rep  Event-Message
 01769076278173248011  Jan 22 05:31:54.518    2  Path         0  BW:0 kbps ERO: 10.10.10.2 17.17.17.2
 17.17.17.3 22.22.22.3 22.22.22.4 192.168.0.4
 01769076278173248012  Jan 22 05:31:54.581    2  Resv         0  BW:0 kbps RRO:
 01769076278173248013  Jan 22 05:32:02.917    2  Self-Ping    0  Aborted (started at Jan 22
05:01:30.769)
 01769076278173248014  Jan 22 05:32:02.925    2  Path Tear    0
 01769076278173248015  Jan 22 05:32:02.936    3  Path         0  BW:0 kbps ERO: 11.11.11.2 17.17.17.2
 17.17.17.3 22.22.22.3 22.22.22.4 192.168.0.4
 01769076278173248016  Jan 22 05:32:02.987    3  Resv         0  BW:0 kbps RRO:
 01769076278173248017  Jan 22 05:32:06.994    3  Self-Ping    0  Succeeded (started at Jan 22
05:01:30.769)
 01769076278173248018  Jan 22 05:32:06.995    3  Oper State   0  New tunnel state: UP
```

Example:

This output shows the event history for a specific tunnel.

```
Router# show mpls traffic-eng event-history tunnels name tunnel-T10
Thu Dec 18 07:30:57.167 UTC
Name: tunnel-T10
 Event history (oldest first):
 ID                   Time                  LSP  Event-Type  Rep  Event-Message
 01765952238563713933  Jan 1 07:15:28.220    5  Path Tear    0
 01765952238563713934  Jan 1 07:15:32.660    8  Path         0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104

 01765952238563713935  Jan 1 07:15:32.763    8  Resv         0  BW:300 kbps RRO:
 01765952238563713936  Jan 1 07:15:32.803    6  Path Tear    0
 01765952238563713937  Jan 1 07:15:37.387    9  Path         0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104

 01765952238563713938  Jan 1 07:15:37.480    9  Resv         0  BW:300 kbps RRO:
 01765952238563713939  Jan 1 07:15:37.517    7  Path Tear    0
 01765952238563713940  Jan 1 07:15:47.193   10  Path         0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104

 01765952238563713941  Jan 1 07:15:47.283   10  Resv         0  BW:300 kbps RRO:
 01765952238563713942  Jan 1 07:15:47.320    8  Path Tear    0
 01765952238563713943  Jan 1 07:16:07.420    9  Path Tear    0
 01765952238563713944  Jan 1 07:16:15.573   11  Path         0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104
```

```
 01765952238563713945  Jan 1 07:16:15.670    11  Resv          0  BW:300 kbps RRO:
 01765952238563713946  Jan 1 12:23:05.711    10  Self-Ping     0  Succeeded (started at Jan  1
12:23:05.709)
 01765952238563713947  Jan 1 07:16:35.810    10  Path Tear     0
 01765952238563713948  Jan 1 07:22:49.863    12  Path          0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104

 01765952238563713949  Jan 1 07:22:49.963    12  Resv          0  BW:300 kbps RRO:
 01765952238563713950  Jan 1 07:23:10.103    11  Path Tear     0
 01765952238563713951  Jan 1 07:23:49.240    13  Path          0  BW:300 kbps ERO: 10.1.2.102 10.2.4.104

 01765952238563713952  Jan 1 07:23:49.340    13  Resv          0  BW:300 kbps RRO:
 01765952238563713953  Jan 1 07:24:09.480    12  Path Tear     0
 01765952238563713954  Jan 1 12:45:45.473    11  Self-Ping     0  Succeeded (started at Jan  1
12:45:45.472)
```

Example:

This output shows the specified event count.

```
Router# show run mpls traffic-eng event-history
Thu Dec 4 06:56:44.650 UTC
mpls traffic-eng
event-history
tunnel
event-count 45
!
!
!
```

Example:

This example shows the event history size.

```
Router# show mpls traffic-eng counters global

Wed Dec 3 14:09:38.405 UTC

Global Statistics:
Number of VIF : 2
Number of LSP : 2
Number of S2L : 2

Checkpoint request queue high watermark : 3
Checkpoint response queue high watermark : 16
Checkpoint reschedules : 28
Checkpoint enqueues (request queue) : 86
Checkpoint dequeues (request queue) : 86
Checkpoint enqueues (response queue) : 86
Checkpoint dequeues (response queue) : 86
Checkpoint write (VIF) : 32
Checkpoint read (VIF) : 0
Checkpoint write (DST) : 0
Checkpoint read (DST) : 0
Checkpoint write (S2L) : 4
Checkpoint read (S2L) : 0
Checkpoint write (Autobackup) : 0
Checkpoint read (Autobackup) : 0
Checkpoint write (PI backup) : 0
Checkpoint read (PI backup) : 0
Number of RSVP connection : 1
Number of RSVP disconnection : 0
Number of RSVP restart time change : 0
Number of LSD connection : 1
Number of LSD disconnection : 0
Number of LSD replay : 1
```

```
Number of LMRIB connection : 1
Number of LMRIB disconnection : 0
Number of LMRIB restart time change : 1
Number of LMRIB restart failed : 0
Number of LMRIB restart passed : 1
Number of LMRIB recovery failed : 0
Number of LMRIB recovery passed : 1
Number of RSI connection : 1
Number of RSI disconnection : 0
Event-history size (bytes)
 Tunnels (excluding chunks) : 16444912
```

Example:

This example displays the memory information for the tunnel event history.

```
Router# show mpls traffic-eng chunks

  Tue Dec  9 06:30:40.055 UTC
Pool name            InUse     Free      Allocs    Deallocs  Sib creat Sib trimm
-------------------- --------- --------- --------- --------- --------- ---------
mpls wavl Chunks             0     32000         0         0         0         0
mpls wavl Chunks            28      7972        28         0         0         0
mpls wavl Chunks           101      3899       101         0         0         0
mpls wavl Chunks            59      1941        59         0         0         0
mpls wavl Chunks            27       973        27         0         0         0
mpls wavl Chunks             9       491         9         0         0         0
mpls wavl Chunks             0       240         0         0         0         0
mpls wavl Chunks             0       120         0         0         0         0
TE S2L chunk                 0       200         0         0         0         0
TE S2L stats chunk           0      1024         0         0         0         0
TE LSP chunk                 0       200         0         0         0         0
TE collab chunk             15        25        15         0         0         0
TE FSM Q chunk               0       128         0         0         0         0
TE NextHop Route Po          0       128         0         0         0         0
TE Binding Sid Cont          0       128         0         0         0         0
TE CHKPT Q Elements          0       600        10        10         0         0
RSVP CHKPT LIST Chu          0      8192         0         0         0         0
TE Tunnel Service R          0       128         0         0         0         0
TE Tunnel Service R          0       128         0         0         0         0
RSVP API CTX                 0       156         0         0         0         0
RSVP API CTX stats           0        48         0         0         0         0
RSVP API CTX event           0      1248         0         0         0         0
RSVP API CTX event           0      1248         0         0         0         0
RSVP API CTX Histor          0      1248         0         0         0         0
TE S2L RW chunk              0       124         0         0         0         0
TE S2L RW chunk              0       128         0         0         0         0
TE Event History             0       200         0         0         0         0
VIF Pulse Context c          0      1024       668       668         0         0
```

Step 4 (Optional) Clear the tunnel event history for all tunnels, if required.

Example:

```
Router# clear mpls traffic-eng event-history tunnels all
```

Configuration Examples for Cisco MPLS-TE

These configuration examples are used for MPLS-TE:

Build MPLS-TE Topology and Tunnels: Example

The following examples show how to build an OSPF and IS-IS topology:

```
(OSPF)
...
configure
  mpls traffic-eng
  interface pos 0/6/0/0
  router id loopback 0
  router ospf 1
  router-id 192.168.25.66
  area 0
  interface pos 0/6/0/0
  interface loopback 0
  mpls traffic-eng router-id 192.168.70.1
  mpls traffic-eng area 0
  rsvp
  interface pos 0/6/0/0
  bandwidth 100
  commit
show mpls traffic-eng topology
show mpls traffic-eng link-management advertisement
!
(IS-IS)
...
configure
  mpls traffic-eng
  interface pos 0/6/0/0
  router id loopback 0
  router isis lab
  address-family ipv4 unicast
  mpls traffic-eng level 2
  mpls traffic-eng router-id 192.168.70.2
  !
  interface POS0/0/0/0
  address-family ipv4 unicast
!
```

The following example shows how to configure tunnel interfaces:

```
interface tunnel-te1
  destination 192.168.92.125
  ipv4 unnumbered loopback 0
  path-option l dynamic
  bandwidth 100
  commit
show mpls traffic-eng tunnels
show ipv4 interface brief
show mpls traffic-eng link-management admission-control
!
interface tunnel-te1
  autoroute announce
  route ipv4 192.168.12.52/32 tunnel-te1
  commit
ping 192.168.12.52
show mpls traffic autoroute
!
interface tunnel-te1
  fast-reroute
```

```
  mpls traffic-eng interface pos 0/6/0/0
  backup-path tunnel-te 2
  interface tunnel-te2
  backup-bw global-pool 5000
  ipv4 unnumbered loopback 0
  path-option l explicit name backup-path
  destination 192.168.92.125
 commit
show mpls traffic-eng tunnels backup
show mpls traffic-eng fast-reroute database
!
rsvp
  interface pos 0/6/0/0
  bandwidth 100 150 sub-pool 50
  interface tunnel-te1
  bandwidth sub-pool 10
commit
```

Related Topics

Building MPLS-TE Topology, on page 260
Creating an MPLS-TE Tunnel, on page 262
How MPLS-TE Works, on page 203

Configure IETF DS-TE Tunnels: Example

The following example shows how to configure DS-TE:

```
rsvp
 interface pos 0/6/0/0
 bandwidth rdm 100 150 bc1 50
 mpls traffic-eng
 ds-te mode ietf
 interface tunnel-te 1
 bandwidth 10 class-type 1
 commit

configure
 rsvp interface 0/6/0/0
 bandwidth mam max-reservable-bw 400 bc0 300 bc1 200
 mpls traffic-eng
 ds-te mode ietf
 ds-te model mam
 interface tunnel-te 1bandwidth 10 class-type 1
 commit



rsvp
 interface pos 0/6/0/0
 bandwidth rdm percentage bc0 100 bc1 50
 bandwidth 10 class-type 1
 commit

configure
 rsvp interface 0/6/0/0
 bandwidth mam percentage bc0 100 bc1 50
 ds-te mode ietf
 ds-te model mam
 bandwidth 10 class-type 1
```

```
commit
```

Related Topics

Configuring a Prestandard DS-TE Tunnel, on page 282
Prestandard DS-TE Mode, on page 208

Configure MPLS-TE and Fast-Reroute on OSPF: Example

CSPF areas are configured on a per-path-option basis. The following example shows how to use the traffic-engineering tunnels (tunnel-te) interface and the active path for the MPLS-TE tunnel:

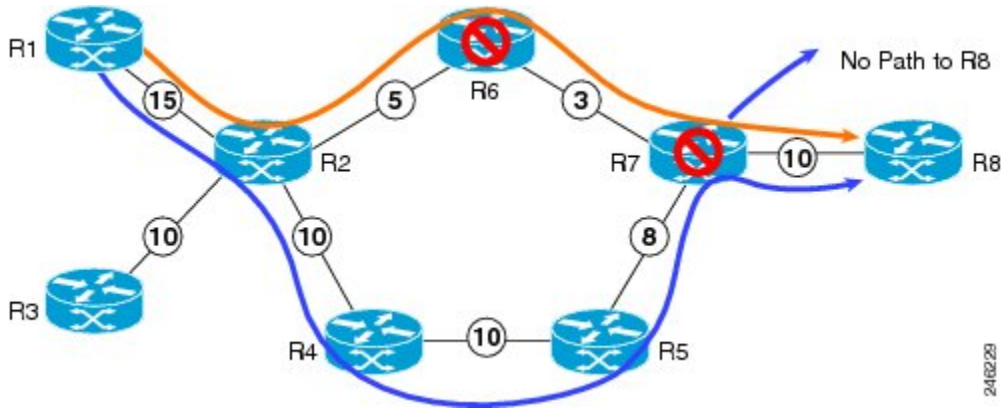
```
configure
 interface tunnel-te 0
  path-option 1 explicit id 6 ospf 126 area 0
  path-option 2 explicit name 234 ospf 3 area 7 verbatim
  path-option 3 dynamic isis mtbf level 1 lockdown
  commit
```

Configure the Ignore IS-IS Overload Bit Setting in MPLS-TE: Example

This example shows how to configure the IS-IS overload bit setting in MPLS-TE:

This figure illustrates the IS-IS overload bit scenario:

Figure 32: IS-IS overload bit



Consider a MPLS TE topology in which usage of nodes that indicated an overload situation was restricted. In this topology, the router R7 exhibits overload situation and hence this node can not be used during TE CSPF. To overcome this limitation, the IS-IS overload bit avoidance (OLA) feature was introduced. This feature allows network administrators to prevent RSVP-TE label switched paths (LSPs) from being disabled when a router in that path has its Intermediate System-to-Intermediate System (IS-IS) overload bit set.

The IS-IS overload bit avoidance feature is activated at router R1 using this command:

```
mpls traffic-eng path-selection ignore overload
```

```
configure
```

```
 mpls traffic-eng
  path-selection ignore overload
   commit
```

Related Topics

Configuring the Ignore Integrated IS-IS Overload Bit Setting in MPLS-TE, on page 289
Ignore Intermediate System-to-Intermediate System Overload Bit Setting in MPLS-TE, on page 212

Configure Flexible Name-based Tunnel Constraints: Example

The following configuration shows the three-step process used to configure flexible name-based tunnel constraints.

```
  R2
  line console
   exec-timeout 0 0
   width 250
  !
  logging console debugging
  explicit-path name mypath
   index 1 next-address loose ipv4 unicast 192.168.0.1 !
  explicit-path name ex_path1
   index 10 next-address loose ipv4 unicast 172.16.0.1  index 20 next-address loose ipv4
unicast 192.168.0.1 !
  interface Loopback0
   ipv4 address 10.22.22.22 255.255.255.255 !
  interface tunnel-te1
   ipv4 unnumbered Loopback0
   signalled-bandwidth 1000000
   destination 192.168.0.1
   affinity include green
   affinity include yellow
   affinity exclude indigo
   affinity exclude orange
   path-option 1 dynamic
  !
  router isis 1
   is-type level-1
   net 47.0001.0000.0000.0001.00
   nsf cisco
   address-family ipv4 unicast
    metric-style wide
    mpls traffic-eng level-1
    mpls traffic-eng router-id 192.168.70.1
   !
   interface Loopback0
    passive
    address-family ipv4 unicast
    !
   !
   interface GigabitEthernet0/1/0/0
    address-family ipv4 unicast
    !
   !
   interface GigabitEthernet0/1/0/1
    address-family ipv4 unicast
    !
   !
   interface GigabitEthernet0/1/0/2
```

```
  address-family ipv4 unicast
  !
 !
 interface GigabitEthernet0/1/0/3
  address-family ipv4 unicast
  !
 !
!
rsvp
 interface GigabitEthernet0/1/0/0
  bandwidth 1000000 1000000
 !
 interface GigabitEthernet0/1/0/1
  bandwidth 1000000 1000000
 !
 interface GigabitEthernet0/1/0/2
  bandwidth 1000000 1000000
 !
 interface GigabitEthernet0/1/0/3
  bandwidth 1000000 1000000
 !
!
mpls traffic-eng
 interface GigabitEthernet0/1/0/0
  attribute-names red purple
 !
 interface GigabitEthernet0/1/0/1
  attribute-names red orange
 !
 interface GigabitEthernet0/1/0/2
  attribute-names green purple
 !
 interface GigabitEthernet0/1/0/3
  attribute-names green orange
 !
 affinity-map red 1
 affinity-map blue 2
 affinity-map teal 80
 affinity-map green 4
 affinity-map indigo 40
 affinity-map orange 20
 affinity-map purple 10
 affinity-map yellow 8
!
```

Related Topics

Assigning Color Names to Numeric Values, on page 290
Associating Affinity-Names with TE Links, on page 291
Associating Affinity Constraints for TE Tunnels, on page 292
Flexible Name-based Tunnel Constraints, on page 213

Configure an Interarea Tunnel: Example

The following configuration example shows how to configure a traffic engineering interarea tunnel. .

Note Specifying the tunnel tailend in the loosely routed path is optional.

```
configure
  interface Tunnel-te1
    ipv4 unnumbered Loopback0
    destination 192.168.20.20
    signalled-bandwidth 300
    path-option 1 explicit name path-tunnel1

explicit-path name path-tunnel1
  index 10 next-address loose ipv4 unicast 192.168.40.40
  index 20 next-address loose ipv4 unicast 192.168.60.60
  index 30 next-address loose ipv4 unicast 192.168.20.20
```

The following configuration example shows how to configure loose-path retry period (range is 30 to 600 seconds) on headend router.

```
config
 mpls traffic-eng
  timers loose-path retry-period 120
```

The following configuration example shows the global configuration for loose hop expansion affinity or metric on ABR.

```
config
 mpls traffic-eng path-selection loose-expansion affinity 0xff
 mpls traffic-eng path-selection loose-expansion metric te class-type 5
```

Configure Forwarding Adjacency: Example

The following configuration example shows how to configure an MPLS-TE forwarding adjacency on tunnel-te 68 with a holdtime value of 60:

```
configure
 interface tunnel-te 68
 forwarding-adjacency holdtime 60
 commit
```

Related Topics

Configuring MPLS-TE Forwarding Adjacency, on page 296
MPLS-TE Forwarding Adjacency Benefits, on page 217

Configure PCE: Example

The following configuration example illustrates a PCE configuration:

```
configure
mpls traffic-eng
  interface pos 0/6/0/0
  pce address ipv4 192.168.25.66
  router id loopback 0
  router ospf 1
  router-id 192.168.25.66
  area 0
```

```
  interface pos 0/6/0/0
  interface loopback 0
  mpls traffic-eng router-id 192.168.70.1
  mpls traffic-eng area 0
  rsvp
  interface pos 0/6/0/0
  bandwidth 100
  commit
```

The following configuration example illustrates PCC configuration:

```
configure
  interface tunnel-te 10
  ipv4 unnumbered loopback 0
  destination 10.2.3.4
  path-option 1 dynamic pce
  mpls traffic-eng
  interface pos 0/6/0/0
  router id loopback 0
  router ospf 1
  router-id 192.168.25.66
  area 0
  interface pos 0/6/0/0
  interface loopback 0
  mpls traffic-eng router-id 192.168.70.1
  mpls traffic-eng area 0
  rsvp
  interface pos 0/6/0/0
  bandwidth 100
  commit
```

Related Topics

Configuring a Path Computation Client, on page 297
Configuring a Path Computation Element Address, on page 298
Configuring PCE Parameters, on page 299
Path Computation Element, on page 218

Configure Fast Repair: Example

The following example shows how to configure fast repair:

```
configure
 mpls traffic-eng
  pce
   stateful-client
    fast-repair
   !
  !
 !
```

Enable PCEP Cisco Extension: Example

The following example shows how to enable PCEP Cisco extension:

```
configure
 mpls traffic-eng
  pce
   stateful-client
    cisco-extension
   !
  !
 !
```

Configure PBTS for IPv4: Examples

These examples show how to configure PBTS for IPv4.

Create rules to classify the ingress packets such as ACL, DSCP, TOS, or EXP to different classes. Associate a forward-class to each type of ingress traffic.

Configure Access List

```
ipv4 access-list prec1
10 permit ipv4 any any precedence priority
!
ipv4 access-list prec2
10 permit ipv4 any any precedence immediate
!
```

Configure Class Map

The following example shows how to configure a classmap using ACL

```
class-map type traffic match-any prec1
match access-group ipv4 prec1
end-class-map
!
class-map type traffic match-any prec2
match access-group ipv4 prec2
end-class-map
!
```

Configure Policy Map

The following example shows how to configure a policy map:

```
policy-map type pbr prec
class type traffic prec1
  set forward-class 1
!
class type traffic prec3
  set forward-class 3
!
class type traffic class-default
!
end-policy-map
!
```

Configure Tunnel Interface

The following example shows how to configure an MPLS TE tunnel interface:

Set up one or more egress MPLS-TE to the destination. Associate the egress MPLS-TE to a forward-class.

```
interface tunnel-te61
ipv4 unnumbered Loopback0
signalled-bandwidth 1000
autoroute announce
destination 6.6.6.6
record-route
forward-class 1
path-option 1 explicit identifier 61
!
```

Configure Policy on a Interface

Enable PBTS on the ingress interface, by applying the service policy (Use already configured classification rules)

```
interface GigabitEthernet0/0/0/1.1
service-policy type pbr input prec
ipv4 address 22.1.1.1 255.255.255.0
encapsulation dot1q 1
!
```

Note

- Only one forward-class can be associated with a TE tunnel at any time.
- The router supports eight unique forwarding class values.
- Forwarding class zero is the default forwarding class and it doesn't require explicit configuration.

Configure PBTS for IPv6: Examples

These examples show how to configure PBTS for IPv6.

Configure Tunnel Interface: Example

The following example shows how to configure MPLS TE tunnel interface:

```
interface tunnel-te5500
 ipv4 unnumbered Loopback0
 ipv6 enable
 destination 19.0.0.1
 fast-reroute
 record-route
 forward-class 1
 forwarding-adjacency
  include-ipv6
 !
 path-option 1 explicit name pri
!
```

Configure Policy on Interface: Example

The following example shows how to configure policy on an interface:

```
interface HundredGigE0/0/0/1
 service-policy type pbr input dscp
```

```
 ipv4 address 111.111.1.1 255.255.255.0
 ipv4 unreachables disable
 ipv6 address 2001:111::1/64
 ipv6 unreachables disable
!
```

Configure Policy Map: Example

The following example shows how to configure policy map:

```
policy-map type pbr dscp
 class type traffic ef
  set forward-class 1
 !
 class type traffic af11
  set forward-class 2
 !
 class type traffic ipv6-ef
  set forward-class 1
 !
 class type traffic af21
  set forward-class 3
 !
 class type traffic af31
  set forward-class 4
 !
 class type traffic af41
  set forward-class 5
 !
 class type traffic class-default
 !
 end-policy-map
!
```

Configure Classmap: Example

The following example shows how to configure classmap using ACL and non ACL:

```
class-map type traffic match-any ef
 match access-group ipv4 acl1
 end-class-map
!
class-map type traffic match-any a11
 match dscp af11
 end-class-map
!

Access-List
ipv4 access-list acl1
 10 permit ipv4 any any dscp ef
!
```

Configure Tunnels for Path Protection: Example

The path protection feature is configured on only the source router. The dynamic path option is a prerequisite to configure a path protection.

```
interface tunnel-te150
 ipv4 unnumbered Loopback150
 autoroute announce
 destination 151.151.151.151
 affinity 11 mask 11
 path-protection
 path-option 2 explicit name p2mp3-p2mp4-p2mp5_1
 path-option 10 dynamic
```

Related Topics

Enabling Path Protection for an Interface, on page 305
Assigning a Dynamic Path Option to a Tunnel, on page 306
Forcing a Manual Switchover on a Path-Protected Tunnel, on page 307
Configuring the Delay the Tunnel Takes Before Reoptimization, on page 308
Path Protection, on page 228
Pre-requisites for Path Protection, on page 229
Restrictions for Path Protection, on page 229

Configure Automatic Bandwidth: Example

The following configuration example illustrates an automatic bandwidth configuration:

```
configure
 interface tunnel-te6
  auto-bw
   bw-limit min 10000 max 500000
   overflow threshold 50 min 1000 limit 3
   adjustment-threshold 20 min 1000
   application 180
```

Related Topics

Configuring the Collection Frequency, on page 309
Configuring the Automatic Bandwidth Functions, on page 311
MPLS-TE Automatic Bandwidth Overview, on page 230

Configure the MPLS-TE Shared Risk Link Groups: Example

The following configuration example shows how to specify the SRLG value of each link that has a shared risk with another link:

```
config t
srlg
    interface POS0/4/0/0
         value 10
         value 11
    |
    interface POS0/4/0/1
         value 10
    |
```

The following example shows the SRLG values configured on a specific link.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng topology brief
My_System_id: 100.0.0.2 (OSPF 0 area 0)
My_System_id: 0000.0000.0002.00 (IS-IS 1 level-1)
My_System_id: 0000.0000.0002.00 (IS-IS 1 level-2)
My_BC_Model_Type: RDM

Signalling error holddown: 10 sec Global Link Generation 389225

IGP Id: 0000.0000.0002.00, MPLS TE Id: 100.0.0.2 Router Node  (IS-IS 1 level-1)

IGP Id: 0000.0000.0002.00, MPLS TE Id: 100.0.0.2 Router Node  (IS-IS 1 level-2)

    Link[1]:Broadcast, DR:0000.0000.0002.07, Nbr Node Id:21, gen:389193
      Frag Id:0, Intf Address:51.2.3.2, Intf Id:0
      Nbr Intf Address:51.2.3.2, Nbr Intf Id:0
      TE Metric:10, IGP Metric:10, Attribute Flags:0x0
      Attribute Names:
      SRLGs: 1, 4, 5
      Switching Capability:, Encoding:
      BC Model ID:RDM
      Physical BW:1000000 (kbps), Max Reservable BW Global:10000 (kbps)
      Max Reservable BW Sub:10000 (kbps)
```

The following example shows the configured tunnels and associated SRLG values.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels

<snip>
Signalling Summary:
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 1363 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 181 seconds
          Auto-bw enabled tunnels:  0 (disabled)

Name: tunnel-te1  Destination: 100.0.0.3
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: recovered

    path option 1,  type explicit path123 (Basis for Setup, path weight 2)
          OSPF 0 area 0
    G-PID: 0x0800 (derived from egress interface properties)
    SRLGs excluded: 2,3,4,5
                    6,7,8,9
    Bandwidth Requested: 0 kbps  CT0
<snip>
```

The following example shows all the interfaces associated with SRLG.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng topo srlg
My_System_id: 100.0.0.5 (OSPF 0 area 0)
My_System_id: 0000.0000.0005.00 (IS-IS 1 level-2)
My_System_id: 0000.0000.0005.00 (IS-IS ISIS-instance-123 level-2)

      SRLG      Interface Addr  TE Router ID    IGP Area  ID
__________      _______________  ____________    _______________
```

```
        10      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
        11      50.2.3.3        100.0.0.3       IS-IS 1 level-2
        12      50.2.3.3        100.0.0.3       IS-IS 1 level-2
        30      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
        77      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
        88      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
      1500      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
  10000000      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
4294967290      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
4294967295      50.4.5.5        100.0.0.5       IS-IS ISIS-instance-123 level-2
```

The following example shows the NHOP and NNHOP backup tunnels with excluded SRLG values.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng topology path dest 100.0.0.5 exclude-srlg
ipaddr
Path Setup to 100.0.0.2:
bw 0 (CT0), min_bw 0, metric: 30
setup_pri 7, hold_pri 7
affinity_bits 0x0, affinity_mask 0xffff
Exclude SRLG Intf Addr : 50.4.5.5
SRLGs Excluded :  10, 30, 1500, 10000000, 4294967290, 4294967295
Hop0:50.5.1.5
Hop1:50.5.1.1
Hop2:50.1.3.1
Hop3:50.1.3.3
Hop4:50.2.3.3
Hop5:50.2.3.2
Hop6:100.0.0.2
```

The following example shows an extract of explicit-path set to protect a specific interface.

```
RP/0/RSP0/CPU0:router#sh mpls traffic-eng topology path dest 10.0.0.5 explicit-path name
name

Path Setup to 100.0.0.5:
bw 0 (CT0), min_bw 9999, metric: 2
setup_pri 7, hold_pri 7
affinity_bits 0x0, affinity_mask 0xffff
SRLGs Excluded: 10, 30, 77, 88, 1500, 10000000
                4294967290, 4294967295

Hop0:50.3.4.3
Hop1:50.3.4.4
Hop2:50.4.5.4
Hop3:50.4.5.5
Hop4:100.0.0.5
```

Related Topics

Configuring the SRLG Values of Each Link that has a Shared Risk with Another Link, on page 313
Creating an Explicit Path With Exclude SRLG, on page 315
Using Explicit Path With Exclude SRLG, on page 316
Creating a Link Protection on Backup Tunnel with SRLG Constraint, on page 318
Creating a Node Protection on Backup Tunnel with SRLG Constraint, on page 321
MPLS Traffic Engineering Shared Risk Link Groups, on page 237
Explicit Path, on page 238

Fast ReRoute with SRLG Constraints, on page 239
Importance of Protection, on page 240
Delivery of Packets During a Failure, on page 241
Multiple Backup Tunnels Protecting the Same Interface, on page 241
Weighted-SRLG Auto-backup Path Computation, on page 241
SRLG Limitations, on page 242
MPLS TE SRLG Scale Enhancements, on page 242

Configure BFD and SRLG Diverse Path-Protection Under Named TE Tunnels

Table 16: Feature History Table

Feature Name	Release Information	Feature Description
Configure BFD and SRLG Diverse Path-Protection Under Named TE Tunnels	Release 7.6.1	Instead of using number IDs, you can now use a string to name MPLS-TE tunnels while configuring Bidirectional Forwarding Detection (BFD) and Shared Risk Link Group (SRLG) diverse path protection. Unlike number IDs, tunnel names are unique across all the routers in your network. This facilitates faster troubleshooting as you use the **show mpls traffic-eng named-tunnels** command to check that the BFD and SRLG configurations meet specified performance requirements.

The following example shows how to configure BFD and SRLG diverse path-protection under named TE tunnels:

```
RP/0/RP0/CPU0:router#config
Wed Feb 16 10:30:55.346 -07
RP/0/RP0/CPU0:router(config)#mpls traffic-eng
RP/0/RP0/CPU0:router(config-mpls-te)# named-tunnels
RP/0/RP0/CPU0:router(config-te-named-tunnels)#tunnel-te TUNNEL-NY-TO-LA
RP/0/RP0/CPU0:router(config-te-tun-name)#destination 202.158.0.1
RP/0/RP0/CPU0:router(config-te-tun-name)#path-protection srlg-diverse
RP/0/RP0/CPU0:router(config-te-tun-name)#bfd
RP/0/RP0/CPU0:router(config-mpls-te-tun-bfd)#multiplier 3
RP/0/RP0/CPU0:router(config-mpls-te-tun-bfd)#fast-detect
RP/0/RP0/CPU0:router(config-mpls-te-tun-bfd)#minimum-interval 300
RP/0/RP0/CPU0:router(config-mpls-te-tun-bfd)#path-option BEST
RP/0/RP0/CPU0:router(config-po-name)#preference 10
RP/0/RP0/CPU0:router(config-po-name)#computation dynamic
```

Verification

This log displays the configured BFD and SRLG diverse path protection for named tunnels:

```
RP/0/RP0/CPU0:router(config)#show mpls traffic-eng named-tunnels
    tunnel-te TUNNEL-NY-TO-LA
      bfd
       multiplier 3
       fast-detect
       minimum-interval 300
    path-option BEST
       preference 10
       computation dynamic
     destination 202.158.0.1
     path-protection
       srlg-diverse
end
```

Configure the MPLS-TE Auto-Tunnel Backup: Example

Table 17: Feature History Table

Feature Name	Release Information	Feature Description
Bandwidth Protection Functions to Enhance auto-tunnel backup Capabilities	Release 7.5.1	This feature introduces bandwidth protection functions for auto-tunnel backups, such as signaled bandwidth, bandwidth protection, and soft-preemption. These functions provide better bandwidth usage and prevent traffic congestion and traffic loss. In earlier releases, auto-tunnel backups provided only link protection and node protection. Backup tunnels were signaled with zero bandwidth, causing traffic congestion when FRR went active. This feature introduces the following commands and keywords: • **bandwidth-protection maximum-aggregate** • **signalled-bandwidth** • **soft-preemption**

The following example shows the auto-tunnel backup configuration for core or edge routers.

```
RP/0/RSP0/CPU0:router(config)#
mpls traffic-eng
    auto-tunnel backup
        tunnel-id min 60000 max 61000

    interface pos 0/1/0/0
       auto-tunnel backup
```

```
          attribute-set ab
```

The following example shows the protection (NNHOP and SRLG) that was set on the auto-tunnel backup.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels 1
Signalling Summary:
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 2524 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 49 seconds
          Auto-bw enabled tunnels:  1

Name: tunnel-te1  Destination: 200.0.0.3 (auto backup)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10,  type explicit (autob_nnhop_srlg_tunnel1) (Basis for Setup, path weight
 11)
    path option 20,  type explicit (autob_nnhop_tunnel1)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Fri Jul 10 01:53:25.581 PST  (1h 25m 17s ago)

  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
  Auto Backup:
     Protected LSPs: 4
     Protected S2L Sharing Families: 0
     Protected S2Ls: 0
     Protected i/f: Gi0/1/0/0     Protected node: 20.0.0.2
     Protection: NNHOP+SRLG
     Unused removal timeout: not running
  History:
    Tunnel has been up for: 00:00:08
    Current LSP:
      Uptime: 00:00:08
    Prior LSP:
      ID: path option 1 [545]
      Removal Trigger: configuration changed

  Path info (OSPF 0 area 0):
  Hop0: 10.0.0.2
  Hop1: 100.0.0.2
  Hop2: 100.0.0.3
  Hop3: 200.0.0.3
```

The following example shows automatically created path options for this backup auto-tunnel.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels 1 detail
Signalling Summary:
```

```
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
           Periodic reoptimization:  every 3600 seconds, next in 2524 seconds
            Periodic FRR Promotion:  every 300 seconds, next in 49 seconds
           Auto-bw enabled tunnels:  1

Name: tunnel-te1  Destination: 200.0.0.3 (auto backup)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10,  type explicit (autob_nnhop_srlg_tunnel1) (Basis for Setup, path weight
 11)
    path option 20,  type explicit (autob_nnhop_tunnel1)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Fri Jul 10 01:53:25.581 PST  (1h 25m 17s ago)

  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
  Auto Backup (NNHOP+SRLG):
     Protected LSPs: 4
     Protected S2L Sharing Families: 0
     Protected S2Ls: 0
     Protected i/f: Gi0/1/0/0     Protected node: 20.0.0.2
     Protection: NNHOP+SRLG
     Unused removal timeout: not running

     Path Options Details:
      10: Explicit Path Name: (autob_nnhop_srlg_te1)
        1: exclude-srlg 50.0.0.1
        2: exclude-address 50.0.0.2
        3: exclude-node 20.0.0.2
      20: Explicit Path Name: (autob_nnhop_te1)
        1: exclude-address 50.0.0.1
        2: exclude-address 50.0.0.2
        3: exclude-node 20.0.0.2
  History:
    Tunnel has been up for: 00:00:08
    Current LSP:
      Uptime: 00:00:08
    Prior LSP:
      ID: path option 1 [545]
      Removal Trigger: configuration changed

  Path info (OSPF 0 area 0):
  Hop0: 10.0.0.2
  Hop1: 100.0.0.2
  Hop2: 100.0.0.3
  Hop3: 200.0.0.3
```

This example shows the automatically created backup tunnels.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels brief
```

```
            TUNNEL NAME          DESTINATION      STATUS  STATE
              tunnel-te0           200.0.0.3          up  up
              tunnel-te1           200.0.0.3          up  up
              tunnel-te2           200.0.0.3          up  up
            tunnel-te50           200.0.0.3          up  up
            *tunnel-te60          200.0.0.3          up  up
            *tunnel-te70          200.0.0.3          up  up
            *tunnel-te80          200.0.0.3          up  up

RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels tabular
            Tunnel    LSP     Destination          Source             FRR    LSP  Path
              Name     ID         Address         Address   State   State   Role  Prot
------------------ ------ --------------- --------------- ------- ------- ------ -----
        tunnel-te0    549       200.0.0.3       200.0.0.1      up   Inact   Head InAct
        tunnel-te1    546       200.0.0.3       200.0.0.1      up   Inact   Head InAct
        tunnel-te2      6       200.0.0.3       200.0.0.1      up   Inact   Head InAct
      tunnel-te50       6       200.0.0.3       200.0.0.1      up  Active   Head InAct
      tunnel-te60       4       200.0.0.3       200.0.0.1      up  Active   Head InAct
      tunnel-te70       4       200.0.0.3       200.0.0.1      up  Active   Head InAct
      tunnel-te80       3       200.0.0.3       200.0.0.1      up  Active   Head InAct
```

This example shows the auto-tunnel backup details.

```
RP/0/RSP0/CPU0:router#  show mpls traffic-eng tunnels auto-tunnel backup detail

Name: tunnel-te400  Destination: 10.0.0.1 (auto-tunnel backup)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 20,  type explicit (autob_nnhop_te400) (Basis for Setup, path weight 2)
    path option 10,  type explicit (autob_nnhop_srlg_te400) [disabled]
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Thu Aug 16 18:30:41 2012 (00:01:28 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7 Affinity: 0x0/0xffff
    Metric Type: TE (default)
    Metric Type: TE (default)
    Hop-limit: disabled
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
    Soft Preemption: Disabled
  Auto Backup:
    Protected LSPs: 1
    Protected S2L Sharing Families: 0
    Protected S2L: 0
    Protected i/f: Gi0/1/0/3    Protected node: 192.168.0.1
    Attribute-set: ab1
    Protection: NNHOP
    Unused removal timeout: not running
    Path Option Details:
      10: Explicit Path Name: (autob_nnhop_srlg_te400)
        1: exclude-srlg 34.9.0.4
        2: exclude-address 34.9.0.3
        3: exclude-node 192.168.0.1
      20: Explicit Path Name: (autob_nnhop_te400)
        1: exclude-address 34.9.0.4
        2: exclude-address 34.9.0.3
        3: exclude-node 192.168.0.1
  SNMP Index: 221
```

```
  History:
    Tunnel has been up for: 00:00:34 (since Thu Aug 16 18:31:35 EST 2012)
    Current LSP:
      Uptime: 00:00:34 (since Thu Aug 16 18:31:35 EST 2012)
  Current LSP Info:
    Instance: 2, Signaling Area: OSPF 100 area 10.2.3.4
    Uptime: 00:00:34 (since Thu Aug 16 18:31:35 EST 2012)
    Outgoing Interface: GigabitEthernet0/1/0/2, Outgoing Label: 16000
    Router-IDs: local      209.165.201.1
                downstream 172.16.0.1
    Soft Preemption: None
    Path Info:
      Outgoing:
        Explicit Route:
          Strict, 24.9.0.2
          Strict, 12.9.1.1
          Strict, 10.0.0.1

      Record Route: Empty
      Tspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
                          Soft Preemption Desired: Not Set
    Resv Info:
      Record Route:
        IPv4 24.9.0.2, flags 0x0
        IPv4 12.9.1.1, flags 0x0
      Fspec: avg rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Displayed 1 (of 104) heads, 0 (of 0) midpoints, 0 (of 201) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This example shows the automatically created backup tunnels.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels auto-tunnel backup tabular

           Tunnel   LSP     Destination          Source    Tun    FRR  LSP  Path
             Name    ID         Address         Address  State  State Role  Prot
----------------- ----- --------------- --------------- ------ ------ ---- -----
    *tunnel-te400     2         10.0.0.1         209.165.201.1     up  Inact Head Inact
    *tunnel-te401     2         192.168.0.1         209.165.201.1     up  Inact Head Inact
* = automatically created backup tunnel

RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels auto-tunnel backup brief
           TUNNEL NAME         DESTINATION      STATUS  STATE
         *tunnel-te400            10.0.0.1          up  up
         *tunnel-te401            192.168.0.1          up  up
* = automatically created backup tunnel
Displayed 2 (of 104) heads, 0 (of 0) midpoints, 0 (of 201) tails
Displayed 2 up, 0 down, 0 recovering, 0 recovered heads
```

This example shows the attribute-set for auto-backup tunnels.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng attribute-set auto-backup

Attribute Set Name: ab (Type: auto-backup)
  Number of affinity constraints: 2
     Include bit map       : 0x4
     Include name          : blue
     Exclude bit map       : 0x2
     Exclude name          : red
  Priority: 7 7 (Default)
  Record-route: Enabled
```

```
  Policy-class: 1
  Logging: reoptimize, state
  List of protected interfaces (count 1)
      POS0_3_0_1
  List of tunnel IDs (count 1)
    3000
```

This example shows the attribute-set for auto-mesh tunnels.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng attribute-set auto-mesh

Attribute Set Name: am (Type: auto-mesh)
  Bandwidth: 100 kbps (CT0)
  Number of affinity constraints: 2
     Include bit map       : 0x8
     Include name          : yellow
     Exclude bit map       : 0x2
     Exclude name          : red
  Priority: 2 2
  Interface Bandwidth: 0 kbps (Default)
  AutoRoute Announce: Disabled
  Auto-bw: Disabled
  Soft Preemption: Disabled
  Fast Reroute: Enabled, Protection Desired: Node, Bandwidth
  Record-route: Enabled
  Policy-class: 0 (Not configured)
  Logging: None
  List of Mesh Groups (count 1)
    1
```

This example shows the details about the tunnel that is using auto-backup type of attribute-set.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels attribute-set auto-backup ab

Name: tunnel-te3000  Destination: 10.0.0.1 (auto-tunnel backup)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 20,  type explicit (autob_nhop_te3000) (Basis for Setup, path weight 2)
    path option 10,  type explicit (autob_nhop_srlg_te3000) [disabled]
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 0 kbps  CT0
    Creation Time: Tue Aug 14 23:24:27 2012 (00:05:28 ago)
  Config Parameters:
    Bandwidth:        0 kbps (CT0) Priority:  7  7
    Number of affinity constraints: 2
       Include bit map       : 0x4
       Include name          : blue
       Exclude bit map       : 0x2
       Exclude name          : red

    Metric Type: TE (default)
    Hop-limit: disabled
    AutoRoute: disabled  LockDown: disabled   Policy class: 1
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Disabled, Protection Desired: None
    Path Protection: Not Enabled
    Soft Preemption: Disabled
  Auto Backup:
    Protected LSPs: 2
    Protected S2L Sharing Families: 0
    Protected S2L: 0
```

```
    Protected i/f: PO0/3/0/1
    Attribute-set: ab
    Protection: NHOP
    Unused removal timeout: not running
  History:
    Tunnel has been up for: 00:04:57 (since Tue Aug 14 23:24:58 EST 2012)
    Current LSP:
      Uptime: 00:04:57 (since Tue Aug 14 23:24:58 EST 2012)

  Path info (OSPF 100 area 16909060):
  Node hop count: 2
  Hop0: 23.9.0.2
  Hop1: 12.9.0.2
  Hop2: 12.9.0.1
  Hop3: 10.0.0.1
Displayed 1 (of 7) heads, 0 (of 3) midpoints, 0 (of 0) tails Displayed 1 up, 0 down, 0
recovering, 0 recovered heads
```

This example shows the protected interface for auto-backup auto-tunnels.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels backup protected-interface

Interface: Gi0/2/0/1 (auto-tunnel backup)
  SRLG: N/A, NHOP-only: No
  Attribute-set: Not configured
  Auto-tunnel backup recreate time remaining:  timer not running
    No backup tunnel found

Interface: Gi0/2/0/3
     tunnel-te340   PROTECTED : out i/f:   PO0/3/0/2   Admin:   up  Oper:   up

Interface: PO0/3/0/1 (auto-tunnel backup)
  SRLG: N/A, NHOP-only: No
  Attribute-set: ab
  Auto-tunnel backup recreate time remaining:  timer not running
    *tunnel-te3000        NHOP : out i/f:   Gi0/2/0/2   Admin:   up  Oper:   up

 * = automatically created backup tunnel
```

This example shows the details about all the tunnels that are using auto-mesh type of attribute-set.

```
RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels attribute-set auto-mesh all

Name: tunnel-te3501  Destination: 10.0.0.1 (auto-tunnel mesh)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10,  type dynamic  (Basis for Setup, path weight 2)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 100 kbps  CT0
    Creation Time: Tue Aug 14 23:25:41 2012 (00:06:13 ago)
  Config Parameters:
    Bandwidth:      100 kbps (CT0) Priority:  2  2
    Number of affinity constraints: 2
       Include bit map       : 0x8
       Include name          : yellow
       Exclude bit map       : 0x2
       Exclude name          : red

    Metric Type: TE (default)
    Hop-limit: disabled
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
```

```
    Auto-bw: disabled
    Fast Reroute: Enabled, Protection Desired: Node, Bandwidth
    Path Protection: Not Enabled
    Attribute-set: am (type auto-mesh)
    Soft Preemption: Disabled
  Auto-tunnel Mesh:
    Group ID: 1
    Destination list: blah
    Unused removal timeout: not running
  History:
    Tunnel has been up for: 00:06:13 (since Tue Aug 14 23:25:41 EST 2012)
    Current LSP:
      Uptime: 00:06:13 (since Tue Aug 14 23:25:41 EST 2012)

  Path info (OSPF 100 area 16909060):
  Node hop count: 2
  Hop0: 23.9.0.2
  Hop1: 12.9.0.2
  Hop2: 12.9.0.1
  Hop3: 10.0.0.1

Name: tunnel-te3502  Destination: 172.16.0.1 (auto-tunnel mesh)
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10,  type dynamic  (Basis for Setup, path weight 1)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 100 kbps  CT0
    Creation Time: Tue Aug 14 23:25:41 2012 (00:06:13 ago)
  Config Parameters:
    Bandwidth:      100 kbps (CT0) Priority:  2  2
    Number of affinity constraints: 2
       Include bit map       : 0x8
       Include name          : yellow
       Exclude bit map       : 0x2
       Exclude name          : red

    Metric Type: TE (default)
    Hop-limit: disabled
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Enabled, Protection Desired: Node, Bandwidth
    Path Protection: Not Enabled
    Attribute-set: am (type auto-mesh)
    Soft Preemption: Disabled
  Auto-tunnel Mesh:
    Group ID: 1
    Destination list: blah
    Unused removal timeout: not running
  History:
    Tunnel has been up for: 00:06:13 (since Tue Aug 14 23:25:41 EST 2012)
    Current LSP:
      Uptime: 00:06:13 (since Tue Aug 14 23:25:41 EST 2012)

  Path info (OSPF 100 area 16909060):
  Node hop count: 1
  Hop0: 23.9.0.2
  Hop1: 172.16.0.1

Name: tunnel-te3503  Destination: 209.165.201.1 (auto-tunnel mesh)
  Status:
    Admin:    up Oper: down   Path: not valid   Signalling: Down
```

```
    path option 10,  type dynamic
    Last PCALC Error: Tue Aug 14 23:31:26 2012
      Info: No path to destination, 209.165.201.1 (affinity)
    G-PID: 0x0800 (derived from egress interface properties)
    Bandwidth Requested: 100 kbps  CT0
    Creation Time: Tue Aug 14 23:25:41 2012 (00:06:13 ago)
  Config Parameters:
    Bandwidth:      100 kbps (CT0) Priority:  2  2
    Number of affinity constraints: 2
       Include bit map       : 0x8
       Include name          : yellow
       Exclude bit map       : 0x2
       Exclude name          : red

    Metric Type: TE (default)
    Hop-limit: disabled
    AutoRoute: disabled  LockDown: disabled   Policy class: not set
    Forwarding-Adjacency: disabled
    Loadshare:          0 equal loadshares
    Auto-bw: disabled
    Fast Reroute: Enabled, Protection Desired: Node, Bandwidth
    Path Protection: Not Enabled
    Attribute-set: am (type auto-mesh)
    Soft Preemption: Disabled
  Auto-tunnel Mesh:
    Group ID: 1
    Destination list: blah
    Unused removal timeout: not running
Displayed 3 (of 7) heads, 0 (of 3) midpoints, 0 (of 0) tails Displayed 2 up, 1 down, 0
recovering, 0 recovered heads
```

Bandwidth Protection Functions to Enhance auto-tunnel backup Capabilities

Without bandwidth protection, auto-tunnel backups provide only link protection and node protection (per next-next-hop), and backup tunnels are signalled with zero bandwidth. This causes traffic congestion when FRR goes active, since the backup tunnels might be protecting huge amount of data, such as LSPs with large bandwidth or multiple LSPs.

To address the congestion issue, bandwidth protection capabilities are added for auto-tunnel backups. Bandwidth protection, signalled bandwidth, and soft-preemption settings are provided. Details:

- *Bandwidth protection* – A link or node protection backup might not provide bandwidth protection. But with this setting (**bandwidth-protection maximum-aggregate**), you can set the maximum bandwidth value that an auto-tunnel can protect.
- *Signalled bandwidth* – Without bandwidth protection, auto-tunnel backups are signaled with zero bandwidth too, with no guarantee that at least some bandwidth is backed up. So, the backup tunnels might be setup on links that are highly utilized, causing congestion drops when the backup tunnels start to transmit traffic after FRR is triggered.

  This setting (**signalled-bandwidth**) addresses the issue, since you can set the signalled bandwidth of the tunnel (and reserve minimal bandwidth for an auto-tunnel backup). When you set the signal bandwidth value for auto-backup tunnels, congestion over backup links reduces.
- *Soft-preemption* – Since bandwidth can be reserved for autobackup tunnels, a setting (**soft-preemption**) is provided for soft-preemption of the reserved bandwidth, if it is needed for a higher-priority tunnel.

Configurations

```
/*Enable Bandwidth Protection On a TE Auto-Tunnel Backup*/
```

```
Router# configure
Router(config)# mpls traffic-eng
Router(config-mpls-te)# interface GigabitEthernet 0/2/0/0 auto-tunnel backup
Router(config-te-if-auto-backup)# bandwidth-protection maximum-aggregate 100000
Router(config-te-if-auto-backup)# commit

/*Enable Signalled Bandwidth On a TE Auto-Tunnel Backup*/

Router# configure
Router(config)# mpls traffic-eng attribute-set auto-backup MyBackupConfig
Router(config-te-attribute-set)# signalled-bandwidth 700000
Router(config-te-attribute-set)# commit
```

After creating the auto backup attribute-set (**MyBackupConfig** in this case), associate with the auto-tunnel backup interface.

```
Router# configure
Router(config)# mpls traffic-eng
Router(config-mpls-te)# interface GigabitEthernet 0/2/0/0 auto-tunnel backup
Router(config-te-if-auto-backup)# attribute-set MyBackupConfig
Router(config-te-if-auto-backup)# auto-tunnel backup tunnel-id min 6000 max 6500
Router(config-mpls-te)# commit

/*Enable Soft-Preemption Bandwidth On a TE Auto-Tunnel Backup*/

Router# configure
Router(config)# mpls traffic-eng attribute-set auto-backup MyBackupConfig
Router(config-te-attribute-set)# soft-preemption
Router(config-te-attribute-set)# commit
```

Verification

```
/*Verify Auto-Tunnel Backup Configuration*/
```

In the output, bandwidth protection details are displayed, as denoted by *BW*.

```
Router# show mpls traffic-eng auto-tunnel backup

AutoTunnel Backup Configuration:
    Interfaces count: 1
    Unused removal timeout: 1h 0m 0s
    Configured tunnel number range: 6000-6500

AutoTunnel Backup Summary:
    AutoTunnel Backups:
             0 created, 0 up, 0 down, 0 unused
            0 NHOP, 0 NNHOP, 0 SRLG strict, 0 SRLG preferred, 0 SRLG weighted, 0 BW protected

  Protected LSPs:
             0 NHOP, 0 NHOP+SRLG, 0 NHOP+BW, 0 NHOP+BW+SRLG
             0 NNHOP, 0 NNHOP+SRLG, 0 NNHOP+BW, 0 NNHOP+BW+SRLG
    Protected S2L Sharing Families:
             0 NHOP, 0 NHOP+SRLG, 0 NNHOP+BW, 0 NNHOP+BW+SRLG
             0 NNHOP, 0 NNHOP+SRLG, 0 NNHOP+BW, 0 NNHOP+BW+SRLG
    Protected S2Ls:
             0 NHOP, 0 NHOP+SRLG, 0 NNHOP+BW, 0 NNHOP+BW+SRLG
             0 NNHOP, 0 NNHOP+SRLG, 0 NNHOP+BW, 0 NNHOP+BW+SRLG

 Cumulative Counters (last cleared 00:08:47 ago):
                        Total   NHOP  NNHOP
    Created:                0       0      0
    Connected:              0       0      0
    Removed (down):         0       0      0
    Removed (unused):       0       0      0
    Removed (in use):       0       0      0
    Range exceeded:         0       0      0
```

Related Topics

Enabling an AutoTunnel Backup, on page 277
Removing an AutoTunnel Backup, on page 278
Establishing MPLS Backup AutoTunnels to Protect Fast Reroutable TE LSPs, on page 279
Establishing Next-Hop Tunnels with Link Protection, on page 280
Backup AutoTunnels, on page 204

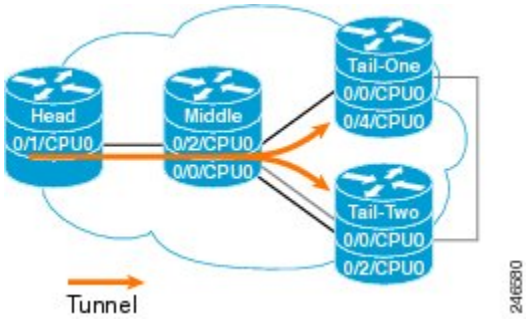
Configure Point-to-Multipoint TE: Examples

These configuration examples show how to configure Point-to-Multipoint TE:

P2MP Topology Scenario: Example

This section describes a typical scenario of point-to-multipoint traffic engineering toplogy. This figure illustrates the P2MP toplogy.

Figure 33: P2MP Topology



This head router describes the configuration at head node. This router does the imposition of MPLS at head node.

```
interface tunnel-mte1
 ipv4 unnumbered Loopback0
 destination 10.0.0.1
  path-option 1 explicit name path-to-tail1
 !
 destination 172.16.0.1
  path-option 1 explicit name path-to-tail2
 !
 fast-reroute

mpls traffic-eng
 interface GigabitEthernet0/1/3/0
!
 interface GigabitEthernet0/1/3/7
 !

multicast-routing
 address-family ipv4
  nsf
  interface all enable
 !
 address-family ipv6
  nsf
  interface all enable
```

```
 !
!
 !
router igmp
 vrf default
  interface tunnel-mte1
   static-group 232.0.0.1 192.168.10.1
  !
```

This mid router describes the configuration at mid node. This router performs the role of MPLS label replication at mid node.

```
mpls traffic-eng
 interface POS0/2/0/0
 !
 interface POS0/2/0/1
  backup-path tunnel-te 1000
 !
 interface TenGigE0/3/0/3
 !
 interface GigabitEthernet0/2/5/0
 !
!
```

This tail router describes the configuration at tail node. This router performs the role of MPLS disposition at tail node.

```
mpls traffic-eng
 interface POS0/0/3/0
 !

!


multicast-routing
 address-family ipv4
  interface all enable
 !
 core-tree-protocol rsvp-te group-list lsm
  static-rpf 192.168.10.1 32 mpls 5.5.5.5
 !
!
```

This configuration describes the Fast Reroute configuration in the MPLS network.

```
explicit-path name backup-path-to-tail1
 index 1 next-address strict 198.1.1.2
 index 2 next-address strick 198.1.2.2
!

interface tunnel-te1000 <<< backup p2p tunnel
 ipv4 unnumbered Loopback0
 destination 140.140.140.140
 path-option 1 explicit name backup-path-to-tail1
!
mpls traffic-eng
 interface POS0/2/0/0
 !
 interface POS0/2/0/1
  backup-path tunnel-te 1000
 !
```

```
 interface TenGigE0/5/0/4
!
```

Configure Point-to-Multipoint for the Source: Example

At the source, multicast routing must be enabled on both the tunnel-mte interface and customer-facing interface. Then, the static-group must be configured on the tunnel-mte interface to forward specified multicast traffic over P2MP LSP.



Note The multicast group address, which is in Source-Specific Multicast (SSM) address range (ff35::/16), must be used on the static-group configuration because Cisco IOS XR software supports only SSM for Label Switch Multicast (LSM). Additionally, the customer-facing interface must have an IPv6 address.

```
multicast-routing
  address-family ipv6
   interface tunnel-mte 1
    enable
   !
   interface GigabitEthernet0/2/0/3
    enable
   !
  !
 !
 router mld
  vrf default
   interface tunnel-mte 1
    static-group ff35::1 2000::1 3eFF::A
   !
  !
 !
 interface tunnel-mte 1
    ipv4 unnumbered Loopback0
    destination 192.168.0.1
       path-option 1 dynamic
    destination 209.165.201.1
       path-option 1 dynamic
 !
!
```

Related Topics

Point-to-Multipoint Traffic-Engineering Overview, on page 232
Point-to-Multipoint RSVP-TE, on page 234

Configure the Point-to-Multipoint Tunnel: Example

There is no difference between logging events at the tunnel level for both P2P and P2MP. The P2MP tunnel reoptimizes only at the per tunnel level.

```
interface tunnel-mte1
      ipv4 unnumbered Loopback0
      destination 60.60.60.60
      logging events lsp-status state
      logging events lsp-status reroute
      path-option 10 explicit name toR6_via_R2andR3
     !
     logging events lsp-status reoptimize
```

```
     logging events lsp-status state
     logging events lsp-status reroute
     fast-reroute
     record-route
    !
explicit-path name PATH7
     index 1 next-address strict ipv4 unicast 192.168.7.2
     index 2 next-address strict ipv4 unicast 192.168.7.1
     index 3 next-address strict ipv4 unicast 192.168.16.1
     index 4 next-address strict ipv4 unicast 192.168.16.2
     !
```

Related Topics

Path Option for Point-to-Multipoint RSVP-TE, on page 235
Point-to-Multipoint Traffic-Engineering Overview, on page 232

Disable a Destination: Example

From the tunnel-mte interface, you can disable the destination.

```
interface tunnel-mte101
 ipv4 unnumbered Loopback0
 destination 150.150.150.150
  disable
  path-option 10 dynamic
 !
 destination 150.150.150.150
  path-option 2 dynamic
 !
!
```

Related Topics

Point-to-Multipoint Traffic-Engineering Overview, on page 232

Configure the Point-to-Multipoint Solution: Example

Requirements for MPLS-TE Configuration

Before the Point-to-Multipoint (P2MP) tunnel is defined, these MPLS-TE requirements must be configured:

- Multiprotocol Label Switching traffic engineering (MPLS-TE)
- Resource ReSerVation Protocol (RSVP)
- Open Shortest Path First (OSPF)

This example shows the entire P2MP solution:

- Source is the location where the P2MP-TE tunnel interface is created.
- Tunnel contains multiple destinations. For example, the P2MP-TE tunnel is configured with two leaf node destinations by using the dynamic and explicit path options.
- Fast-Reroute (FRR) is specified on the P2MP tunnel.
- All regular TE tunnel options such as affinity or bandwidth are configured.
- Static mapping of the group address to the P2MP tunnel is done in IGMP.

  Internet Group Management Protocol (IGMP).

- The P2MP-TE midpoint configuration requires only TE and Interior Gateway Protocol (IGP) information.
- The P2MP-TE receiver configuration requires a static group and RPF map.

```
!
explicit-path name g2-r2-r1
 index 1 next-address strict ipv4 unicast 10.2.15.1
!
explicit-path name g2-r2-r3
 index 1 next-address strict ipv4 unicast 10.2.25.1
 index 2 next-address strict ipv4 unicast 10.2.23.2
!
explicit-path name g2-r2-r4
 index 1 next-address strict ipv4 unicast 10.2.25.1
 index 2 next-address strict ipv4 unicast 10.2.24.2
!
ipv4 access-list ssm
 10 permit ipv4 232.1.0.0/16 any
 20 permit ipv4 232.3.0.0/16 any
 30 permit ipv4 232.4.0.0/16 any
!
ipv4 access-list ssm-test
 10 permit ipv4 235.0.0.0/8 any
!
interface Loopback0
 ipv4 address 192.168.1.2 255.255.255.255
!
interface tunnel-mte221
 ipv4 unnumbered Loopback0
 destination 192.168.1.1
  path-option 1 dynamic
 !
 destination 192.168.1.3
  path-option 1 dynamic
 !
 destination 192.168.1.4
  path-option 1 dynamic
 !
!
interface tunnel-mte222
 ipv4 unnumbered Loopback0
 destination 192.168.1.1
  path-option 1 explicit name g2-r2-r1
 !
 destination 192.168.1.3
  path-option 1 explicit name g2-r2-r3
 !
 destination 192.168.1.4
  path-option 1 explicit name g2-r2-r4
 !
 signalled-bandwidth 1000
!
interface MgmtEth0/RP0/CPU0/0
 ipv4 address 172.20.163.12 255.255.255.128
!
interface MgmtEth0/RP1/CPU0/0
 shutdown
!
interface GigabitEthernet0/0/0/0
 ipv4 address 172.2.1.2 255.255.255.0
 load-interval 30
!
interface GigabitEthernet0/0/0/1
```

```
 ipv4 address 10.1.15.2 255.255.255.0
!
interface GigabitEthernet0/0/0/1.2
 ipv4 address 10.2.15.2 255.255.255.0
 encapsulation dot1q 2
!
interface GigabitEthernet0/0/0/2
 ipv4 address 10.1.25.2 255.255.255.0
!
interface GigabitEthernet0/0/0/2.2
 ipv4 address 10.2.25.2 255.255.255.0
 encapsulation dot1q 2
!
interface GigabitEthernet0/0/0/3
 shutdown
!
interface GigabitEthernet0/0/0/4
 shutdown
!
interface GigabitEthernet0/0/0/5
 shutdown
!
interface GigabitEthernet0/0/0/6
 shutdown
!
interface GigabitEthernet0/0/0/7
 shutdown
!
router static
 address-family ipv4 unicast
  0.0.0.0/0 1.56.0.1
  0.0.0.0/0 172.20.163.1
 !
!
router ospf 100
 nsr
 router-id 192.168.70.1
 area 0
  mpls traffic-eng
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/0
  !
  interface GigabitEthernet0/0/0/1
  !
  interface GigabitEthernet0/0/0/1.2
  !
  interface GigabitEthernet0/0/0/2
  !
  interface GigabitEthernet0/0/0/2.2
  !
 !
 mpls traffic-eng router-id 192.168.70.1
!
mpls oam
!
rsvp
 interface GigabitEthernet0/0/0/0
  bandwidth 20000
 !
 interface GigabitEthernet0/0/0/1
  bandwidth 20000
 !
 interface GigabitEthernet0/0/0/2
```

```
  bandwidth 20000
 !
 interface GigabitEthernet0/0/0/1.2
  bandwidth 20000
 !
 interface GigabitEthernet0/0/0/2.2
  bandwidth 20000
 !
!
mpls traffic-eng
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/1.2
 !
 interface GigabitEthernet0/0/0/2.2
 !
!
mpls ldp
 router-id 192.168.1.2
 nsr
 graceful-restart
 interface GigabitEthernet0/0/0/0
 !
 interface GigabitEthernet0/0/0/1
 !
 interface GigabitEthernet0/0/0/1.2
 !
 interface GigabitEthernet0/0/0/2
 !
 interface GigabitEthernet0/0/0/2.2
 !
!
multicast-routing
 address-family ipv4
  core-tree-protocol rsvp-te
  ssm range ssm
  static-rpf 172.1.1.1 32 mpls 192.168.1.1
  static-rpf 172.3.1.1 32 mpls 192.168.1.3
  static-rpf 172.4.1.1 32 mpls 192.168.1.4
  interface all enable
 !
!
router igmp
 !
 interface tunnel-mte221
  static-group 232.2.2.1 172.2.1.1
 !
 interface tunnel-mte222
  static-group 232.2.2.2 172.2.1.1
 !
 interface GigabitEthernet0/0/0/0
  static-group 232.1.2.1 172.1.1.1
  static-group 232.1.2.2 172.1.1.1
  static-group 232.3.2.1 172.3.1.1
  static-group 232.3.2.2 172.3.1.1
  static-group 232.4.2.1 172.4.1.1
  static-group 232.4.2.2 172.4.1.1
 !
!
end
```

Related Topics

Point-to-Multipoint Traffic-Engineering Overview, on page 232
Point-to-Multipoint RSVP-TE, on page 234
Path Option for Point-to-Multipoint RSVP-TE, on page 235

Configure MPLS TE Path-selection Cost Limit: Example

This example shows how to set the path-selection cost limit for MPLS TE tunnels at global, TE tunnel interface, and path-option attribute-set levels. By default, the cost-limit set at path-option attribute set takes the priority, if all options are configured and per tunnel interface level takes priority over global cost-limit. At per tunnel interface level, the global cost-limit takes the priority.

```
interface tunnel-te1
 path-selection cost-limit 2
!
mpls traffic-eng
 attribute-set path-option PO3AttrSet
  path-selection cost-limit 3
 !
 path-selection cost-limit 1
!
!
```

Regular expressions in MPLS-TE tunnel names

In large scale MPLS-TE tunnel deployments, regular expressions (regex) can provide a scalable way to filter tunnels for visibility, run actions on group of tunnels, and avoid issuing commands one tunnel at a time.

Table 18: Feature History Table

Feature Name	Release Information	Feature Description
Regular expressions in MPLS-TE tunnel names	Release 26.2.1	This feature enhances operational scalability and usability by allowing regex-based tunnel name filtering for MPLS-TE show and execution commands, without changing configuration models, architecture, or security posture. This feature supports regular expression in all MPLS-TE show and execution commands using tunnel names.

Starting from Cisco IOS XR Release 26.2.1, you can use regular expressions in execution and show commands with MPLS-TE tunnel names to filter multiple tunnels at a time.

Regular expressions enable operators to quickly filter show command output for MPLS-TE tunnel names, allowing them to

- view all tunnels for a specific region, customer, or service

- reduce noise in large outputs, and
- troubleshoot issues more quickly during outages or convergence events

By using regular expressions, operators can identify all related MPLS-TE tunnels at once, streamlining operational tasks across large-scale deployments.

Benefits of using regular expressions in MPLS-TE tunnel names

- Manage all related tunnels at once in large scale deployments.
- Apply actions to multiple tunnels in a single command, such as reoptimizing paths, rerouting tunnels, and clearing auto-bandwidth state.
- Leverage existing naming conventions without changing tunnel configuration.
- Allow fine-grained selection preventing incorrect matches in large MPLS-TE networks.

Limitations of using regex in MPLS-TE tunnels

The gNMI, Netconf, and programmability interfaces do not support regular expressions.

Usage guidelines of regex in MPLS-TE tunnel names

Follow these guidelines to use regex with MPLS-TE tunnel names:

- Tunnel names support the dot character ('.'). However, using `.` as a regex in tunnel names does not match any single character. To filter tunnel names in this way, use regex patterns such as `b[0-9a-zA-Z_-]r` or `b(.)r`.

  `.*` and `.+` are exceptions that are considered as regular expressions matching any character N times.

- When your regex includes '(', ')', or '|', enclose the pattern in double quotes. Without double quotes, it will be reported as an unsupported character.

```
Router# mpls traffic-eng reoptimize name "(FROM-nyc.*)"
Router# mpls traffic-eng reoptimize name "(FROM-nyc|To-LA)"
```

- Regex patterns containing backslash (\) do not work because the IOS XR parser removes all backslash characters from the string before processing.
  - Use `[0-9]` instead of `\d`
  - Use `[A-Za-z0-9_]` instead of `\w`
  - Using a dot (.) matches literal `'.'`, and there is no need to use `\.`

    Example using `\w`:

```
Router# show mpls traffic-eng tunnels name fo.\w brief
TUNNEL NAME         DESTINATION      STATUS  STATE
       fo.w         192.168.0.3          up     up
```

    Example using `.`(dot):

```
Router# show mpls traffic-eng tunnels name fo.o brief

TUNNEL NAME         DESTINATION      STATUS  STATE
```

```
       fo.o         192.168.0.3          up     up

Router# show mpls traffic-eng tunnels name fo[.f]o brief

TUNNEL NAME         DESTINATION      STATUS  STATE
       fo.o         192.168.0.3          up     up
       fofo         192.168.0.3          up     up
```

- For backward compatibility, all patterns are automatically wrapped as `^pattern$`.
- To match substrings, explicitly include wildcards such as `.*pattern.*`.

  Example:

```
/* Matches only the tunnel name "foo". */
Router# show mpls traffic-eng tunnels name foo

/* Matches all tunnels containing "foo" */
Router# show mpls traffic-eng tunnels name .*foo.*
```

- The question mark ('?') is interpreted by the CLI for command help or auto-completion. Hence, avoid using `?` in regex.

Table 19: Regex summary

Typical regex	Parser behavior	Usage
`'.'`	Literal only	Use `'.'` or character class such as `[a-zA-Z0-9_-.]`
`'(', ')', '|'`	Not allowed	Not allowed unless inside double quotes
`\`	Stripped	Use explicit character classes
`?`	CLI help character	Do not use
`^$`	Auto-applied	Explicit use has no impact
Substring match	Disabled by default	Use `.*pattern.*`

By following these guidelines, you ensure your regex patterns for MPLS-TE tunnel names are parsed and executed as intended in show and execution commands.

Regular expressions in MPLS-TE tunnel name filtering commands

You can filter and manage MPLS-TE tunnels efficiently by specifying name patterns with regular expressions in CLI commands. Regular expressions allow you to match tunnels based on their naming patterns for more effective tunnel management.

Supported show commands and execution commands

Execution commands	Show commands
mpls traffic-eng reoptimize name *<tunn-name with regex>*	**show mpls traffic-eng tunnels name** *<tunn-name with regex>* **[affinity | auto-bw | brief | detail | fsm | name-lookup | signame | source | standby | tabular]**
mpls traffic-eng tunnels resetup name *<tunn-name with regex>*	**show mpls traffic-eng event-history tunnels name** *<tunn-name with regex>*
mpls traffic-eng tunnels reroute name *<tunn-name with regex>*	**show mpls traffic-eng autoroute name** *<tunn-name with regex>* **[ip | standby]**
mpls traffic-eng tunnels reroute name *<tunn-name with regex>*	**show mpls traffic-eng autoroute -destination name** *<tunn-name with regex>* **[ip | standby]**
clear mpls traffic-eng auto-bw name *<tunn-name with regex>*	**show mpls traffic-eng tunnels protection [frr] name** *<tunn-name with regex>* **[name-lookup | standby]**
	show mpls traffic-eng tunnels name *<tunn-name with regex>* **role [all | head | middle | tail]**

Some examples include:

- Execution commands:

```
Router# mpls traffic-eng reoptimize name FROM-nyc.*
Router# mpls traffic-eng tunnels reroute name .*TO-LA
```

- Show commands:

```
Router# show mpls traffic-eng tunnels name FROM-nyc.*
Router# show mpls traffic-eng tunnels name .*TO-LA
Router# show mpls traffic-eng tunnels name .*CUSTOMER-A.*
```

These examples demonstrate how to use regular expressions, such as '.*', to match tunnels that begin with , end with, or contain specific name patterns.

Configuring Performance Measurement

Network performance metrics such as packet loss, delay, delay variation, and bandwidth utilization is a critical measure for traffic engineering (TE) in service provider networks. These network performance metrics provide network operators information about the performance characteristics of their networks for performance evaluation and helps to ensure compliance with service level agreements. The service-level agreements (SLAs) of service providers depend on the ability to measure and monitor these network performance metrics. Network operators can use performance measurement (PM) feature to monitor the network metrics for links as well as end-to-end TE label switched paths (LSPs).

Path Calculation Metric Type

To configure the metric type to be used for path calculation for a given tunnel, use the **path-selection metric** command in either the MPLS-TE configuration mode or under the tunnel interface configuration mode.

The metric type specified per interface takes the highest priority, followed by the MPLS-TE global metric type.



Note If the delay metric is configured, CSPF finds a path with optimized*minimum* link delay metric. See the *Configuring Performance Measurement* chapter in the Segment Routing Configuration Guide for information on configuring interface performance delay measurement.

Configuration Example

The following example shows how to set the path-selection metric to use the IGP metric under a specific tunnel interface:

```
Router# configure
Router(config)# interface tunnel-te 1
Router(config-if)# path-selection metric igp
Router(config-if)# commit
```

The following example shows how to set the path-selection metric to use the delay metric under the MPLS-TE configuration mode:

```
Router# configure
Router(config)# mpls traffic-eng
Router(config-mpls-te)# path-selection metric delay
Router(config-mpls-te)# commit
```

Path-Selection Delay Limit

Apply the **path-selection delay-limit** configuration to set the upper limit on the path aggregate delay when computing paths for MPLS-TE LSPs. After you configure the **path-selection delay-limit** value, if the sum of minimum-delay metric from all links that are traversed by the path exceeds the specified delay-limit, CSPF will not return any path. The periodic path verification checks if the delay-limit is crossed.

The **path-selection delay-limit** value can be configured at the global MPLS-TE, per-interface tunnel, and per path-option attribute set. The path-selection delay-limit per path-option attribute set takes the highest priority, followed by per-interface, and then the MPLS-TE global path-selection delay-limit values.

The delay limit range is a value from 1 to 4294967295 microseconds.



Note See the *Configuring Performance Measurement* chapter in the Segment Routing Configuration Guide for information on configuring interface performance delay measurement.

Configuration Example

The following example shows how to set the path-selection delay limit under a specific tunnel interface:

```
Router# configure
Router(config)# interface tunnel-te2000
Router(config-if)# path-selection metric delay
Router(config-if)# path-selection delay-limit 200
Router(config-if)# commit
```

The following example shows how to set the path-selection delay limit under a path-option attribute set:

```
Router# configure
Router(config)# mpls traffic-eng
Router(config-mpls-te)# attribute-set path-option test
Router(config-te-attribute-set)# path-selection delay-limit 300
Router(config-te-attribute-set)# root
Router(config)# interface tunnel-te1000
Router(config-if)# path-option 10 dynamic attribute-set test
Router(config-if)# commit
```

The following example shows how to set the path-selection delay limit under the global MPLS-TE configuration mode:

```
Router# configure
Router(config)# mpls traffic-eng
Router(config-mpls-te)# path-selection metric delay
Router(config-mpls-te)# path-selection delay-limit 150
Router(config-mpls-te)# commit
```

Additional References

For additional information related to implementing MPLS-TE, refer to the following references:

Related Documents

Related Topic	Document Title
MPLS-TE commands	*MPLS Traffic Engineering Commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

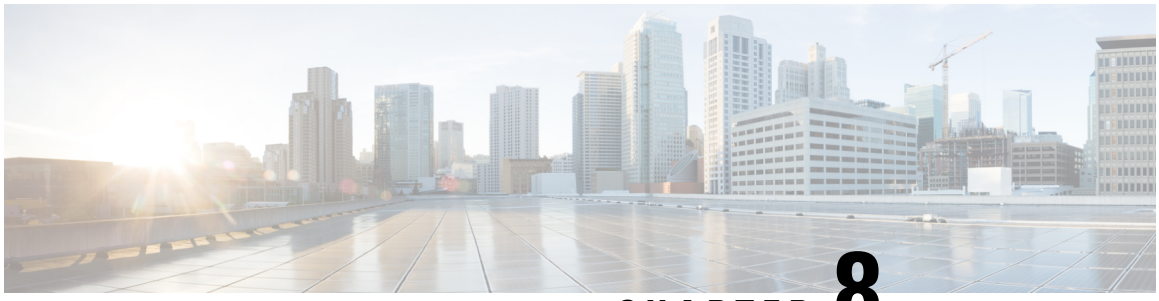
MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
RFC 4124	*Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*, F. Le Faucheur, Ed. June 2005. (Format: TXT=79265 bytes) (Status: PROPOSED STANDARD)
RFC 4125	*Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*, F. Le Faucheur, W. Lai. June 2005. (Format: TXT=22585 bytes) (Status: EXPERIMENTAL)
RFC 4127	*Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*, F. Le Faucheur, Ed. June 2005. (Format: TXT=23694 bytes) (Status: EXPERIMENTAL)

Technical Assistance

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



CHAPTER 8

GMPLS UNI

The Generalized Multiprotocol Label Switching (GMPLS) User Network Interface (UNI) creates a circuit connection between two clients (UNI-C) of an optical network. This connection is achieved by signaling exchanges between UNI Client (UNI-C) and UNI Network (UNI-N) nodes. The UNI-C nodes are router nodes and UNI-N nodes are optical nodes.

- Prerequisites for Implementing GMPLS UNI, on page 425
- Restrictions for Implementing GMPLS UNI, on page 425
- Information About Implementing GMPLS UNI , on page 426
- nLight Enhancements, on page 429
- How to Implement GMPLS UNI, on page 433
- Configuration Examples for GMPLS UNI, on page 465
- Additional References, on page 467

Prerequisites for Implementing GMPLS UNI

The following prerequisites are required to implement GMPLS UNI:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- Router that runs Cisco IOS XR software.
- Installation of the Cisco IOS XR software mini-image on the router.
- Installation of the Cisco IOS XR MPLS software package on the router.

Restrictions for Implementing GMPLS UNI

- The total number of configured GMPLS UNI controllers should not exceed the platform scale limit of 500 GMPLS interfaces.
- Each UNI-N (ingress or egress) should be routable from its adjacent UNI-C. The UNI-C nodes need to be routable from the UNI-N nodes too.
- GMPLS UNI is supported only over DWDM controllers and so, over POS and GigabitEthernet interfaces.

- GMPLS UNI is supported only with these Cisco ASR 9000 Enhanced Ethernet Line Cards:
  - A9K-MOD80-SE : 80G Modular Line Card, Service Edge Optimized
  - A9K-MOD80-TR : 80G Modular Line Card, Packet Transport Optimized
  - A9K-36X10GE-SE - Cisco ASR 9000 36-Port 10GE Service Edge Optimized Line Card
  - A9K-36X10GE-TR - Cisco ASR 9000 36-Port 10GE Packet Transport Optimized Line Card
  - A9K-24X10GE-SE - Cisco ASR 9000 24-Port 10GE Service Edge Optimized Line Card
  - A9K-24X10GE-TR - Cisco ASR 9000 24-Port 10GE Packet Transport Optimized Line Card

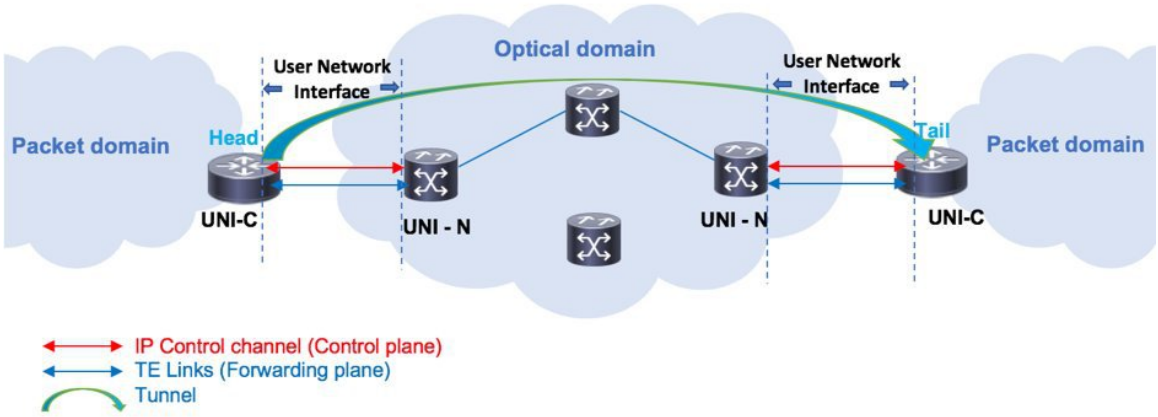
Information About Implementing GMPLS UNI

To implement GMPLS UNI, you should understand these concepts:

GMPLS UNI vs GMPLS NNI

In case of GMPLS NNI, the optical network topology is known and path calculations are performed at the NNI head. In case of GMPLS UNI, the optical network topology is unknown to the UNI-C nodes and path calculations are performed by the UNI-N nodes.

GMPLS UNI Use Case



The UNI components are UNI-N and UNI-C. The tunnel originates on the headend UNI, depicted in the left part of the image. The tunnel terminates on the tailend UNI, depicted in the right part of the image. Enable the following configurations on the headend UNI and tailend UNI:

- Control plane - IP control channel between the UNI-C and UNI-N router IDs. This creates LMP adjacency over the control channel.
- Forwarding plane - TE Link between UNI-C and UNI-N optical interfaces.
- Tunnel configuration from Head UNI-C to a Tail UNI-C optical interface, over the optical network.

For each tunnel, you must enable corresponding tunnel and TE link configurations.

Link Management Protocol (LMP) – LMP manages the control channel across the UNIs, verifies TE link connectivity between the UNI interfaces, and performs fault management.

Dynamic LMP – In release 7.0(1), you can enable the Dynamic LMP function which validates LMP configuration consistency across the headend and tailend UNIs. Consistency check examples:

- You have configured one end of a TE link as an unnumbered interface, and the other end with an IP address.
- You have entered the wrong neighbor interface ID when configuring an unnumbered neighbor interface.

Ensure that you enable the preceding configurations correctly.

GMPLS LSP Signaling

The GMPLS overlay model architecture is used for LSP signaling for GMPLS connections. In GMPLS UNI, UNI-C nodes send a request for a connection to UNI-N node. The connection request does not contain an end-to-end path. This is because, as mentioned previously, UNI-C nodes do not have knowledge of the topology of the optical network and therefore cannot determine the end-to-end path. The UNI-C node signals a connection request without an ERO.

The LSP diversity is signaled on a GMPLS UNI tunnel with a path-option. A path-option is permitted on a GMPLS UNI tunnel with a "no ERO" and an optional "XRO" attribute sets to specify LSP diversity requirements. If multiple LSP exclusions are configured in the attribute-set, they can be added to the path message along with an appropriate LSP connection diversity sub-object.

Release 7.0(1) supports the following LSP encoding and corresponding switching types.

Switching Type	LSP Encoding Type
LSC	Lambda
FSC	EthernetType1, EthernetType2, Fiber
DCSC	EthernetType2

A packet network is switched across a fiber, optic, or data channel network. Enable the LSP encoding and switching types under the GMPLS UNI and LMP configuration modes. Also, enable the Generalized PID (G-PID) under the GMPLS UNI configuration mode. G-PID is an identifier of the type of payload that the LSP carries, and the LSP endpoints (the UNI-C devices) use.

The LSP encoding, switching type, and G-PID are updated to the GMPLS label.

Path Message without an ERO

In GMPLS UNI, UNI-C nodes send a request for a connection to UNI-N node. The connection request does not contain an end-to-end path, because, UNI-C nodes do not have knowledge of the topology of the optical network and therefore cannot determine the end-to-end path. The UNI-C node signals a connection request without an ERO.

When no ERO is present in a received path message, the UNI-N node calculates a route to the destination and includes that route in an ERO, before forwarding the path message. If no route is found, the UNI-N returns a path error message with an error code and subcode of *24,5 - "No route available toward destination"*.

The destination address of a GMPLS LSP can be either the optical router-id of the tail UNI-C node, or the optical address of the ingress interface to the tail UNI-C node. Supplying the router-id allows the UNI-N to route the tunnel to the tail UNI-C node via any attached UNI-N node; supplying the UNI-C's ingress interface address forces the tunnel's path to traverse the UNI-N node attached to that interface.



Note The optical router-ids and interface addresses may or may not be the same as the packet ones.

XRO Attribute-set

An optional XRO attribute-set can be specified as part of the path-option to specify LSP diversity requirements. An empty XRO attribute set results in the GMPLS tunnel being signaled with no exclusions, and therefore no XRO.



Note A non-existent XRO attribute-set can be configured in the GMPLS UNI tunnel path-option; in this case no attempt will be made to bring up the GMPLS tunnel until the configuration is complete.

Connection Diversity

Connection diversity is required to ensure that GMPLS tunnels can be established without sharing resources, thus, greatly reducing the probability of simultaneous connection failures. For example, an edge-node wishes to establish multiple LSPs towards the same destination edge-node, and these LSPs need to have few or no resources in common.

Connection diversity supports the establishment of a GMPLS LSP which is diverse from the path taken by an existing LSP. An XRO is added to the tunnel's path message with appropriate LSP diversity sub-objects or exclusions. A maximum of 20 connection diversity exclusions per XRO is supported.

GMPLS RSVP VRF Signaling

The Cisco IOS XR software supports a single non-default VRF for the GMPLS RSVP signaling. This allows GMPLS signaling to work even when the only available communication between the UNI-C and UNI-N nodes is through a VRF. This non-default VRF is supported only for GMPLS signaling; whereas the MPLS-TE signaling continues to support only the default VRF.

DWDM Transponder Integration

A GMPLS UNI based solution preserves all the advantages of the integration of the DWDM transponder into the router blade. These advantages include:

- improved CAPEX and OPEX models
- component, space and power savings
- improved IP availability through pro-active protection.

nLight Enhancements

These topics describe the enhancements made to nLight (also known as GMPLS UNI):

Explicit Route Object

Explicit Route Objects (EROs) limit LSP routing to a specified list of LSRs. Formerly, the UNI Client (UNI-C) node signaled a connection request, without an ERO, to the UNI Network (UNI-N) node. In this IOS XR Software release, the UNI-C node provides support for path message with ERO for GMPLS tunnels. This includes the capability to specify either a strict or a loose ERO to a path option to be included in the path message for processing by the ingress UNI-N.

An ERO in constructed using the strict and loose hops, specified in the explicit path, by the path option.

When a loose hop is configured, it identifies one or more transit LSRs which suggests the preferred path for the LSP. If a suggested path fails, another LSR is tried.

When a strict hop is configured, it identifies an exact path through which the LSP must be routed. Strict hop EROs specify the exact sequence of LSRs in the LSP.

As a result of these operations, a LSP is established from the sender to the destination of the session, following the explicitly routed path specified in the ERO.



Note

- *lockdown* and *verbatim* are mandatory in ERO path option.
- A path option may still be configured to use no ERO.
- In no ERO, *lockdown* is mandatory.

Wavelength Specification

The wavelength (also called label) specification enhancement enables the network planning tool to determine the wavelength, and specify the same at the UNI-C. The UNI-N then accepts the label provided by the UNI-C, or rejects the path entirely. Previously, the wavelength to be used for the GMPLS UNI tunnel was determined by the UNI-N, taking into account the headend UNI-C's capabilities.

The wavelength to be used is added to the path option configuration. This optional configuration allows a fixed wavelength to be specified for the path option.

When signaling using a path option with the specified wavelength takes place, the following changes happen because of the wavelength specification enhancement:

- The configured wavelength is validated against the controller’s capabilities; signaling fails if the wavelength cannot be used by the controller.
- The upstream label is set to the specified wavelength.
- The label-set in the Path message, instead of containing one label for each supported wavelength, contains only the specified wavelength.

- A path-error message with error code 25 and subcode 6 no longer receives special handling. If a suggested label is supplied, it is ignored.

Note A suggested label received in response to signaling with a path option that specifies a different label, is not stored for future use. Other path options, in general, have different constraints and therefore require path calculation to be redone.

Multiple Path Options

Multiple path options are permitted per GMPLS UNI tunnel. The index given to each path option indicates its relative preference level, with lower indices being preferred. This is similar to the existing multiple path option functionality available for packet TE. This allows the provision of multiple path options with, for example, progressively free constraints.

The path-option index is no longer fixed to ten and is now set by the user and distinguishes path options in the same manner as for packet tunnels. In all situations where a tunnel is being brought up or reoptimized, the path-option with the lowest index is tried first; if no LSP can be established with this path option, then subsequent path options are tried in ascending order. This also applies to recovery from failures, unless any recovery path option is specified.

Reoptimization

Reoptimization differs from restoration though the mechanisms involved are similar. Reoptimization occurs without the original connection having failed.

Unlike packet tunnels, reoptimization in GMPLS tunnels is not supposed to be loss free.

Manual Reoptimization

Manual reoptimazation of a single GMPLS UNI tunnel can be triggered from the UNI-C node (headend). Use the **mpls traffic-eng optical-uni reoptimize tunnel-id** command to trigger manual reoptimization of a GMPLS UNI tunnel.

The manual trigger for reoptimization causes the currently established LSP to be torn down and signals a new LSP using the normal bring-up process (though the new LSP is same as the current one).

It is not possible to trigger reoptimization for multiple GMPLS UNI tunnels or at the tailend of a tunnel.

SRLG Discovery

Note SRLG (Shared Risk Link Group) discovery, SRLG collection and SRLG recording represent the same function.

The head and tail UNI-C routers have no direct knowledge of the path taken through the optical network by a GMPLS UNI tunnel, or of the properties of that path. All information about the path of a particular GMPLS UNI connection must therefore be explicitly requested and learned during the signaling process.

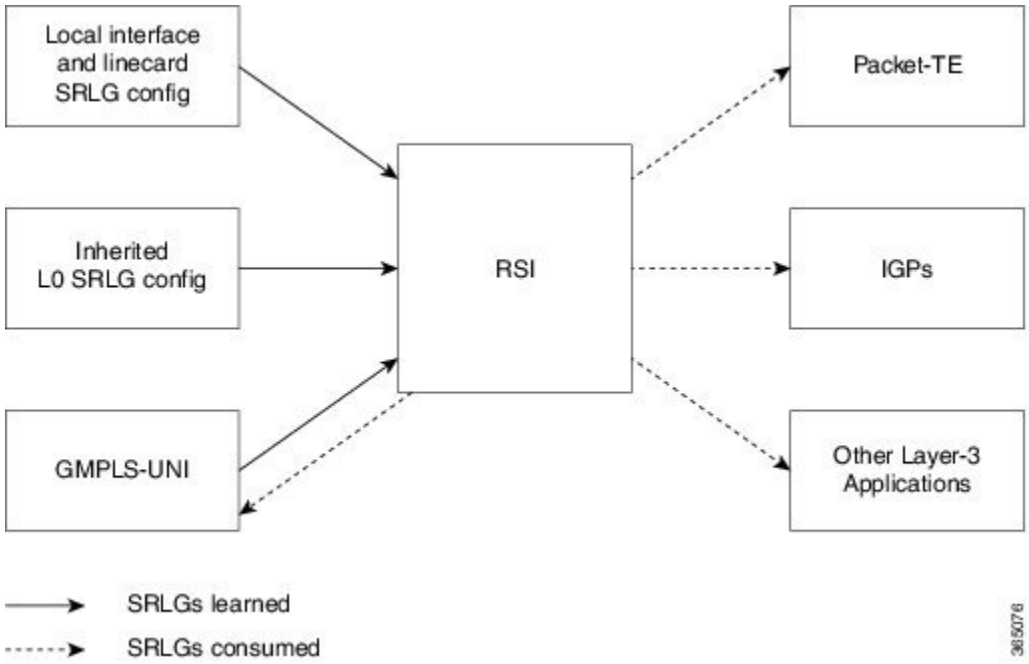
A key property of a GMPLS UNI connection is the set of SRLGs used by the optical links along the connection. It is necessary for the UNI-C routers to learn the set of SRLGs associated with a connection, so that this information can be used, both by GMPLS UNI in the specification of diversity requirements for other connections and by Layer-3 applications for effecting routing and protection decision making.

The learning of SRLGs during GMPLS UNI LSP signaling is done by requesting SRLG collection when LSP signaling is initiated, and by the addition of SRLG RRO sub-objects to the Path and Resv messages during signaling as described in IETF draft *SRLG-collect*. Path message learns egress interfaces from head to tail and Resv message learns egress interfaces from tail to head

Provision of Discovered SRLGs to RSI

Once the SRLGs used by a GMPLS UNI connection are collected during signaling as in SRLG discovery, they are made available to the Layer-3 processes. This is done through RSI (Router Space Infrastructure), as illustrated in the following diagram:

Figure 34: SRLG Communication



An API is provided by the RSI component to allow SRLGs discovered during GMPLS UNI signaling to be communicated to RSI, as documented in IETF draft *RSI-SRLG*. RSI combines the SRLG sets learned from GMPLS and configuration for an interface and deliver a single set of SRLGs to applications registered as SRLG clients.

The SRLGs discovered during GMPLS UNI signaling are given to RSI for application to the Layer-3 interface of the DWDM controller associated with the GMPLS UNI tunnel. This may be a POS, GigE or an OTN interface.

SRLG Announce

All SRLGs discovered through GMPLS signaling are announced to RSI once the tunnel is up. These SRLGs are withdrawn from RSI when the tunnel goes down.

SRLG Diversity



Note SRLG diversity and SRLG exclusion represent the same function.

Support is added for signaling SRLG based diversity requirements, based on the XRO SRLG sub-object defined in RFC 4874. The use of SRLGs removes the restrictions of LSP based diversity, as SRLGs are flooded throughout the optical network, and by their very nature, reduce the risk of concurrent failure.

SRLG diversity is configured under the XRO attribute-set.

Head UNI-C Behavior

SRLG diversity is configured at the tunnel head. Individual SRLG exclusions are added to an XRO attribute-set; each is specified as either *best-effort* or mandatory (*strict*). Whenever any exclusion is specified, an XRO object is added to the Path message by the head UNI-C. The XRO contains a SRLG sub-object for each specified SRLG. The SRLG exclusions may coexist in the same XRO with LSP exclusions.

The XRO attribute-set is associated with tunnel path options in the same manner as for LSP exclusions.

If a SRLG with a strict exclusion matches an SRLG configured on the local DWDM controller, the bring-up attempt fails.

The SRLG exclusions requested by the head UNI-C are processed by the ingress UNI-N node during path calculation for the tunnel.

Tail UNI-C Behavior

On receiving a Path message containing an XRO, the tail UNI-C inspects each SRLG sub-object. If a SRLG sub-object, with a strict exclusion, matches an SRLG configured on the local DWDM controller, the Path message is rejected and a path-error is generated with error codes. No action is taken if the SRLG sub-object specifies a *best-effort* exclusion.

Multi-Layer Restoration - Optical

Multi-Layer Restoration-Optical (MLR-O) involves restoration from failures in the optical network that can leverage the same router interfaces at both ends.

Optical restoration involves the repair of a failure by the optical network locally. Although the routers may see loss of light until the failure is repaired, there is no signaling involving the routers, and from the routers perspective the GMPLS UNI LSP remains unchanged.

Optical Restoration: Same Wavelength

When a failure occurs on a physical link within the optical network, the routers identify that the link is down and Layer 3 protection mechanisms, such as FRR, are used to minimize the traffic loss. The optical network re-routes the GMPLS connection to an alternative path. This is done without any involvement of the routers.

Limitation

A significant limitation of optical restoration in this case, is that the wavelength in use for the connection cannot be changed. This is because the wavelength must be the same along the entire path and cannot be

changed without end-to-end signaling. The constraints imposed on the connection during its initial signaling are also unchanged, which may reduce the chance of finding an alternative path.

Optical Restoration: Wavelength Change

Optical restoration may occur with an associated wavelength change, in the case where the optical network finds an alternative path with the same constraints as were originally signaled, but using a different wavelength. Some signaling is required, since the wavelength (and therefore the labels) used by the GMPLS connection are to change.

Consider a failure within the optical network on the path of a GMPLS UNI LSP. The restoration proceeds as in the previous case (same wavelength), but the new path found, uses a different wavelength. The ingress UNI-N then sends a path-error message indicating the new wavelength to be used; this has error code 24 (routing), sub-error 6 (unacceptable label set) and contains a suggested-label sub-object with the new label to be used. The head UNI-C then signals a new LSP with the new wavelength.

Although the wavelength in use may change in this case, the constraints used in signaling the original LSP remain unchanged.

How to Implement GMPLS UNI

A new submode is introduced under the main TE submode to enable GMPLS UNI and to contain GMPLS UNI configuration.

To implement GMPLS UNI, follow these procedures:

Configuring TE for GMPLS UNI

TE configuration specific to packet tunnels does not affect GMPLS UNI tunnels.

To implement TE configuration for GMPLS UNI, follow these procedures:

Enabling GMPLS UNI Submode

Perform this task to enable GMPLS UNI configuration submode and to configure GMPLS UNI tunnels.



Note Removal of the GMPLS UNI submode results in the removal of all configuration within it, including any other parser submode, and the immediate destruction of all GMPLS UNI tunnels.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.

Step 3	**gmpls optical-uni**
	Example:
	`RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`
	`RP/0/RSP0/CPU0:router(config-te-gmpls)#`
		Enters GMPLS UNI configuration submode.

Step 4	**commit**	

Configuring GMPLS UNI Controller

Perform this task to setup a GMPLS tail in MPLS-TE configuration. This task enables GMPLS UNI controller submode to configure controllers for establishing GMPLS UNI tunnels. This is the minimal configuration required at the tunnel tail.

Note Removal of the GMPLS UNI controller submode results in the immediate destruction of any GMPLS tunnel established over the controller referenced.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.

Step 4	**controller dwdm** *interface*
	Example:
	`RP/0/RSP0/CPU0:router(config-te-gmpls)# controller dwdm 0/1/0/1`
	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)#`
		Enters GMPLS UNI controller submode.

Step 5	**commit**	

Configuring the GMPLS UNI Controller as a Tunnel Head

Perform this task to configure the tunnel properties for a GMPLS UNI controller.

This configuration designates the controller as a tunnel-head, rather than a tunnel tail. After you configure the tunnel properties, the incoming path messages are rejected and any existing tailend tunnel is torn down.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **mtu** *value*
6. **tunnel-properties**
7. **g-pid** *ID*
8. **encoding-type** *type*
9. **tunnel-id** *number*
10. **destination ipv4 unicast** *address*
11. **path-option 10 no-ero lockdown**
12. **exit**
13. **switching-type** *type*
14. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.

Step 4	**controller dwdm** *interface*
	Example:
	`RP/0/RSP0/CPU0:router(config-te-gmpls)# controller dwdm 0/1/0/1`
	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)#`
		Enters GMPLS UNI controller submode.

Step 5	**mtu** *value* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# mtu 9000`	Enable the maximum traffic limit on the interface.

Step 6	**tunnel-properties**
	Example:
	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)#`
		Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.

Step 7	**g-pid** *ID* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# g-pid 37`	Assigns the Generalized PID (G-PID) which is an identifier of the payload that is carried by the LSP. The LSP endpoints (the UNI-C devices) use the G-PID.
Step 8	**encoding-type** *type* **Example:**	Assigns the LSP encoding type.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# encoding-type lambda`	
Step 9	**tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# tunnel-id 100`	Specifies a tunnel-id for a headend router of a GMPLS tunnel. The tunnel-id is a 16-bit number ranging 0–65535.
Step 10	**destination ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# destination ipv4 unicast 10.10.3.4`	Specifies a tunnel destination for a headend router of a GMPLS tunnel. The destination argument is an IPv4 address.
Step 11	**path-option 10 no-ero lockdown** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 10 no-ero lockdown`	Specifies the path-option for a headend router of a GMPLS tunnel. **Note** You can specify an XRO attribute-set as part of the path-option.
Step 12	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# exit`	Exits the mode and enters the controller mode.
Step 13	**switching-type** *type* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# switching-type lsc`	Assigns the switching type of the LSP traffic.
Step 14	**commit**	

Configuring Other Tunnel Properties for a GMPLS UNI Tunnel

Perform this task to configure the optional tunnel properties for a GMPLS UNI tunnel. This configuration is optional, and if omitted, the GMPLS tunnel is established with the default property values.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **tunnel-properties**
6. **priority** *setup-priority hold-priority*
7. **record-route**

8. **signalled-name** *name*
9. **logging events lsp-status state**
10. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls)# controller dwdm 0/1/0/1`	Enters GMPLS UNI controller submode.
Step 5	**tunnel-properties** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`	Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.
Step 6	**priority** *setup-priority hold-priority* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# priority 3 2`	Specifies the priority for a GMPLS tunnel. The default priority value is 7 for both setup and hold priorities. **Note** The setup-priority and hold-priority values are numbers ranging from 0 to 7, where 0 represents the highest priority. The hold-priority must be equal or higher (numerically less) than the setup-priority.
Step 7	**record-route** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# record-route`	Enables record-route functionality for a GMPLS tunnel.

	Command or Action	Purpose
Step 8	**signalled-name** *name* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# signalled-name sign1`	Configures signalled-name for a GMPLS tunnel. **Note** If no signalled name is configured, TE will generate a default name in the form of *router-name_tunnel-id_destination-address*, for example, te-ma1_123_10.10.10.10.
Step 9	**logging events lsp-status state** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# logging events lsp-status state`	Configure events to generate system log messages when state changes occur on the GMPLS tunnel. If omitted, no events will result in the generation of system log messages.
Step 10	**commit**	

Configuring LSP Diversity

To configure an XRO attribute-set as part of the path-option for MPLS-TE, and to specify exclusions for an attribute set for LSP diversity, follow these procedures:

Configuring XRO Attribute-set

Perform this task to configure XRO attribute set in the GMPLS UNI tunnel path-option, under MPLS-TE submode.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **tunnel-properties**
6. **path-option 10 no-ero [xro-attribute-set** *name* **] lockdown**
7. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.

	Command or Action	Purpose
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls)# controller dwdm 0/1/0/1`	Enters GMPLS UNI controller submode.
Step 5	**tunnel-properties** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`	Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.
Step 6	**path-option 10 no-ero [xro-attribute-set** *name* **] lockdown** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 10 no-ero xro-attribute-set A01 lockdown`	Specifies the path-option for a headend router of a GMPLS tunnel.
Step 7	**commit**	

Configuring Connection Diversity

Perform this task to specify exclusions for an attribute set for LSP diversity, under MPLS-TE attribute-set configuration mode.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **attribute-set xro** *name*
4. **exclude** {**best-effort** | **strict**} **lsp source** *source-address* **destination** *destination-address* **tunnel-id** *tunnel-id* **extended-tunnel-id** *extended-tunnel-id* [**lsp-id** *lsp-id*]
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**attribute-set xro** *name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# attribute-set xro attrset01`	Configures an XRO attribute-set for a GMPLS tunnel.

Step 4	**exclude** {**best-effort** | **strict**} **lsp source** *source-address* **destination** *destination-address* **tunnel-id** *tunnel-id* **extended-tunnel-id** *extended-tunnel-id* [**lsp-id** *lsp-id*]
	Example:
	`RP/0/RSP0/CPU0:router(config-te-attribute-set)# exclude best-effort lsp source 10.10.1.2 destination 10.20.4.4 tunnel-id 17 extended-tunnel-id 10.20.3.3 lsp-id 17`
	`RP/0/RSP0/CPU0:router(config-te-attribute-set)#`
		Specifies exclusions for an attribute set for LSP diversity.
		Note
		A maximum of 20 LSP exclusions per XRO is supported.

Step 5	**commit**	

Configuring LMP for GMPLS UNI

To implement LMP configuration for GMPLS UNI, follow these procedures:

Configuring Optical Router ID

Perform this task to enable GMPLS UNI LMP functionality and to configure LMP unicast router ID.

SUMMARY STEPS

1. **configure**
2. **lmp**
3. **gmpls optical-uni**
4. **router-id ipv4 unicast** *address*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	

	Command or Action	Purpose
Step 2	**lmp** **Example:** `RP/0/RSP0/CPU0:router(config)# lmp`	Enters LMP configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-lmp)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**router-id ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni)# router-id ipv4 unicast 10.10.4.4`	Configures the LMP unicast router ID for GMPLS.
Step 5	**commit**	

Configuring an LMP Neighbor

Perform this task to configure an LMP neighbor for a GMPLS UNI tunnel.

SUMMARY STEPS

1. **configure**
2. **lmp**
3. **gmpls optical-uni**
4. **neighbor** *name*
5. **dynamic**
6. **hello** *interval dead-interval*
7. **ipcc routed**
8. **router-id ipv4 unicast** *address*
9. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**lmp** **Example:**	Enters LMP configuration mode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config)# lmp`	
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-lmp)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**neighbor** *name* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni)# neighbor nbr1`	Specifies an LMP neighbor for GMPLS and enters the LMP GMPLS UNI neighbor configuration submode.
Step 5	**dynamic** **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-nbr1)# dynamic`	Configures Dynamic LMP function.
Step 6	**hello** *interval dead-interval* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-nbr1)# hello 1000 10000`	Specifies the LMP hello message frequency (in milliseconds) sent between LMP enabled routers. It also specifies the time duration (in milliseconds) after which the device sends an LMP hello expiry message. The LMP hello expiry message duration must be three times more than the LMP hello interval duration. If you do not use the LMP fast keep-alive mechanism, ensure that you set the two interval values to zero.
Step 7	**ipcc routed** **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-nbr-nbr1)# ipcc routed`	Specifies the LMP neighbor IPCC configuration for GMPLS UNI.
Step 8	**router-id ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-nbr-nbr1)# router-id ipv4 unicast 10.10.4.5`	Configures the LMP unicast router ID for GMPLS.
Step 9	**commit**	

Configuring an LMP Controller

Perform this task to configure an LMP link for a GMPLS UNI controller.

SUMMARY STEPS

1. **configure**
2. **lmp**
3. **gmpls optical-uni**
4. **controller dwdm** *controller*
5. **neighbor** *name*
6. **link-id ipv4 unicast** *address*
7. **switching-type** *type*
8. **encoding-type** *type*
9. **neighbor link-id ipv4 unicast** *address*
10. **neighbor interface-id unnumbered** *interface-id*
11. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**lmp** **Example:** `RP/0/RSP0/CPU0:router(config)# lmp`	Enters LMP configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-lmp)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *controller* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni)# controller dwdm 0/4/0/0`	Specifies a controller for GMPLS UNI.
Step 5	**neighbor** *name* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-cntl)#`	Specifies an LMP neighbor for GMPLS and enters the LMP GMPLS UNI neighbor configuration submode.

	Command or Action	Purpose
	`neighbor nbr1`	
Step 6	**link-id ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-cntl)# link-id ipv4 unicast 10.2.2.4`	Specifies the optical interface address for an LMP link for a GMPLS UNI controller.
Step 7	**switching-type** *type* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-cntl)# switching-type lsc`	Specifies type of switching traffic that the LSP carries.
Step 8	**encoding-type** *type* **Example:** `(RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-cntl)# encoding-type Lambda`	Specifies the signaling technology that you use for transporting traffic.
Step 9	**neighbor link-id ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-cntl)# neighbor link-id ipv4 unicast 10.2.2.5`	Specifies the neighbor's optical address of an LMP link for a GMPLS UNI controller.
Step 10	**neighbor interface-id unnumbered** *interface-id* **Example:** `RP/0/RSP0/CPU0:router(config-lmp-gmpls-uni-cntl)# neighbor interface-id unnumbered 17`	Specifies the neighbor's optical interface ID of an LMP link for a GMPLS UNI controller.
Step 11	**commit**	

Configuring RSVP Optical Refresh Interval and Missed Count

Perform this task to configure optical refresh interval under the RSVP controller submode and to configure the number of missed refresh messages allowed before optical tunnel states are deleted.

SUMMARY STEPS

1. **configure**
2. **rsvp**
3. **controller dwdm** *interface*
4. **signalling refresh out-of-band interval** *interval*

5. **signalling refresh out-of-band missed** *miss-count*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**rsvp** **Example:** `RP/0/RSP0/CPU0:router(config)# rsvp`	Enters RSVP configuration mode.
Step 3	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp)# controller dwdm 0/1/0/1`	Configures a controller for establishing a GMPLS UNI tunnel.
Step 4	**signalling refresh out-of-band interval** *interval* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-cntl)# signalling refresh out-of-band interval 200`	Configures optical refresh interval. The interval argument is the interval (in seconds) at which refresh messages are sent and expected to be received. The range is 180 to 86400 (a refresh-interval of 1 day).
Step 5	**signalling refresh out-of-band missed** *miss-count* **Example:** `RP/0/RSP0/CPU0:router(config-rsvp-cntl)# signalling refresh out-of-band missed 30`	Configures number of missed refresh messages allowed before optical tunnel states are deleted. The miss-count argument is the number of refresh messages, expected at the configured refresh-interval, which can be missed before optical tunnel states time out. The accepted range is 1 to 48. The default value is 12.
Step 6	**commit**	

nLight Enhancements: Configurations and Verifications

These topics describe the configurations and verifications for the nLight enhancements made:

Configuring an ERO for a GMPLS Tunnel

Perform this task to configure an ERO for a GMPLS tunnel.

SUMMARY STEPS

1. **configure**

2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **tunnel-properties**
6. **tunnel-id** *number*
7. **logging events lsp-status state**
8. **destination ipv4 unicast** *address*
9. **path-option** *number* **explicit name** *name* **lockdown verbatim**
10. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-uni)# controller dwdm 0/2/1/1`	Enters GMPLS UNI controller submode.

Step 5	**tunnel-properties**
	Example:
	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)#`
		Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.

	Command or Action	Purpose
Step 6	**tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# tunnel-id 1001`	Specifies a tunnel-ID for a headend router of a GMPLS tunnel. The tunnel-ID is a 16-bit number ranging from 0 to 65535.
Step 7	**logging events lsp-status state** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# logging events lsp-status state`	Configure events to generate system log messages when state changes occur on the GMPLS tunnel. If omitted, no events will result in the generation of system log messages.
Step 8	**destination ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# destination ipv4 unicast 102.3.233.1`	Specifies a tunnel destination for a headend router of a GMPLS tunnel. The destination argument is an IPv4 address.
Step 9	**path-option** *number* **explicit name** *name* **lockdown verbatim** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 10 explicit name explicit_path_a lockdown verbatim`	Specifies an explicit path for a headend router of a GMPLS tunnel. The path-option range is 1 to 1000. **Note** lockdown and verbatim are mandatory in ERO path option.
Step 10	**commit**	

Verifying an ERO Configuration: Example

The following example shows how to verify an ERO configuration:

```
RP/0/RP0/CPU0:router# show mpls traffic-eng tunnels 1001 detail

Name: GMPLS-UNI-dwdm0_3_0_0  Destination: 172.16.0.1
  Signalled-Name: head_ot1001_172.16.0.1
GMPLS UNI tunnel controlling link dwdm0/3/0/0, tunnel-id: 1001
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10, (LOCKDOWN verbatim) type explicit explicit_path_a (Basis for Setup,
path weight 0)
    G-PID: 0x0800 (derived from egress interface properties)
    Creation Time: Fri Jul 17 08:41:21 ---- (3d07h ago)
 ……
  Current LSP Info:
    Instance: 20
    Uptime: 00:00:33 (since Mon Jul 20 ---- 15:45:22)
    Upstream label:
      Optical label:
      Grid               : DWDM
      Channel spacing    : 50 GHz
```

```
    Identifier          : 0
    Channel Number      : 60
  Downstream label:
    Optical label:
    Grid                : DWDM
    Channel spacing     : 50 GHz
    Identifier          : 0
    Channel Number      : 60
  Router-IDs: local      10.0.0.1
              downstream 172.16.0.1
  Soft Preemption: None
  SRLGs: not collected
  Path Info:
    Outgoing:
      Explicit Route:
        Strict, 10.10.10.2
        Strict, 11.11.11.3
        Strict, 12.12.12.3
```

…….

Configuring Wavelength for a Path Option

Perform this task to configure wavelength for a path option for a GMPLS tunnel.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **tunnel-properties**
6. **tunnel-id** *number*
7. **destination ipv4 unicast** *address*
8. **path-option** *number* **explicit name** *name* **signaled-label dwdm wavelength** *dwdm channel number* **lockdown verbatim**
9. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.

	Command or Action	Purpose
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-uni)# controller dwdm 0/3/0/0`	Enters GMPLS UNI controller submode.

Step 5	**tunnel-properties**
	Example:
	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)#`
		Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.

Step 6	**tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# tunnel-id 1001`	Specifies a tunnel-ID for a headend router of a GMPLS tunnel. The tunnel-ID is a 16-bit number ranging from 0 to 65535.
Step 7	**destination ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# destination ipv4 unicast 172.16.0.1`	Specifies a tunnel destination for a headend router of a GMPLS tunnel. The destination argument is an IPv4 address.
Step 8	**path-option** *number* **explicit name** *name* **signaled-label dwdm wavelength** *dwdm channel number* **lockdown verbatim** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 10 explicit name exp_all_loose_hop signaled-label dwdm wavelength 10 lockdown verbatim`	Specifies a wavelength for the path option. The DWDM channel number range is 1 to 89. The DWDM channel number configured is formulated as 61-channel number. So, if we want channel number 42 (in the supported channel list), the configured "DWDM channel number" will be 61 - 42 = 19.
Step 9	**commit**	

Configuring and Verifying Wavelength Configuration: Examples

The following sequence of examples show how to add a wavelength to a path option for a GMPLS tunnel and verify the outgoing label is set accordingly.

This example shows how to configure a GMPLS tunnel with no ERO path option.

```
gmpls optical-uni
  controller dwdm0/3/0/0
   tunnel-properties
    tunnel-id 1001
    destination ipv4 unicast 172.16.0.1
    path-option 10 no-ero lockdown
   !
  !
 !
```

This example shows how to verify the default values for the outgoing label (UNI-N source, channel number same as Default Channel) and the list of valid wavelengths.

```
RP/0/RP0/CPU0:router#show mpls traffic-eng link-management optical-uni controller dwdm
0/3/0/0

Optical interface: dwdm0/3/0/0
  Overview:
    IM state: Up
    Child interface: POS0_3_0_0: IM state Up
    OLM/LMP state: Up
    Optical tunnel state: up
  Connection:
    Tunnel role: Head
    Tunnel-id: 1001, LSP-id 21, Extended tunnel-id 10.0.0.1
    Tunnel source: 10.0.0.1, destination: 172.16.0.1
    Optical router-ids: Local: 10.0.0.1, Remote: 172.16.0.1
    Label source: UNI-N
    Upstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 60
    Downstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 60
    SRLG discovery: Disabled
    SRLG announcement: None
...
  Optical capabilities:
    Controller type: DWDM
    Channel spacing: 50 GHz
    Default channel: 60
    89 supported channels:
      -28, -27, -26, -25, -24, -23, -22, -21
      -20, -19, -18, -17, -16, -15, -14, -13
      -12, -11, -10, -9, -8, -7, -6, -5
      -4, -3, -2, -1, 0, 1, 2, 3
      4, 5, 6, 7, 8, 9, 10, 11
      12, 13, 14, 15, 16, 17, 18, 19
      20, 21, 22, 23, 24, 25, 26, 27
      28, 29, 30, 31, 32, 33, 34, 35
      36, 37, 38, 39, 40, 41, 42, 43
      44, 45, 46, 47, 48, 49, 50, 51
      52, 53, 54, 55, 56, 57, 58, 59
      60
```

```
    Controller SRLGs
      None
```

This example shows how to set valid wavelength 10 (61 - 51) for the current path.

```
gmpls optical-uni
  controller dwdm0/3/0/0
   tunnel-properties
    tunnel-id 1001
    destination ipv4 unicast 172.16.0.1
   path-option 10 explicit name explicit_all_loose_multi_hop signaled-label dwdm wavelength
 10 lockdown verbatim
   !
  !
 !
```

This example shows how to verify that the tunnel is up and the specified wavelength is used (label source is UNI-C and outgoing label is 51).

```
RP/0/RP0/CPU0:router#show mpls traffic-eng link-management optical-uni controller dwdm
0/3/0/0

Optical interface: dwdm0/3/0/0
  Overview:
    IM state: Up
    Child interface: POS0_3_0_0: IM state Up
    OLM/LMP state: Up
    Optical tunnel state: up
  Connection:
    Tunnel role: Head
    Tunnel-id: 1001, LSP-id 23, Extended tunnel-id 10.0.0.1
    Tunnel source: 10.0.0.1, destination: 172.16.0.1
    Optical router-ids: Local: 10.0.0.1, Remote: 172.16.0.1
    Label source: UNI-C
    Upstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 51
    Downstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 51
    SRLG discovery: Disabled
    SRLG announcement: None
...
  Optical capabilities:
    Controller type: DWDM
    Channel spacing: 50 GHz
    Default channel: 60
    89 supported channels:
      -28, -27, -26, -25, -24, -23, -22, -21
      -20, -19, -18, -17, -16, -15, -14, -13
      -12, -11, -10, -9, -8, -7, -6, -5
      -4, -3, -2, -1, 0, 1, 2, 3
      4, 5, 6, 7, 8, 9, 10, 11
      12, 13, 14, 15, 16, 17, 18, 19
      20, 21, 22, 23, 24, 25, 26, 27
```

```
      28, 29, 30, 31, 32, 33, 34, 35
      36, 37, 38, 39, 40, 41, 42, 43
      44, 45, 46, 47, 48, 49, 50, 51
      52, 53, 54, 55, 56, 57, 58, 59
      60
    Controller SRLGs
      None
```

This example shows how to verify the upstream label on the tunnel tail.

```
RP/0/RP0/CPU0:router#show mpls traffic-eng link-management optical-uni controller dwdm
0/3/0/0

Optical interface: dwdm0/3/0/0
  Overview:
    IM state: Up
    Child interface: POS0_3_0_0: IM state Up
    OLM/LMP state: Up
    Optical tunnel state: up
  Connection:
    Tunnel role: Tail
    Tunnel-id: 1001, LSP-id 23, Extended tunnel-id 10.0.0.1
    Tunnel source: 10.0.0.1, destination: 172.16.0.1
    Optical router-ids: Local: 172.16.0.1, Remote: 10.0.0.1
    Label source: UNI-N
    Upstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 51
    Downstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 51
    SRLG discovery: Disabled
    SRLG announcement: None
…..
  Optical capabilities:
    Controller type: DWDM
    Channel spacing: 50 GHz
    Default channel: 60
    89 supported channels:
      -28, -27, -26, -25, -24, -23, -22, -21
      -20, -19, -18, -17, -16, -15, -14, -13
      -12, -11, -10, -9, -8, -7, -6, -5
      -4, -3, -2, -1, 0, 1, 2, 3
      4, 5, 6, 7, 8, 9, 10, 11
      12, 13, 14, 15, 16, 17, 18, 19
      20, 21, 22, 23, 24, 25, 26, 27
      28, 29, 30, 31, 32, 33, 34, 35
      36, 37, 38, 39, 40, 41, 42, 43
      44, 45, 46, 47, 48, 49, 50, 51
      52, 53, 54, 55, 56, 57, 58, 59
      60
    Controller SRLGs
      None
```

Configuring Multiple Path Options

Perform this task to configure multiple path options for a single tunnel.

Note If a tunnel is up and a lower index path option is configured, the tunnel does not try the lower index path option, unless for some reason the tunnel is flapped or reoptimized.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **tunnel-properties**
6. **tunnel-id** *number*
7. **logging events lsp-status state**
8. **destination ipv4 unicast** *address*
9. **path-option** *number* **explicit name** *name* **lockdown verbatim**
10. **path-option** *number* **explicit name** *name* **lockdown verbatim**
11. **path-option** *number* **no-ero lockdown**
12. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *interface* **Example:**	Enters GMPLS UNI controller submode.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-te-gmpls-uni)# controller dwdm 0/3/0/0`	

Step 5	**tunnel-properties**
	Example:
	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)#`
		Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.

Step 6	**tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# tunnel-id 1001`	Specifies a tunnel-ID for a headend router of a GMPLS tunnel. The tunnel-ID is a 16-bit number ranging from 0 to 65535.
Step 7	**logging events lsp-status state** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# logging events lsp-status state`	Configure events to generate system log messages when state changes occur on the GMPLS tunnel. If omitted, no events will result in the generation of system log messages.
Step 8	**destination ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# destination ipv4 unicast 172.16.0.1`	Specifies a tunnel destination for a headend router of a GMPLS tunnel. The destination argument is an IPv4 address.
Step 9	**path-option** *number* **explicit name** *name* **lockdown verbatim** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 10 explicit name explicit_path_a lockdown verbatim`	Specifies a path option for a headend router of a GMPLS tunnel. The path-option range is 1 to 1000.
Step 10	**path-option** *number* **explicit name** *name* **lockdown verbatim** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 20 explicit name explicit_path_b lockdown verbatim`	Specifies a path option. The path-option range is 1 to 1000.
Step 11	**path-option** *number* **no-ero lockdown** **Example:**	Specifies a path option with no ERO.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)#` **`path-option 30 no-ero lockdown`**	
Step 12	**commit**	

Configuring and Verifying Multiple Path Options: Examples

This example shows how to configure multiple path options.

```
mpls traffic-eng
 gmpls optical-uni
   controller dwdm0/2/0/2
    tunnel-properties
     path-option 10 explicit name explicit_path_a lockdown verbatim
     path-option 20 explicit name explicit_path_b lockdown verbatim
     path-option 30 no-ero lockdown
    !
   !
```

The following sequence of examples show how to configure a GMPLS tunnel, add a new path option with a lower index than the path option in use, flap the tunnel and verify that the new path option (with a lower index) is used .

This example shows how to configure a GMPLS tunnel with one path option.

```
gmpls optical-uni
  controller dwdm0/3/0/0
   tunnel-properties
    tunnel-id 1001
    destination ipv4 unicast 172.16.0.1
    path-option 10 explicit name explicit_path_a lockdown verbatim
   !
  !
 !
```

This example shows how to verify the tunnel path and status with a show command.

```
RP/0/RP0/CPU0:router#show mpls traffic-eng tunnels 1001 detail

Name: GMPLS-UNI-dwdm0_3_0_0  Destination: 172.16.0.1
  Signalled-Name: head_ot1001_172.16.0.1
GMPLS UNI tunnel controlling link dwdm0/3/0/0, tunnel-id: 1001
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10, (LOCKDOWN verbatim) type explicit explicit_path_a (Basis for Setup,
path weight 0)
    G-PID: 0x0800 (derived from egress interface properties)
    Creation Time: Fri Jul 17 08:41:21 ---- (3d06h ago)
...
```

This example shows how to add another path option with a lower index.

```
gmpls optical-uni
  controller dwdm0/3/0/0
```

```
   tunnel-properties
    tunnel-id 1001
    destination ipv4 unicast 172.16.0.1
    path-option 1 no-ero lockdown
    path-option 10 explicit name explicit_path_a lockdown verbatim
   !
  !
 !
```

Flag the tunnel (or trigger reoptimization) and verify that the tunnel comes up on the path with a lower index.

```
RP/0/RP0/CPU0:router#show mpls traffic-eng tunnels 1001 detail

Name: GMPLS-UNI-dwdm0_3_0_0  Destination: 172.16.0.1
  Signalled-Name: head_ot1001_172.16.0.1
GMPLS UNI tunnel controlling link dwdm0/3/0/0, tunnel-id: 1001
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 1, (LOCKDOWN) type no-ero  (Basis for Setup, path weight 0)
    Last Signalled Error : Mon Jul 20 17:03:00 2015
      Info: [24] PathErr(2,2)-(Admin, reason unknown) at 50.0.0.2
    path option 10, (LOCKDOWN verbatim) type explicit explicit_all_loose_multi_hop
    Last Signalled Error : Mon Jul 20 17:03:00 ----
      Info: [25] PathErr(2,2)-(Admin, reason unknown) at 50.0.0.2
```

Enabling SRLG Discovery

Perform this task to enable SRLG discovery on the head node of a nLight tunnel.

Note

- SRLG discovery/recording is enabled only on the headend for each tunnel.
- SRLG discovery/recording allows a maximum of 62 SRLGs in RSVP, which is different from the maximum count of 64 in RSI.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **tunnel-properties**
6. **logging events lsp-status state**
7. **tunnel-id** *number*
8. **record srlg**
9. **destination ipv4 unicast** *address*
10. **path-option** *number* **no-ero lockdown**
11. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-uni)# controller dwdm 0/2/0/0`	Enters GMPLS UNI controller submode.

Step 5	**tunnel-properties**
	Example:
	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)#`
		Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.

Step 6	**logging events lsp-status state** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# logging events lsp-status state`	Configure events to generate system log messages when state changes occur on the GMPLS tunnel. If omitted, no events will result in the generation of system log messages.
Step 7	**tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# tunnel-id 100`	Specifies a tunnel-ID for a headend router of a GMPLS tunnel. The tunnel-ID is a 16-bit number ranging from 0 to 65535.

	Command or Action	Purpose
Step 8	**record srlg** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# record srlg`	Enables SRLG recording.
Step 9	**destination ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# destination ipv4 unicast 192.168.1.2`	Specifies a tunnel destination for a headend router of a GMPLS tunnel. The destination argument is an IPv4 address.
Step 10	**path-option** *number* **no-ero lockdown** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 10 no-ero lockdown`	Specifies the path option for a headend router of a nLight (GMPLS) tunnel. The path-option range is 1 to 1000.
Step 11	**commit**	

Verifying SRLG Discovery Configuration: Examples

This example shows how to verify SRLG discovery configuration.

```
RP/0/0/CPU0:router#show mpls traffic-eng tunnels 100 detail

Name: GMPLS-UNI-dwdm0_2_0_0  Destination: 192.168.1.2
  Signalled-Name: rtrA_ot100_192.168.1.2
GMPLS UNI tunnel controlling link dwdm0/2/0/0, tunnel-id: 100
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected

    path option 10, (LOCKDOWN) type no-ero  (Basis for Setup, path weight 0)
    G-PID: 0x0800 (derived from egress interface properties)
    Creation Time: Mon Jul 20 19:32:03 ---- (00:48:02 ago)
  Config Parameters:
    Priority:  7  7 Affinity: 0x0/0xffff
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    SRLG discovery: Enabled
….
 Soft Preemption: None
    SRLGs: mandatory collection
    Path Info:
  ….
    Resv Info:
      Record Route:
        IPv4 10.10.10.2, flags 0x0
        SRLGs: 21, 22, 23, 24
      Fspec: avg rate=10000 kbits, burst=1000 bytes, peak rate=10000 kbits
Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 2) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

This example shows how to verify SRLG discovery configuration at the headend and the tailend. The output shows the list of SRLGs.

```
RP/0/0/CPU0:router#show srlg

  System Information::
  Interface Count          : 4 (Maximum Interfaces Supported 512)
  Group Count              : 0 (Maximum Groups Supported 50)
  Inherit Location Count   : 0 (Maximum Inherit Locations Supported 10)
  Optical Interfaces Count : 4 (Maximum Optical Interfaces Supported 500)

  Interface    : GigabitEthernet0/2/0/0, Value Count : 10, Registrations : 2
  SRLG Values  : 11, 12, 13, 14, 15
                 21, 22, 23, 24, 25                                          -> Note:
These are announced srlgs.

  Interface    : GigabitEthernet0/2/0/2, Value Count : 0, Registrations : 1
  SRLG Values  :

  Interface    : GigabitEthernet0/2/0/4, Value Count : 0, Registrations : 2
  SRLG Values  :

  Interface    : GigabitEthernet0/2/0/5, Value Count : 0, Registrations : 2
  SRLG Values  :

  Optical Interface: dwdm0/2/0/0, Value Count : 5, References: 2
  SRLG Values      : 11, 12, 13, 14, 15                                       -> Note:
These are locally configured srlgs for controller (dwdm)

  Optical Interface: dwdm0/2/0/1, Value Count : 0, References: 1
  SRLG Values      :

  Optical Interface: dwdm0/2/0/2, Value Count : 0, References: 1
  SRLG Values      :

  Optical Interface: dwdm0/2/0/3, Value Count : 0, References: 1
  SRLG Values      :
```

Enabling SRLG Announce

Perform this task to enable SRLG announce. SRLG announce can be enabled on both headend and tailend.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **gmpls optical-uni**
4. **controller dwdm** *interface*
5. **announce srlgs**
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 4	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-uni)# controller dwdm 0/1/0/1`	Enters GMPLS UNI controller submode.
Step 5	**announce srlgs** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# announce srlgs`	Announces discovered SRLGs to the system.
Step 6	**commit**	

Verifying SRLG Announce Configuration: Example

The following example shows how to verify SRLG announce configuration:

```
RP/0/0/CPU0:router#show srlg

  System Information::
  Interface Count          : 2 (Maximum Interfaces Supported 512)
  Group Count              : 0 (Maximum Groups Supported 50)
  Inherit Location Count   : 0 (Maximum Inherit Locations Supported 10)
  Optical Interfaces Count : 5 (Maximum Optical Interfaces Supported 500)

  Interface    : GigabitEthernet0/2/0/4, Value Count : 0, Registrations : 2
  SRLG Values  :
```

```
Interface    : GigabitEthernet0/2/0/5, Value Count : 0, Registrations : 2
SRLG Values  :

Interface: GigabitEthernet0/2/0/0, Value Count : 4, References: 1
SRLG Values      : 21, 22, 23, 24

Optical Interface: dwdm0/2/0/0, Value Count : 3, References: 2
SRLG Values      : 11, 12, 13

Optical Interface: dwdm0/2/0/1, Value Count : 0, References: 1
SRLG Values      :

Optical Interface: dwdm0/2/0/2, Value Count : 0, References: 1
SRLG Values      :

Optical Interface: dwdm0/2/0/3, Value Count : 0, References: 1
SRLG Values      :
```

Configuring SRLG Diversity

Perform this task to configure SRLG diversity with the best-effort or strict exclusion.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **attribute-set xro** *name*
4. **exclude [best-effort | strict] srlg value** *number*
5. **exit**
6. **gmpls optical-uni**
7. **controller dwdm** *interface*
8. **announce srlgs**
9. **tunnel-properties**
10. **logging events lsp-status state**
11. **tunnel-id** *number*
12. **record srlg**
13. **destination ipv4 unicast** *address*
14. **path-option** *number* **no-ero xro-attribute-set exclude_srlgs lockdown**
15. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure** **Example:** `RP/0/RSP0/CPU0:router# configure`	Enters Global Configuration mode.

	Command or Action	Purpose
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS-TE configuration mode.
Step 3	**attribute-set xro** *name* **Example:** `RP/0/RSP0/CPU0:router(config-te)# attribute-set xro exclude_srlgs`	Enters the attribute set submode and specifies the attribute set name.
Step 4	**exclude [best-effort | strict] srlg value** *number* **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# exclude best-effort srlg value 21`	Specifies path diversity based on SRLG.
Step 5	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-te-attribute-set)# exit`	Exits attribute-set submode.
Step 6	**gmpls optical-uni** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# gmpls optical-uni`	Enters GMPLS UNI configuration submode.
Step 7	**controller dwdm** *interface* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-uni)# controller dwdm 0/2/0/0`	Enters GMPLS UNI controller submode.
Step 8	**announce srlgs** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# announce srlgs`	Announces discovered SRLGs to the system.
Step 9	**tunnel-properties** **Example:**	Enters the submode to configure tunnel-specific information for a GMPLS UNI controller.

	Command or Action	Purpose

	`RP/0/RSP0/CPU0:router(config-te-gmpls-cntl)# tunnel-properties`
	
	`RP/0/RSP0/CPU0:router(config-te-gmpls-tun)#`	

Step 10	**logging events lsp-status state** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# logging events lsp-status state`	Configure events to generate system log messages when state changes occur on the GMPLS tunnel. If omitted, no events will result in the generation of system log messages.
Step 11	**tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# tunnel-id 100`	Specifies a tunnel-ID for a headend router of a GMPLS tunnel. The tunnel-ID is a 16-bit number ranging from 0 to 65535.
Step 12	**record srlg** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# record srlg`	Enables SRLG recording.
Step 13	**destination ipv4 unicast** *address* **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# destination ipv4 unicast 192.168.1.2`	Specifies a tunnel destination for a headend router of a GMPLS tunnel. The destination argument is an IPv4 address.
Step 14	**path-option** *number* **no-ero xro-attribute-set exclude_srlgs lockdown** **Example:** `RP/0/RSP0/CPU0:router(config-te-gmpls-tun)# path-option 10 no-ero xro-attribute-set exclude_srlgs lockdown`	The XRO attribute set is attached to the GMPLS UNI tunnel through the path option. The path-option range is 1 to 1000.
Step 15	**commit**	

Verifying SRLG Diversity Configuration: Example

The following example shows how to verify SRLG diversity configuration:

```
RP/0/0/CPU0:router#show mpls traffic-eng tunnels 100 detail

Name: GMPLS-UNI-dwdm0_2_0_0  Destination: 192.168.1.2
  Signalled-Name: rtrA_ot100_192.168.1.2
GMPLS UNI tunnel controlling link dwdm0/2/0/0, tunnel-id: 100
  Status:
    Admin:    up Oper:   up   Path:  valid   Signalling: connected
```

```
    path option 10, (LOCKDOWN) type no-ero  (Basis for Setup, path weight 0)
      XRO attribute-set: exclude_srlgs
        Best-effort, SRLG id 21
    Last Signalled Error : Mon Jul 20 20:55:33 ----
      Info: [5] PathErr(24,67)-(routing, route blocked by exclude route) at 10.10.10.2
    G-PID: 0x0800 (derived from egress interface properties)
    Creation Time: Mon Jul 20 19:32:03 2015 (01:25:19 ago)
  Config Parameters:
    Priority:  7  7 Affinity: 0x0/0xffff
    Path Protection: Not Enabled
    BFD Fast Detection: Disabled
    Reoptimization after affinity failure: Enabled
    SRLG discovery: Enabled
  Binding Label: 0
  History:
    Tunnel has been up for: 00:00:23 (since Mon Jul 20 20:56:59 EDT 2015)
    Current LSP:
      Uptime: 00:00:23 (since Mon Jul 20 20:56:59 EDT ----)
  Current LSP Info:
    Instance: 6
    Uptime: 00:00:23 (since Mon Jul 20 20:56:59 EDT ----)
    Upstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 16
    Downstream label:
      Optical label:
      Grid                : DWDM
      Channel spacing     : 50 GHz
      Identifier          : 0
      Channel Number      : 16
    Router-IDs: local      192.168.1.1
                downstream 192.168.1.2
    Soft Preemption: None
    SRLGs: mandatory collection
    Path Info:
      Outgoing:
        No ERO
      Route Exclusions:
        Best-effort, SRLG id 21
      Record Route: Disabled
      Tspec: avg rate=10000 kbits, burst=1000 bytes, peak rate=10000 kbits
      Session Attributes: Local Prot: Not Set, Node Prot: Not Set, BW Prot: Not Set
    Resv Info:
      Record Route:
        IPv4 10.10.10.2, flags 0x0
        SRLGs: 21, 22, 23, 24
      Fspec: avg rate=10000 kbits, burst=1000 bytes, peak rate=10000 kbits
Displayed 1 (of 3) heads, 0 (of 0) midpoints, 0 (of 2) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads
```

Configuration Examples for GMPLS UNI

These configuration examples are provided for GMPLS UNI:

Configuring Head UNI-C for a GMPLS Tunnel: Example

This example shows the minimal head UNI-C configuration require to establish a GMPLS tunnel:

```
rsvp
  controller dwdm 0/1/0/1
    signalling refresh out-of-band interval 3600
    signalling refresh out-of-band missed 24
  !
!
mpls traffic-eng
  gmpls optical-uni
    controller dwdm 0/1/0/1
      tunnel-properties
        tunnel-id 100
        destination 100.20.20.20
        path-option 10 no-ero
      !
    !
  !
!
lmp
  gmpls optical-uni
    router-id 100.11.11.11
    neighbor nbr_A
      ipcc routed
      neighbor router-id ipv4 unicast 100.12.12.12
    !
    controller dwdm 0/1/0/1
      neighbor nbr_A
      link-id ipv4 unicast 192.168.100.1
      neighbor link-id ipv4 unicast 192.168.100.2
      neighbor interface-id unnumbered 13
    !
  !
!
```

Configuring Tail UNI-C for a GMPLS Tunnel: Example

This example shows the minimal tail UNI-C configuration require to establish a GMPLS tunnel:



Note The controller must be specified under the GMPLS UNI submode to inform TE that incoming GMPLS path messages are to be accepted and processed.

```
rsvp
  controller dwdm 0/1/0/1
    signalling refresh out-of-band interval 3600
    signalling refresh out-of-band missed 24
  !
!
mpls traffic-eng
  gmpls optical-uni
    controller dwdm 0/1/0/1
    !
```

```
    !
  !
  lmp
    gmpls optical-uni
      router-id 100.20.20.20
      neighbor nbr_B
        ipcc routed
        neighbor router-id ipv4 unicast 100.19.19.19
      !
      controller dwdm 0/1/0/1
        neighbor nbr_B
        link-id ipv4 unicast 192.168.103.2
        neighbor link-id ipv4 unicast 192.168.103.1
        neighbor interface-id unnumbered 22
      !
    !
  !
```

Configuring LSP Diversity: Example

This example shows the configuration for two diverse LSPs:

```
  mpls traffic-eng
   attribute-set xro exclude-tun1
    exclude best-effort lsp source 88.0.0.8 destination 10.0.0.2 tunnel-id 1
extended-tunnel-id 88.0.0.8
    !
   attribute-set xro exclude-tun2
    exclude strict lsp source 88.0.0.8 destination 10.0.1.2 tunnel-id 2 extended-tunnel-id
 88.0.0.8 lsp-id 2
    !
   gmpls optical-uni
    controller dwdm 0/1/0/0
     tunnel-properties
      logging events lsp-status state
      tunnel-id 1
      destination ipv4 unicast 10.0.0.2
      path-option 10 no-ero xro-attribute-set exclude-tun2
     !
    !
    controller dwdm 0/1/0/1
     tunnel-properties
      logging events lsp-status state
      tunnel-id 2
      destination ipv4 unicast 10.0.1.2
      path-option 10 no-ero xro-attribute-set exclude-tun1
     !
    !
   !
  !
```

Additional References

For additional information related to implementing GMPLS UNI, refer to the following references:

Related Documents

Related Topic	Document Title
GMPLS UNI commands	*GMPLS UNI Commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*
MPLS Traffic Engineering commands	*MPLS Traffic Engineering commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*
RSVP commands	*RSVP commands* module in *MPLS Command Reference for Cisco ASR 9000 Series Routers*
Getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
Information about user groups and task IDs	*Configuring AAA Services* module in *System Security Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

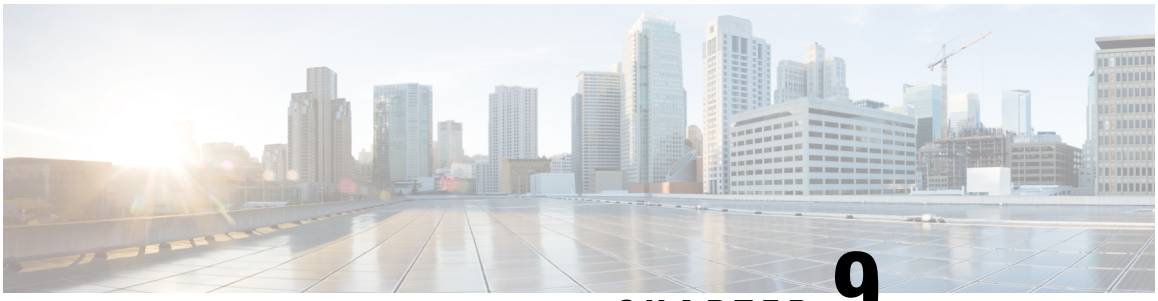
RFCs

RFCs	Title
RFC 3471	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*
RFC 3473	*Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*
RFC 4208	*Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model*

RFCs	Title
RFC 4872	*RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*
RFC 4874	*Exclude Routes - Extension to Resource ReserVation Protocol-Traffic Engineering (RSVP-TE)*
RFC 6205	*Generalized Labels for Lambda-Switch-Capable (LSC) Label Switching Routers*

Technical Assistance

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



CHAPTER 9

Implementing MPLS OAM

- Implementing MPLS OAM, on page 471

Implementing MPLS OAM

MPLS Operations, Administration, and Maintenance (OAM) helps service providers to monitor label-switched paths (LSPs) and quickly isolate MPLS forwarding problems to assist with fault detection and troubleshooting in an MPLS network. This module describes MPLS LSP Ping and Traceroute features which can be used for failure detection and troubleshooting of MPLS networks.

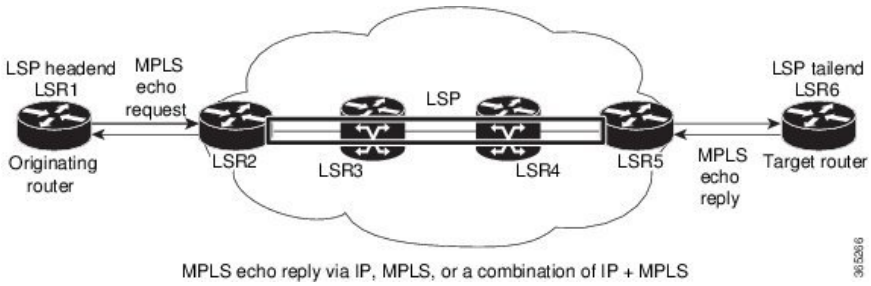
MPLS LSP Ping

The MPLS LSP Ping feature is used to check the connectivity between Ingress LSR and egress LSRs along an LSP. MPLS LSP ping uses MPLS echo request and reply messages, similar to Internet Control Message Protocol (ICMP) echo request and reply messages, to validate an LSP. While ICMP echo request and reply messages validate IP networks, MPLS echo and reply messages validate MPLS networks. The MPLS echo request packet is sent to a target router through the use of the appropriate label stack associated with the LSP to be validated. Use of the label stack causes the packet to be forwarded over the LSP itself. The destination IP address of the MPLS echo request packet is different from the address used to select the label stack. The destination IP address is defined as a 127.x.y.z/8 address and it prevents the IP packet from being IP switched to its destination, if the LSP is broken.

An MPLS echo reply is sent in response to an MPLS echo request. The reply is sent as an IP packet and it is forwarded using IP, MPLS, or a combination of both types of switching. The source address of the MPLS echo reply packet is an address obtained from the router generating the echo reply. The destination address is the source address of the router that originated the MPLS echo request packet. The MPLS echo reply destination port is set to the echo request source port.

The following figure shows MPLS LSP ping echo request and echo reply paths.

Figure 35: MPLS LSP Ping Echo Request and Reply Paths



By default, the **ping mpls ipv4** command tries to determine the Forwarding Equivalence Class (FEC) being used automatically. However, this is only applicable at head-end and works only if the FEC at the destination is same as the source. If the source and destination FEC types are not the same, the **ping mpls ipv4** command may fail to identify the targeted FEC type. You can overcome this limitation by specifying the FEC type in MPLS LSP ping using the **fec-type** command option. If the user is not sure about the FEC type at the transit or the destination, or it may change through network, use of the **generic** FEC type command option is recommended. Generic FEC is not coupled to a particular control plane and allows path verification when the advertising protocol is unknown, or may change during the path of the echo request. If you are aware of the destination FEC type, specify the target FEC as BGP or LDP.

Configuration Examples

This example shows how to use MPLS LSP ping to test the connectivity of an IPv4 LDP LSP. The destination is specified as a Label Distribution Protocol (LDP) IPv4 address.

```
RP/0/RSP0/CPU0:router# ping mpls ipv4 10.1.1.2/32 verbose

Sun Nov 15 11:27:43.070 UTC

Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!      size 100, reply addr 10.1.0.2, return code 3
!      size 100, reply addr 10.1.0.2, return code 3
!      size 100, reply addr 10.1.0.2, return code 3
!      size 100, reply addr 10.1.0.2, return code 3
!      size 100, reply addr 10.1.0.2, return code 3

Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/4 ms
```

In this example, the destination is specified as a Label Distribution Protocol (LDP) IPv4 prefix and Forwarding Equivalence Class (FEC) type is specified as generic.

```
RP/0/RSP0/CPU0:router# ping mpls ipv4 10.1.1.2/32 fec-type generic

Wed Nov 25 03:36:33.143 UTC
Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      timeout is 2 seconds, send interval is 0 msec:
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

In this example, the destination is specified as a Label Distribution Protocol (LDP) IPv4 prefix and the FEC type is specified as BGP.

```
RP/0/RSP0/CPU0:router# ping mpls ipv4 10.1.1.2/32 fec-type bgp

Wed Nov 25 03:38:33.143 UTC
Sending 5, 100-byte MPLS Echos to 10.1.1.2/32,
      timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

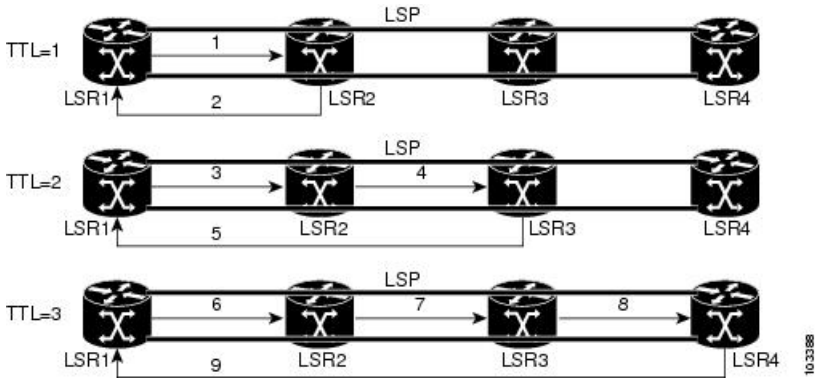
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
```

MPLS LSP Traceroute

The MPLS LSP Traceroute feature is used to isolate the failure point of an LSP. It is used for hop-by-hop fault localization and path tracing. The MPLS LSP Traceroute feature relies on the expiration of the Time to Live (TTL) value of the packet that carries the echo request. When the MPLS echo request message hits a transit node, it checks the TTL value and if it is expired, the packet is passed to the control plane, else the message is forwarded. If the echo message is passed to the control plane, a reply message is generated based on the contents of the request message.

The following figure shows an MPLS LSP traceroute example with an LSP from LSR1 to LSR4.

Figure 36: MPLS LSP Traceroute



By default, the **traceroute mpls ipv4** command tries to determine the Forwarding Equivalence Class (FEC) being used automatically. However, this is only applicable at head-end and works only if the FEC at the destination is same as the source. If the source and destination FEC types are not the same, the **traceroute mpls ipv4** command may fail to identify the targeted FEC type. You can overcome this limitation by specifying the FEC type in MPLS LSP traceroute using the **fec-type** command option. If the user is not sure about the FEC type at the transit or the destination, or it may change through network, use of the **generic** FEC type command option is recommended. Generic FEC is not coupled to a particular control plane and allows path verification when the advertising protocol is unknown, or may change during the path of the echo request. If you are aware of the destination FEC type, specify the target FEC as BGP or LDP.

Configuration Examples

This example shows how to use the **traceroute** command to trace to a destination.

```
RP/0/RSP0/CPU0:router# traceroute mpls ipv4 10.1.1.2/32 destination 127.0.0.3 127.0.0.6 2
Sat Jan 27 03:50:23.746 UTC

Tracing MPLS Label Switched Path to 10.1.1.2/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

Destination address 127.0.0.3
  0 10.2.1.2 MRU 1500 [Labels: 24000 Exp: 0]
L 1 10.2.1.1 MRU 1500 [Labels: implicit-null Exp: 0] 8 ms
! 2 10.1.0.2 3 ms

Destination address 127.0.0.5
  0 10.2.1.2 MRU 1500 [Labels: 24000 Exp: 0]
L 1 10.2.1.1 MRU 1500 [Labels: implicit-null Exp: 0] 5 ms
! 2 10.1.0.2 2 ms
```

This example shows how to use the **traceroute** command and how to specify the maximum number of hops for the traceroute to traverse by specifying the **ttl** value.

```
RP/0/RSP0/CPU0:router# traceroute mpls ipv4 10.1.1.2/32 ttl 1
Sun Nov 15 12:20:14.145 UTC
Tracing MPLS Label Switched Path to 10.1.1.2/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

  0 10.1.0.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.1.0.2 3 ms
```

This example shows how to use the **traceroute** command to trace to a destination and FEC type is specified as generic.

```
RP/0/RSP0/CPU0:router# traceroute mpls ipv4 10.1.1.2/32 fec-type generic
Sun Nov 15 12:25:14.145 UTC
Tracing MPLS Label Switched Path to 10.1.1.2/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 2 ms
```

This example shows how to use the **traceroute** command to trace to a destination and FEC type is specified as BGP.

```
RP/0/RSP0/CPU0:router# traceroute mpls ipv4 10.1.1.2/32 fec-type bgp
Sun Nov 15 12:25:14.145 UTC
Tracing MPLS Label Switched Path to 10.1.1.2/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
Type escape sequence to abort.
0 10.12.12.1 MRU 1500 [Labels: implicit-null Exp: 0]
! 1 10.12.12.2 2 ms
```

Overview of P2MP TE Network

A Point to Multipoint (P2MP) TE network contains the following elements:

- *Headend Router*

  The headend router, also called the source or ingress router, is responsible for initiating the signaling messages that set up the P2MP TE LSP. The headend router can also be a branch point, which means the router performs packet replication and the sub-LSPs split into different directions.

- *Midpoint Router*

  The midpoint router is where the sub-LSP signaling is processed. The midpoint router can be a branch point.

- *Tailend Router*

  The tailend router, also called the destination, egress, or leaf-node router, is where sub-LSP signaling ends. The router which is one of potentially many destinations of the P2MP TE LSP.

- *Bud Router*

  A bud router is a midpoint and tailend router at the same time. An LSR that is an egress LSR, but also has one or more directly connected downstream LSRs.

- *Branch Router*

  A branch router is either a midpoint or tailend router at any given time.

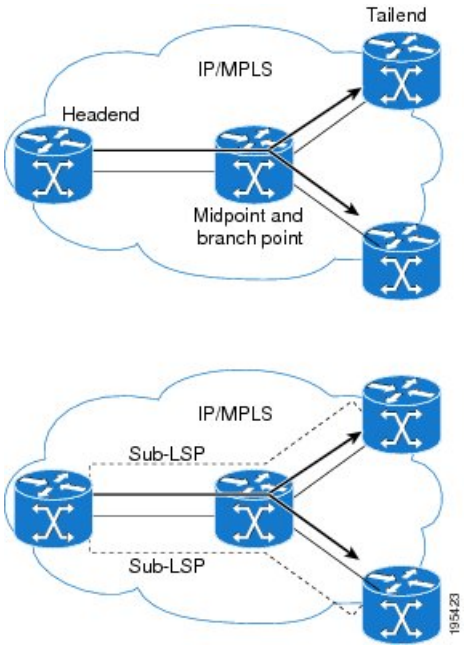
- *Transit Router*

  A transit router is an LSR that is not an egress router, but also has one or more directly connected downstream routers.

- A P2MP tunnel consists of one or more sub-LSPs.All sub-LSPs belonging to the same P2MP tunnel employ the same constraints, protection policies, and so on, which are configured at the headend router.

Elements of P2MP TE Network illustrates the elements of P2MP TE network.

Figure 37: Elements of P2MP TE Network



P2MP TE tunnels build on the features that exist in basic point-to-point TE tunnels. The P2MP TE tunnels have the following characteristics:

- There is one source (headend) but more than one destination (tailend).
- They are unidirectional.

- They are explicitly routed.
- Multiple sub-LSPs connect the headend router to various tailend routers.

P2MP Ping

The P2MP ping feature is used to check the connectivity between Ingress LSR and egress LSR, along a P2MP LSP. The Ingress LSR sends the P2MP echo request message along the specified P2MP LSP. All egress LSRs which receive the P2MP echo request message from the ingress LSR must send a P2MP echo reply message to the ingress LSR, according to the reply mode specified in the P2MP echo request message.

P2MP Traceroute

The P2MP traceroute feature is used to isolate the failure point of a P2MP LSP.

Traceroute can be applied to all nodes in the P2MP tree. However, you can select a specific traceroute target through the P2MP Responder Identifier TLV. An entry in this TLV represents an responder-id or a transit node. This is only the case for P2MP TE LSPs.



Note Only P2MP TE LSP IPv4 is supported. If the Responder Identifier TLV is missing, the **echo request** requests information from all responder-ids.

MPLS OAM Support for BGP 3107

The MPLS OAM Support for BGP 3107 feature provides support for ping, traceroute and treetrace (traceroute multipath) operations for LSPs signaled via BGP for the IPv4 unicast prefix FECs in the default VRF, according to the *RFC 3107 - Carrying Label Information in BGP-4*. This feature adds support for MPLS OAM operations in the seamless MPLS architecture deployments, i.e., combinations of BGP and LDP signaled LSPs.

For more information about ping and traceroute, see *Implementing MPLS OAM* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information about ping and traceroute commands, see *MPLS OAM Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

IP-Less MPLS-TP Ping and MPLS-TP Traceroute

According to RFC-6426, IP-Less MPLS-TP ping and MPLS-TP traceroute with the ACH header, if a node receives an MPLS-TP ping or traceroute request packet over ACH, without IP or UDP headers, the node drops the echo request packet and does not send a response when:

- the reply mode is 4
- the node does not have a return MPLS LSP path to the echo request source.

If a node receives an MPLS echo request with a reply mode other than 4 (i.e., reply via application-level control channel), the node responds to using that reply mode. If the node does not support the reply mode requested, or is unable to reply using the requested reply mode in any specific instance, the node drops the echo request packet and does not send a response.

For more information about ping and traceroute, see *Implementing MPLS OAM* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*. For more information about ping and traceroute commands, see *MPLS OAM Commands* chapter in the *MPLS Command Reference for Cisco ASR 9000 Series Routers*.

Configuration Examples: P2MP Ping and P2MP Traceroute

This example shows an extract of the P2MP ping command.

```
RP/0/RSP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10
Sending 1, 100-byte MPLS Echos to tunnel-mte10,
      timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 192.168.222.2
! reply addr 192.168.140.2
! reply addr 192.168.170.1

Success rate is 100 percent (3 received replies/3 expected replies),
     round-trip min/avg/max = 154/232/302 ms
```

This example shows an extract of the P2MP ping command with the jitter option.

```
RP/0/RSP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10 jitter 300

Sending 1, 100-byte MPLS Echos to tunnel-mte10,
      timeout is 2.3 seconds, send interval is 0 msec, jitter value is 300 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 192.168.222.2
! reply addr 192.168.140.2
! reply addr 192.168.170.1

Success rate is 100 percent (3 received replies/3 expected replies),
     round-trip min/avg/max = 148/191/256 ms
```

This example shows an extract of the P2MP ping command with the ddmap option.

```
RP/0/RSP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10 ddmap

Sending 1, 100-byte MPLS Echos to tunnel-mte10,
      timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 192.168.222.2
! reply addr 192.168.140.2
! reply addr 192.168.170.1

Success rate is 100 percent (3 received replies/3 expected replies),
     round-trip min/avg/max = 105/178/237 ms



RP/0/RSP0/CPU0:router# show mpls traffic-eng tunnels p2mp 10
Mon Apr 12 12:13:55.075 EST
Signalling Summary:
              LSP Tunnels Process:  running
                     RSVP Process:  running
                       Forwarding:  enabled
          Periodic reoptimization:  every 3600 seconds, next in 654 seconds
           Periodic FRR Promotion:  every 300 seconds, next in 70 seconds
          Auto-bw enabled tunnels:  0 (disabled)

Name: tunnel-mte10
   Status:
     Admin: up  Oper: up (Up for 12w4d)

     Config Parameters:
      Bandwidth: 0 kbps (CT0) Priority: 7 7 Affinity: 0x0/0xffff
      Metric Type: TE (default)
      Fast Reroute: Not Enabled, Protection Desired: None
      Record Route: Not Enabled

      Destination summary: (3 up, 0 down, 0 disabled) Affinity: 0x0/0xffff
      Auto-bw: disabled
      Destination: 10.1.0.1
        State: Up for 12w4d
        Path options:
          path-option 1 dynamic     [active]
      Destination: 10.2.0.1
        State: Up for 12w4d
        Path options:
          path-option 1 dynamic     [active]
      Destination: 10.3.0.1
        State: Up for 12w4d
        Path options:
          path-option 1 dynamic     [active]

     History:
       Reopt. LSP:
         Last Failure:
```

```
            LSP not signalled, identical to the [CURRENT] LSP
            Date/Time: Thu Jan 14 02:49:22 EST 2010 [12w4d ago]

      Current LSP:
        lsp-id: 10002 p2mp-id: 10 tun-id: 10 src: 10.0.0.1 extid: 10.0.0.1
        LSP up for: 12w4d
        Reroute Pending: No
        Inuse Bandwidth: 0 kbps (CT0)
        Number of S2Ls: 3 connected, 0 signaling proceeding, 0 down

        S2L Sub LSP: Destination 10.1.0.1 Signaling Status: connected
          S2L up for: 12w4d
          Sub Group ID: 1 Sub Group Originator ID: 10.1.0.1
          Path option path-option 1 dynamic    (path weight 1)
          Path info (OSPF 1 area 0)
            192.168.222.2
            10.1.0.1

        S2L Sub LSP: Destination 10.2.0.1 Signaling Status: connected
          S2L up for: 12w4d
          Sub Group ID: 2 Sub Group Originator ID: 10.0.0.1
          Path option path-option 1 dynamic    (path weight 2)
          Path info (OSPF 1 area 0)
            192.168.222.2
            192.168.140.3
            192.168.140.2
            10.2.0.1

        S2L Sub LSP: Destination 10.3.0.1 Signaling Status: connected
          S2L up for: 12w4d
          Sub Group ID: 3 Sub Group Originator ID: 10.0.0.1
          Path option path-option 1 dynamic    (path weight 2)
          Path info (OSPF 1 area 0)
            192.168.222.2
            192.168.170.3
            192.168.170.1
            10.3.0.1

      Reoptimized LSP (Install Timer Remaining 0 Seconds):
        None
      Cleaned LSP (Cleanup Timer Remaining 0 Seconds):
        None
Displayed 1 (of 16) heads, 0 (of 0) midpoints, 0 (of 0) tails
Displayed 1 up, 0 down, 0 recovering, 0 recovered heads

RP/0/RSP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10 lsp id 10002
Mon Apr 12 12:14:04.532 EST

Sending 1, 100-byte MPLS Echos to tunnel-mte10,
      timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 192.168.222.2
! reply addr 192.168.170.1
```

```
! reply addr 192.168.140.2

Success rate is 100 percent (3 received replies/3 expected replies),
     round-trip min/avg/max = 128/153/167 ms
```

This example shows an extract of the P2MP ping command with the responder-id.

```
RP/0/RSP0/CPU0:router# ping mpls traffic-eng tunnel-mte 10 responder-id 10.3.0.1
Mon Apr 12 12:15:34.205 EST

Sending 1, 100-byte MPLS Echos to tunnel-mte10,
      timeout is 2.2 seconds, send interval is 0 msec, jitter value is 200 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

Request #1
! reply addr 192.168.170.1

Success rate is 100 percent (1 received reply/1 expected reply),
     round-trip min/avg/max = 179/179/179 ms
```

This example shows an extract of the P2MP traceroute command with the ttl option.

```
RP/0/RSP0/CPU0:router# traceroute mpls traffic-eng tunnel-mte 10  ttl 4
Mon Apr 12 12:16:50.095 EST

Tracing MPLS MTE Label Switched Path on tunnel-mte10, timeout is 2.2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

! 1 192.168.222.2 186 ms [Estimated Role: Bud]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]

! 2 192.168.222.2 115 ms [Estimated Role: Bud]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 2 192.168.140.2 213 ms [Estimated Role: Egress]
! 2 192.168.170.1 254 ms [Estimated Role: Egress]

! 3 192.168.222.2 108 ms [Estimated Role: Bud]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 3 192.168.170.1 164 ms [Estimated Role: Egress]
! 3 192.168.140.2 199 ms [Estimated Role: Egress]
```

```
! 4 192.168.170.1 198 ms [Estimated Role: Egress]
! 4 192.168.222.2 206 ms [Estimated Role: Bud]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500
```

This example shows an extract of the P2MP traceroute command with the responder-id option.

```
RP/0/RSP0/CPU0:router# traceroute mpls traffic-eng tunnel-mte 10 responder-id 10.3.0.1
Mon Apr 12 12:18:01.994 EST

Tracing MPLS MTE Label Switched Path on tunnel-mte10, timeout is 2.2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

Type escape sequence to abort.

d 1 192.168.222.2 113 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]

d 2 192.168.222.2 118 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 2 192.168.170.1 244 ms [Estimated Role: Egress]

d 3 192.168.222.2 141 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 3 192.168.170.1 204 ms [Estimated Role: Egress]

d 4 192.168.222.2 110 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 4 192.168.170.1 174 ms [Estimated Role: Egress]
```

This example shows an extract of the P2MP traceroute command with the jitter option.

```
RP/0/RSP0/CPU0:router# traceroute mpls traffic-eng tunnel-mte 10 responder-id 10.3.0.1 ttl
 4 jitter 500
Mon Apr 12 12:19:00.292 EST

Tracing MPLS MTE Label Switched Path on tunnel-mte10, timeout is 2.5 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0, 'd' - DDMAP

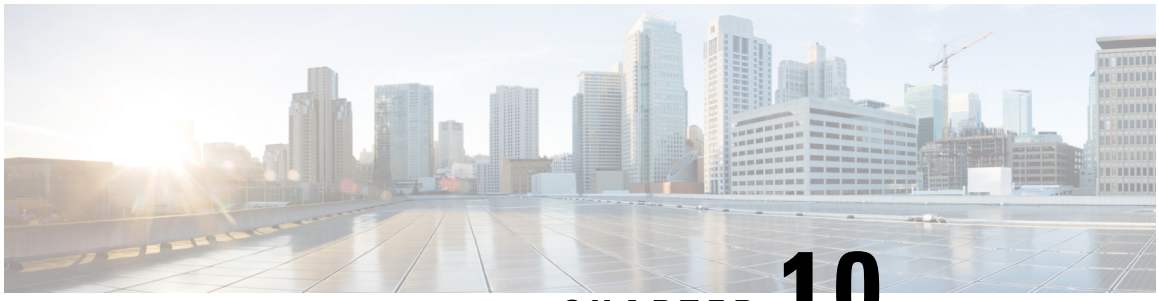
Type escape sequence to abort.
```

```
d 1 192.168.222.2 238 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]

d 2 192.168.222.2 188 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 2 192.168.170.1 290 ms [Estimated Role: Egress]

d 3 192.168.222.2 115 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 3 192.168.170.1 428 ms [Estimated Role: Egress]

d 4 192.168.222.2 127 ms [Estimated Role: Branch]
    [L] DDMAP 0: 192.168.140.2 192.168.140.2 MRU 1500 [Labels: 16001 Exp: 0]
    [L] DDMAP 1: 192.168.170.1 192.168.170.1 MRU 1500 [Labels: 16000 Exp: 0]
! 4 192.168.170.1 327 ms [Estimated Role: Egress]
```



CHAPTER 10

Implementing MPLS Transport Profile

This module describes how to implement MPLS transport profile (MPLS-TP) on the router. MPLS-TP supported by IETF enables the migration of transport networks to a packet-based network that efficiently scale to support packet services in a simple and cost-effective way. MPLS-TP combines the necessary existing capabilities of MPLS with additional minimal mechanisms in order that it can be used in a transport role.

MPLS transport profile enables you to create tunnels that provide the transport network service layer over which IP and MPLS traffic traverse.

Feature History for Implementing MPLS Transport Profile

Release	Modification
Release 4.2.0	This feature was introduced.

- Restrictions for MPLS-TP, on page 485
- Information About Implementing MPLS Transport Profile, on page 486
- How to Implement MPLS Transport Profile, on page 491

Restrictions for MPLS-TP

- Penultimate hop popping is not supported. Only ultimate hop popping is supported, because label mappings are configured at the MPLS-TP endpoints.
- MPLS-TP links must be configured with IP addresses.
- IPv6 addressing is not supported.

L2VPN Restrictions

- Pseudowire ID Forward Equivalence Class (FEC) (type 128) is supported, but generalized ID FEC (type 129) is not supported.
- BFD over pseudowire is not supported. Static pseudowire OAM protocol is used to signal fault on static pseudowire placed over TP tunnels using pseudowire status.
- Only Ethernet pseudowire type is supported.

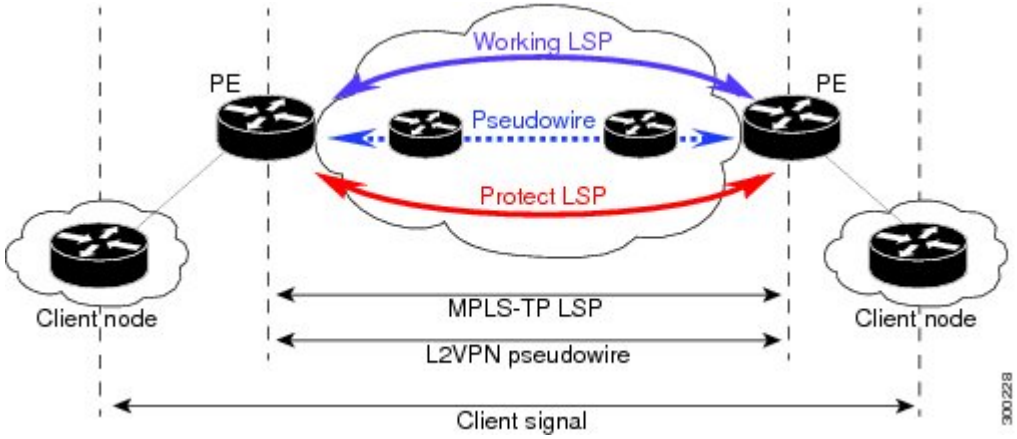
Information About Implementing MPLS Transport Profile

To implement MPLS-TP, you should understand these concepts:

MPLS Transport Profile

MPLS Transport Profile (TP) enables you to create tunnels that provide the transport network service layer over which IP and MPLS traffic traverse. MPLS-TP tunnels enable a transition from Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) time-division multiplexing (TDM) technologies to packet switching, to support services with high bandwidth utilization and low cost. Transport networks are connection oriented, statically provisioned, and have long-lived connections. Transport networks usually avoid control protocols that change identifiers like labels. MPLS-TP tunnels provide this functionality through statically provisioned bidirectional label switched paths (LSPs). This figure shows the MPLS-TP tunnel:

Figure 38: MPLS Transport Profile Tunnel



MPLS-TP combines the necessary existing capabilities of MPLS with additional minimal mechanisms in order that it can be used in a transport role. You can set up MPLS-TP through a CLI or a network management system.

MPLS-TP tunnels have these characteristics:

- An MPLS-TP tunnel can be associated with working LSP, protect LSP, or both LSP
- Statically provisioned bidirectional MPLS-TP label switched paths (LSPs)
- Symmetric or asymmetric bandwidth reservation
- 1:1 path protection with revertive mode for MPLS-TP LSP with revertive mode for MPLS-TP LSP
- Use of Generic Alert Label (GAL) and Generic Associated Channel Header (G-ACH) to transport control packets; for example, BFD packets and pseudowire OAM packets
- BFD is used as a continuity check (CC) mechanism over MPLS-TP LSP
- Remote Defect Indication (RDI) based on BFD
- Fault OAM functions

These services are supported over MPLS-TP tunnels:

- Dynamic spoke pseudowire (for H-VPLS) over static MPLS-TP tunnels.
- Static spoke pseudowire (for H-VPLS) over static MPLS-TP tunnels.
- MS-PW services where static and dynamic pseudowire segments can be concatenated.
- MPLS ping and traceroute over MPLS TP LSP and PW.
- Static routes over MPLS-TP tunnels.
- Pseudowire redundancy for static pseudowire.
- VPWS using static or dynamic pseudowire pinned down to MPLS-TP tunnels.
- VPLS and H-VPLS using static or dynamic pseudowire pinned down to MPLS-TP tunnels.

Bidirectional LSPs

MPLS transport profile (MPLS-TP) LSPs are bidirectional and congruent where LSPs traverse the same path in both directions. An MPLS-TP tunnel can be associated with either working MPLS-TP LSP, protect MPLS-TP LSP, or both. The working LSP is the primary LSP backed up by the protect LSP. When a working LSP goes down, protect LSP is automatically activated. In order for an MPLS-TP tunnel to be operationally up, it must be configured with at least one LSP.

MPLS-TP Path Protection

Path protection provides an end-to-end failure recovery mechanism (that is, full path protection) for MPLS-TP tunnels. MPLS-TP LSPs support 1:1 path protection. You can configure the working and protect LSPs as part of configuring the MPLS-TP tunnel. The working LSP is the primary LSP used to route traffic, while the protect LSP is a backup for a working LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time traffic forwarding reverts back to the working LSP (revertive mode).

Fault OAM Support

The fault OAM protocols and messages support the provisioning and maintenance of MPLS-TP tunnels and bidirectional LSPs:

- **Generic Associated Channel**

  Generic Associated Channel (G-ACh) is the control channel mechanism associated with MPLS LSPs in addition to MPLS pseudowire. The G-ACh Label (GAL) (Label 13) is a generic alert label to identify the presence of the G-ACh in the label packet. It is taken from the reserved MPLS label space.

  G-ACh or GAL is used to support in-band OAMs of MPLS-TP LSPs and pseudowires. The OAM messages are used for fault management, connection verification, continuity check and other functions.

  These messages are forwarded along the specified MPLS LSP:

  - OAM Fault Management: Alarm Indication Signal (AIS), Link Down Indication (LDI), and Lock Report (LKR) messages (GAL with fault-OAM channel)
  - OAM Connection Verification: Ping and traceroute messages (GAL with IP channel)

- BFD messages (GAL with BFD channel)

These messages are forwarded along the specified pseudowire:

- Static pseudowire OAM messages (static pseudowire status)
- Pseudowire ping and traceroute messages

- **Fault Management: Alarm Indication Signal (AIS), Link Down Indication (LDI), and Lock Report (LKR) messages**

  LDI messages are generated at midpoint nodes when a failure is detected. The midpoint sends the LDI message to the endpoint that is reachable with the existing failure. The midpoint node also sends LKR messages to the reachable endpoint, when an interface is administratively down. AIS messages are not generated by Cisco platforms, but are processed if received. By default, the reception of LDI and LKR on the active LSP at an endpoint will cause a path protection switchover, while AIS will not.

- **Fault Management: Emulated Protection Switching for LSP Lockout**

  You can implement a form of **Emulated Protection Switching** in support of LSP Lockout using customized fault messages. When a Cisco Lockout message is sent, it does not cause the LSP to be administratively down. The Cisco Lockout message causes a path protection switchover and prevents data traffic from using the LSP. The LSP's data path remains up so that BFD and other OAM messages can continue to traverse it. Maintenance of the LSP can take place such as reconfiguring or replacing a midpoint LSR. BFD state over LSP must be **up** and MPLS ping and traceroute can be used to verify the LSP connectivity, before the LSP is put back into service by removing the lockout. You cannot lockout working and protect LSPs simultaneously.

- **LSP ping and traceroute**

  For MPLS-TP connectivity verification, you can use **ping mpls traffic-eng tunnel-tp** and **traceroute mpls traffic-eng tunnel-tp** commands. You can specify that the echo requests be sent along the working LSP or the protect LSP. You can also specify that the echo request be sent on a locked out MPLS-TP tunnel LSP (either working or protect) if the working or protect LSP is explicitly specified.

- **Continuity Check through BFD**

  BFD session is automatically created on MPLS-TP LSPs with default parameters. You can override the default BFD parameters either through global commands or per-tunnel commands. Furthermore, you can optionally specify different BFD parameters for standby LSPs. For example, when an LSP is in standby, BFD hello messages can be sent at smaller frequency to reduce line-card CPU usage. However, when a standby LSP becomes active (for example, due to protection switching), nominal BFD parameters are used for that LSPs (for example, to run BFD hello messages at higher frequency).

MPLS-TP Links and Physical Interfaces

MPLS-TP link IDs may be assigned to physical interfaces only. Bundled interfaces and virtual interfaces are not supported for MPLS-TP link IDs.

The MPLS-TP link is used to create a level of indirection between the MPLS-TP tunnel and midpoint LSP configuration and the physical interface. The MPLS-TP **link-id** command is used to associate an MPLS-TP link ID with a physical interface and next-hop node address.

Multiple tunnels and LSPs may then refer to the MPLS-TP link to indicate they are traversing that interface. You can move the MPLS-TP link from one interface to another without reconfiguring all the MPLS-TP tunnels and LSPs that refer to the link.

Link IDs must be unique on the router or node. For more information, see the *Configuring MPLS-TP Links and Physical Interfaces* section.

Tunnel LSPs

Tunnel LSPs, whether endpoint or midpoint, use the same identifying information. However, it is entered differently.

- A midpoint consists of a forward LSP and a reverse LSP. A MPLS-TP LSP mid point is identified by its name, and forward LSP, reverse LSP, or both are configured under a submode.
- At the midpoint, determining which end is source and which is destination is arbitrary. That is, if you are configuring a tunnel between your router and a coworker's router, then your router is the source. However, your coworker considers his or her router to be the source. At the midpoint, either router could be considered the source. At the midpoint, the forward direction is from source to destination, and the reverse direction is from destination to source. For more information, see the *Configuring MPLS-TP LSPs at Midpoints* section.
- At the midpoint, the LSP number does not assume default values, and hence must be explicitly configured.
- At the endpoint, the local information (source) either comes from the global node ID and global ID, or from locally configured information using the **source** command after you enter the **interface tunnel-tp** *number* command, where number is the local or source tunnel-number.
- At the endpoint, the remote information (destination) is configured using the **destination** command after you enter the **interface tunnel-tp** *number* command. The **destination** command includes the destination node ID, optionally the global ID, and optionally the destination tunnel number. If you do not specify the destination tunnel number, the source tunnel number is used.

MPLS-TP IP-less support

Generally, MPLS-TP functionality can be deployed with or without an IP address. However, the main motivation for the IP-less model is this: an LSR can be inserted into an MPLS-TP network without changing the configurations on adjacent LSRs. In the past Cisco IOS-XR MPLS-TP release, if an interface does not have a valid IP address, BFD packets cannot be transmitted over that link, and hence MPLS-TP LSP cannot be brought up on that link. In this release, the IP-less TP link operates only in a **point-to-point** mode.

This feature, therefore, makes the need for an IP address on a TP link optional. You may deploy LSRs running Cisco IOS-XR in MPLS-TP networks with or without an IP address. With such extra flexibility, LSRs running Cisco IOS-XR can be easily deployed not only with LSRs running IOS, but with LSRs from other vendors too.

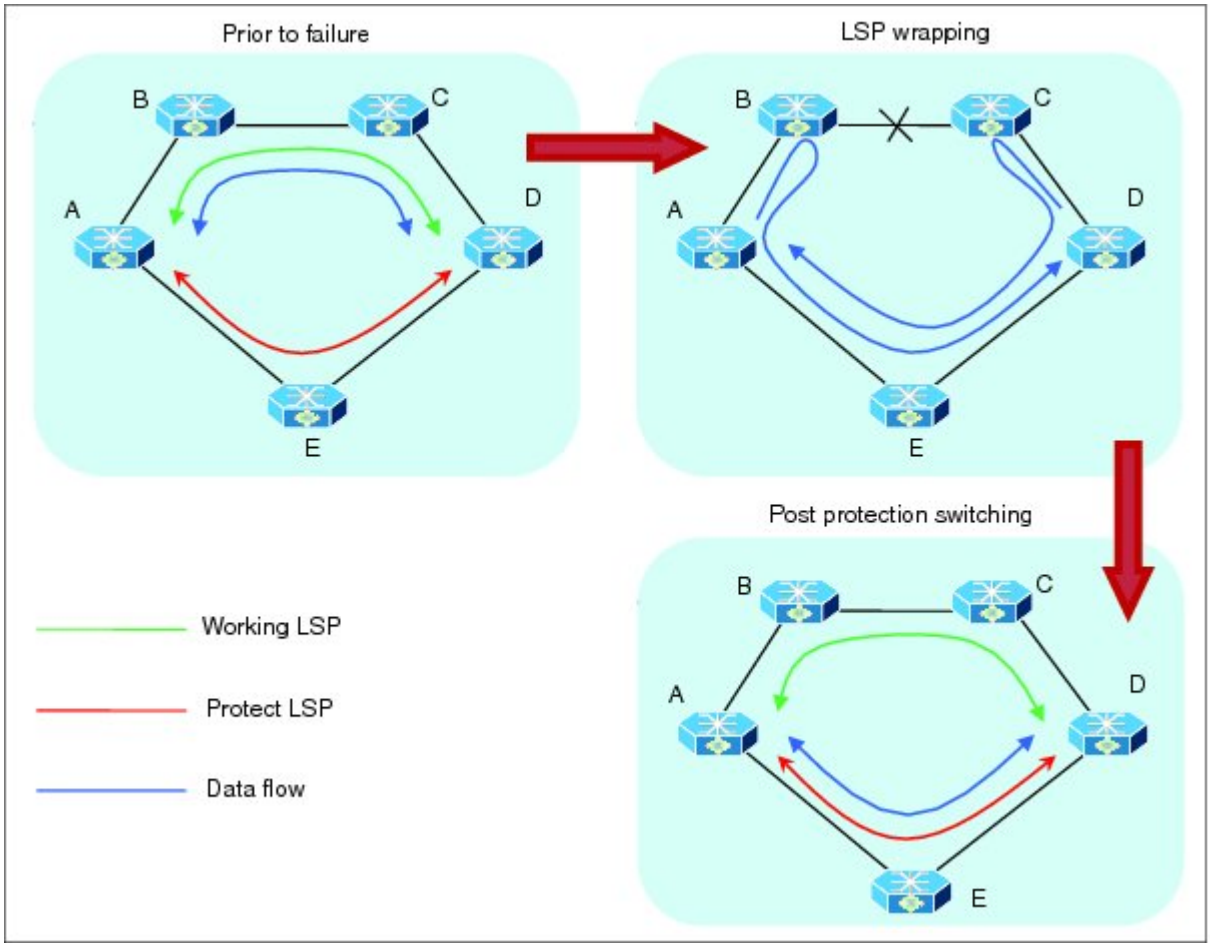
MPLS-TP LSP Wrapping

In the MPLS-TP LSP Wrapping protection scheme, a protected MPLS-TP tunnel is associated with a working LSP and protect LSP. This helps to prevent traffic loss as soon as a mid-point LSR detects a failure at physical layer rather than waiting for BFD to time-out. Also, a delay in activating protection switch due to mid-point failure does not further increase the traffic loss.

MPLS-TP LSP wrapping has to enabled only on the MID node. MPLS-TP LSP wrapping helps in detecting mid-link failure scenarios; other failures and failures on end node is detected by BFD timeout and TP-OAM message.

As shown in the figure below, when an LSR (e.g., Router B) detects a failure, it forwards the incoming traffic over an impacted LSP onto the reverse LSP, if it exists. The traffic re-directed into the reverse LSP is loopback traffic. Looping back traffic is carried out by the forwarding engine without control plane's involvement. The label stack of a loopback packet will be modified such that the source of the traffic identifies the packet.

Figure 39: MPLS-TP LSP Wrapping Mechanism



When the forwarding engine at an end-point recognizes a packet from loopback traffic, it sforwards the packet on protect LSP. As BFD packets over impacted LSPs are also looped-back, the end-point will drop such BFD packets so that BFD sessions over the impacted LSPs is timed-out and protection switching is activated. Optionally, when an end-point receives the first looped-back packet, it activates protection switching.

A working LSP remains wrapped until protection switching is activated. Once activated, protect LSP will carry traffic as usual. When failure is removed and BFD session comes back up resulting in activation of working LSP.

How to Implement MPLS Transport Profile

MPLS Transport Profile (MPLS-TP) supported by IETF enables the migration of transport networks to a packet-based network that efficiently scale to support packet services in a simple and cost effective way.

These procedures are used to implement MPLS-TP:

Configuring the Node ID and Global ID

Perform this task to configure node ID and global ID on the router.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **tp**
4. **node-id** *node-id*
5. **global-id** *num*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS TE configuration mode.
Step 3	**tp** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# mpls tp`	Enters MPLS transport profile (TP) configuration mode. You can configure MPLS TP specific parameters for the router from this mode.
Step 4	**node-id** *node-id* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tp)# node-id 10.0.0.1`	Specifies the default MPLS TP node ID, which is used as the default source node ID for all MPLS TP tunnels configured on the router. **Note** The node ID is a 32-bit number represented in IPv4 address format, and can be optionally assigned to each node.
Step 5	**global-id** *num* **Example:**	Specifies the default global ID used for all endpoints and midpoints. This command makes the node ID globally

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-mpls-te-tp)# global-id 10`	unique in a multi-provider tunnel. Otherwise, the node ID is only locally meaningful. **Note** The global ID is a 32-bit number, and can be assigned to each node.
Step 6	**commit**	

Configuring Pseudowire OAM Attributes

Perform this task to configure pseudowire OAM attributes.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **pw-oam refresh transmit** *value*
4. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters L2VPN configuration mode.
Step 3	**pw-oam refresh transmit** *value* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn)# pw-oam refresh transmit 20`	Specifies the OAM timeout refresh intervals.
Step 4	**commit**	

Configuring the Pseudowire Class

When you create the pseudowire class, you specify the parameters of the pseudowire, such as the use of the control word and preferred path.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **pw-class** *name*
4. **encapsulation mpls**
5. **preferred-path interface tunnel-tp** *tunnel-number*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**l2vpn** **Example:** `RP/0/RSP0/CPU0:router(config)# l2vpn`	Enters L2VPN configuration mode.
Step 3	**pw-class** *name* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn)# pw-class foo`	Creates a pseudowire OAM class named foo and enters pseudowire OAM class configuration mode.
Step 4	**encapsulation mpls** **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-pwc)# encapsulation mpls`	Sets pseudowire encapsulation to MPLS.
Step 5	**preferred-path interface tunnel-tp** *tunnel-number* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-pwc-mpls)# preferred-path interface tunnel-tp 10`	Specifies TP tunnel interface 10 for the preferred-path.
Step 6	**commit**	

Configuring the Pseudowire

Perform this task to configure the pseudowire.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*

3. **pseudowire-class** *class-name*
4. **encapsulation mpls**
5. **preferred-path interface tunnel-tp** *tunnel-number*
6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-tp 20`	Enters MPLS transport protocol tunnel interface configuration mode.
Step 3	**pseudowire-class** *class-name* **Example:** `RP/0/RSP0/CPU0:router(config-if)# pseudowire-class foo`	Creates a pseudowire class and enters pseudowire class configuration mode.
Step 4	**encapsulation mpls** **Example:** `RP/0/RSP0/CPU0:router# encapsulation mpls`	Specifies the encapsulation type.
Step 5	**preferred-path interface tunnel-tp** *tunnel-number* **Example:** `RP/0/RSP0/CPU0:router# preferred-path interface tunnel-tp 10`	Specifies TP tunnel interface 10 for the preferred-path. **Note** When a PW class with tunnel-tp interface as a preferred path is defined, this specified class can be associated with any PW.
Step 6	**commit**	

Configuring the MPLS TP Tunnel

On the endpoint routers, create an MPLS TP tunnel and configure its parameters.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-tp** *number*
3. **description** *tunnel-desc*
4. **bandwidth** *num*

5. **source** *source node-ID*
6. **destination** *destination node-ID* [**global-id** *destination global ID*] **tunnel-id** *destination tunnel ID*]
7. **working-lsp**
8. **in-label** *num*
9. **out-label** *mpls label* **out-link** *link ID*
10. **lsp-number** *value*
11. **exit**
12. **protect-lsp**
13. **in-label** *num*
14. **out-label** *mpls label* **out-link** *link ID*
15. **lsp-number** *value*
16. exit
17. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**interface tunnel-tp** *number* **Example:** `RP/0/RSP0/CPU0:router(config)# interface tunnel-tp 10`	Enters tunnel tp interface configuration mode. The range is from 0 to 65535.
Step 3	**description** *tunnel-desc* **Example:** `RP/0/RSP0/CPU0:router(config-if)# description head-end tunnel`	Specifies a tunnel tp description.
Step 4	**bandwidth** *num* **Example:** `RP/0/RSP0/CPU0:router(config-if)# tp bandwidth 1000`	Specifies the tunnel bandwidth in kbps. The range is from 0 to 4294967295.
Step 5	**source** *source node-ID* **Example:** `RP/0/RSP0/CPU0:router(config-if)# source 10.0.0.1`	Specifies the source node of the tunnel.
Step 6	**destination** *destination node-ID* [**global-id** *destination global ID*] **tunnel-id** *destination tunnel ID*] **Example:**	Specifies the destination node of the tunnel.

	Command or Action	Purpose
	`RP/0/RSP0/CPU0:router(config-if)# destination 10.0.0.1 global-id 10 tunnel-id 2`	
Step 7	**working-lsp** **Example:** `RP/0/RSP0/CPU0:router(config-if)# working-lsp`	Specifies a working LSP, also known as the primary LSP. This LSP is used to route traffic.
Step 8	**in-label** *num* **Example:** `RP/0/RSP0/CPU0:router(config-if-work)# in-label 111`	Specifies the in-label.
Step 9	**out-label** *mpls label* **out-link** *link ID* **Example:** `RP/0/RSP0/CPU0:router(config-if-work)# out-label 111 out-link 10`	Specifies the out-label.
Step 10	**lsp-number** *value* **Example:** `RP/0/RSP0/CPU0:router(config-if-work)# lsp-number 10`	Specifies the LSP ID of the working LSP.
Step 11	**exit** **Example:** `RP/0/RSP0/CPU0:router(config-if-work)# exit`	Exits from working LSP interface configuration mode.
Step 12	**protect-lsp** **Example:** `RP/0/RSP0/CPU0:router(config-if)# protect-lsp`	Specifies a backup for a working LSP. If the working LSP fails, traffic is switched to the protect LSP until the working LSP is restored, at which time traffic forwarding reverts back to the working LSP.
Step 13	**in-label** *num* **Example:** `RP/0/RSP0/CPU0:router(config-if-protect)# in-label 113`	Specifies the in-label.
Step 14	**out-label** *mpls label* **out-link** *link ID* **Example:** `RP/0/RSP0/CPU0:router(config-if-protect)# out-label 112 out-link 2`	Specifies the out-label and out-link.

	Command or Action	Purpose
Step 15	**lsp-number** *value* **Example:** `RP/0/RSP0/CPU0:router(config-if-protect)# lsp-number 10`	Specifies the LSP ID of the protect LSP.
Step 16	exit **Example:** `RP/0/RSP0/CPU0:router(config-if-protect)# exit`	Exits from protect LSP interface configuration mode.
Step 17	**commit**	

Configuring MPLS-TP LSPs at Midpoint

Perform this task to configure the MPLS-TP LSPs at the midpoint router.

Note When configuring the LSPs at the midpoint routers, make sure that the configuration does not reflect traffic back to the originating node.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **tp mid** *name*
4. **tunnel-name** *name*
5. **lsp-number** *value*
6. **source** *node -ID* **tunnel-id** *number*
7. **destination** *node -ID* **tunnel-id** *number*
8. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS TE configuration mode.

	Command or Action	Purpose
Step 3	**tp mid** *name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# tp mid foo`	Specifies the MPLS-TP tunnel mid-point identifier.
Step 4	**tunnel-name** *name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tp-mid)# tunnel-name midtunnel`	Specifies the name of the tunnel whose mid point is being configured.
Step 5	**lsp-number** *value* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tp-mid)# lsp-number 10`	Specifies the LSP ID.
Step 6	**source** *node -ID* **tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tp-mid-fwd)# source 10.0.0.1 tunnel-id 12`	Specifies the source node ID and tunnel ID.
Step 7	**destination** *node -ID* **tunnel-id** *number* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tp-mid-rev)# source 10.0.0.2 tunnel-id 12`	Specifies the destination node ID and tunnel ID.
Step 8	**commit**	

Configuring MPLS-TP Links and Physical Interfaces

MPLS-TP link IDs may be assigned to physical interfaces only.

Note Bundled interfaces and virtual interfaces are not supported for MPLS-TP link IDs.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **interface** *type interface-path-id*
4. **link-id** *value* **next-hop** *address*
5. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# mpls traffic-eng`	Enters MPLS TE configuration mode.
Step 3	**interface** *type interface-path-id* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# interface POS 0/6/0/0`	Configures an interface type and path ID to be associated with a MPLS TE mode.
Step 4	**link-id** *value* **next-hop** *address* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-if)# link-id 22 next-hop 10.1.1.2`	Configures an interface type and path ID to be associated with a MPLS TE mode. **Note** You must provide the next-hop IP address. **Note** You can define a link ID once. If you attempt to use the same MPLS-TP link ID with different interface or next-hop address, the configuration gets rejected. You have to remove the existing link ID configuration before using the same link ID with a different interface or next-hop address.
Step 5	**commit**	

Configuring MPLS-TP LSP Wrapping

Perform this task to configure the MPLS-TP LSP wrapping.

Note When configuring the LSPs at the midpoint routers, make sure that the configuration does not reflect traffic back to the originating node.

SUMMARY STEPS

1. **configure**
2. **mpls traffic-eng**
3. **tp mid** *name*
4. **tunnel-name** *name*
5. **fast-protect**

6. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**mpls traffic-eng** **Example:** `RP/0/RSP0/CPU0:router(config)# mpls traffic-eng`	Enters MPLS TE configuration mode.
Step 3	**tp mid** *name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te)# tp mid midpt1`	Specifies the MPLS-TP tunnel mid-point identifier.
Step 4	**tunnel-name** *name* **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tp-mid)# tunnel-name midtunnel`	(Optional) Specifies the name of the tunnel whose mid point is being configured.
Step 5	**fast-protect** **Example:** `RP/0/RSP0/CPU0:router(config-mpls-te-tp-mid)# fast-protect`	Enables MPLS-TP LSP wrapping.
Step 6	**commit**	