Junos® OS

GMPLS Configuration Guide

Release
12.1

Published: 2012-03-13

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS GMPLS Configuration Guide
12.1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```


3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   [edit system scripts]
   user@host# **load merge relative /var/tmp/ex-script-snippet.conf**
   load complete

For more information about the **load** command, see the *Junos OS CLI User Guide*.

Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>;
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (*string1* | *string2* | *string3*)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

Indention and braces ({ })	Identify a level in the configuration hierarchy.	[edit]
		routing-options {
		static {
		route default {
		nexthop *address*;
		retain;
		}
		}
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@juniper.net**, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html .

PART 1

Overview

CHAPTER 1

Introduction to GMPLS

Introduction to GMPLS

Traditional MPLS is designed to carry Layer 3 IP traffic using established IP-based paths and associating these paths with arbitrarily assigned labels. These labels can be configured explicitly by a network administrator, or can be dynamically assigned by means of a protocol such as LDP or RSVP.

GMPLS generalizes MPLS in that it defines labels for switching varying types of Layer 1, Layer 2, or Layer 3 traffic. GMPLS nodes can have links with one or more of the following switching capabilities:

- Fiber-switched capable (FSC)
- Lambda-switched capable (LSC)
- Time-division multiplexing (TDM) switched-capable (TSC)
- Packet-switched capable (PSC)

Label-switched paths (LSPs) must start and end on links with the same switching capability. For example, routers can establish packet-switched LSPs with other routers. The LSPs might be carried over a TDM-switched LSP between SONET add/drop multiplexers (ADMs), which in turn might be carried over a lambda-switched LSP.

The result of this extension of the MPLS protocol is an expansion in the number of devices that can participate in label switching. Lower-layer devices, such as OXCs and SONET ADMs, can now participate in GMPLS signaling and set up paths to transfer data. A router can participate in signaling optical paths across a transport network.

Two service models determine the visibility that a client node (a router, for example) has into the optical core or transport network. The first is through a user-to-network interface

(UNI), which is often referred to as the overlay model. The second is known as the peer model. Juniper Networks supports both models.

NOTE: There is not necessarily a one-to-one correspondence between a physical interface and a GMPLS interface. If a GMPLS connection uses a nonchannelized physical connector, the GMPLS label can use the physical port ID. However, the label for channelized interfaces often is based on a channel or time slot. Consequently, it is best to refer to GMPLS labels as identifiers for a resource on a traffic engineering link.

To establish LSPs, GMPLS uses the following mechanisms:

- An out-of-band control channel and a data channel—RSVP messages for LSP setup are sent over an out-of-band control network. Once the LSP setup is complete and the path is provisioned, the data channel is up and can be used to carry traffic. The Link Management Protocol (LMP) is used to define and manage the data channels between a pair of nodes. You can optionally use LMP to establish and maintain LMP control channels between peers running the same Junos OS Release.
- RSVP-TE extensions for GMPLS—RSVP-TE is already designed to signal the setup of packet LSPs. This has been extended for GMPLS to be able to request path setup for various kinds of LSPs (nonpacket) and request labels like wavelengths, time slots, and fibers as label objects.
- Bidirectional LSPs—Data can travel both ways between GMPLS devices over a single path, so nonpacket LSPs are signaled to be bidirectional.

GMPLS Operation

The basic functionality of GMPLS requires close interaction between RSVP and LMP. It works in the following sequence:

1. LMP notifies RSVP of the new entities:
   - Traffic engineering link (forwarding adjacency)
   - Resources available for the traffic engineering link
   - Control peer
2. GMPLS extracts the LSP attributes from the configuration and requests RSVP to signal one or more specific paths, which are specified by the traffic engineering link addresses.
3. RSVP determines the local traffic engineering link, corresponding control adjacency and active control channel, and transmission parameters (such as IP destination). It requests that LMP allocate a resource from the traffic engineering link with the specified attributes. If LMP finds a resource matching the attributes, label allocation succeeds. RSVP sends a PathMsg hop by hop until it reaches the target router.

4. When the target router receives the PathMsg, RSVP again requests that LMP allocate a resource based on the signaled parameters. If label allocation succeeds, the router sends back a ResvMsg.
5. If the signaling is successful, a bidirectional optical path is provisioned.

GMPLS and OSPF

You can configure OSPF for GMPLS. OSPF is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). OSPF uses link-state information to make routing decisions.

GMPLS and CSPF

GMPLS introduces extra constraints for computing paths for GMPLS LSPs that use CSPF. These additional constraints affect the following link attributes:

- Signal type (minimum LSP bandwidth)
- Encoding type
- Switching type

These new constraints are populated in the traffic engineering database with the exchange of an interface-switching capability descriptor type, length, value (TLV) through an IGP.

The ignored constraints that are exchanged through the interface switching capability descriptor include:

- Maximum LSP bandwidth
- Maximum transmission unit (MTU)

The CSPF path computation is the same as in non-GMPLS environments, except that the links are also limited by GMPLS constraints.

Each link can have multiple interface-switching capability descriptors. All the descriptors are checked before a link is rejected.

The constraints are checked in the following order:

1. The signal type configured for the GMPLS LSP signifies the amount of bandwidth requested. If the desired bandwidth is less than the minimum LSP bandwidth, the interface-switching descriptor is rejected.
2. The encoding type of the link for the ingress and the egress interfaces should match. The encoding type is selected and stored at the ingress node after all the constraints are satisfied by the link and is used to select the link on the egress node.
3. The switching type of the links of the intermediate switches should match that of the GMPLS LSP specified in the configuration.

GMPLS Features

The Junos OS includes the following GMPLS functionality:

- An out-of-band control plane makes it possible to signal LSP path setup.
- RSVP-TE extensions support additional objects beyond Layer 3 packets, such as ports, time slots, and wavelengths.
- The LMP protocol creates and maintains a database of traffic engineering links and peer information. Only the static version of this protocol is supported in the Junos OS. You can optionally configure LMP to establish and maintain LMP control channels between peers running the same Junos OS Release.
- Bidirectional LSPs are required between devices.
- Several GMPLS label types that are defined in RFC 3471, *Generalized MPLS—Signaling Functional Description*, such as MPLS, Generalized, SONET/SDH, Suggested, and Upstream, are supported. Generalized labels do not contain a type field, because the nodes should know from the context of their connection what type of label to expect.
- Traffic parameters facilitate GMPLS bandwidth encoding and SONET/SDH formatting.
- Other supported attributes include interface identification and errored interface identification, user-to-network (UNI)-style signaling, and secondary LSP paths.

CHAPTER 2

Hierarchy of RSVP LSPs Configuration Guidelines Overview

Hierarchy of RSVP LSPs Overview

This chapter provides overview information and configuration instructions for hierarchies of RSVP label-switched paths (LSPs), which enable you to tunnel multiple RSVP LSPs over a single RSVP LSP.

The following sections provide an overview of how a hierarchy of RSVP LSPs functions:

- Hierarchy of RSVP LSPs on page 7
- Advertising the Forwarding Adjacency with OSPF on page 8

Hierarchy of RSVP LSPs

Forwarding adjacencies are configured and managed as point-to-point traffic engineering links by including statements at the **[edit protocols link-management]** hierarchy level. For the forwarding adjacency to function properly, you also need to make RSVP aware of the forwarding adjacency by configuring the corresponding peer interface at the **[edit protocols rsvp]** hierarchy level.

Although forwarding adjacency LSPs are configured and managed as traffic engineering links on the local router, it is not necessary to advertise these traffic engineering links to other routers in the network. However, if you want to automatically forward MPLS traffic over the forwarding adjacency or want other routers to compute paths over the forwarding adjacency, you must configure OSPF to advertise the forwarding adjacency to the other routers in the network and add the forwarding adjacency to the traffic engineering database. OSPF is the only supported interior gateway protocol (IGP).

Advertising the Forwarding Adjacency with OSPF

Once a forwarding adjacency LSP and the corresponding traffic engineering link you have configured, you can configure OSPF to advertise the forwarding adjacency. Unlike regular traffic engineering links, OSPF hellos are not exchanged between the forwarding adjacency LSP endpoints and therefore no routing adjacency is created between the forwarding adjacency endpoints. If you issue a **show ospf neighbor** command on an ingress forwarding adjacency, the command displays the egress router of the forwarding adjacency LSP as a neighbor. However, no real OSPF adjacency is established (no OSPF hellos are exchanged) between the ingress and egress routers. For display purposes only, OSPF creates a pseudo-neighbor corresponding to the peer.

You can configure forwarding adjacencies over existing MPLS networks. A forwarding adjacency LSP is signaled as a regular MPLS LSP without generalized MPLS (GMPLS) extensions. When the forwarding adjacency LSP is advertised as a traffic engineering link in OSPF, the corresponding traffic engineering link in OSPF is also advertised as a regular MPLS traffic engineering link without GMPLS extensions.

PART 2

Configuration

CHAPTER 3

GMPLS Configuration Guidelines

LMP Configuration Overview

You need to configure the Link Management Protocol (LMP) to define the data channel connection and the control channel connection between devices. Include the following statements at the **[edit protocols link-management]** hierarchy level:

```
[edit protocols link-management]
peer peer-name {
  address address;
  control-channel control-channel-name;
  lmp-control-channel control-channel-interface {
    remote-address ip-address;
  }
  lmp-protocol {
    hello-dead-interval milliseconds;
    hello-interval milliseconds;
    retransmission-interval milliseconds;
    retry-limit number;
    passive;
  }
  te-link te-link-name;
}
te-link te-link-name {
  disable;
  interface interface-name {
    disable;
    local-address ip-address;
    remote-address ip-address;
    remote-id id-number;
```

```
    }
    label-switched-path lsp-name;
    local-address ip-address;
    remote-address ip-address;
    remote-id id-number;
  }
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
```

NOTE: Although you can include GMPLS configuration statements at the **[edit logical-systems *logical-system-name*]** hierarchy level, GMPLS is not supported on logical systems.

For information about configuring LMP, see the following sections:

- Configuring LMP Traffic Engineering Links on page 12
- Configuring LMP Peers on page 14
- Configuring RSVP and OSPF for LMP Peer Interfaces on page 19
- Configuring MPLS Paths for GMPLS on page 20
- Tracing LMP Traffic on page 21

Configuring LMP Traffic Engineering Links

An LMP traffic engineering link acts as a data channel connection between GMPLS devices.

To configure a traffic engineering link, include the **te-link** statement at the **[edit protocols link-management]** hierarchy level:

```
  [edit protocols link-management]
  te-link te-link-name {
    disable;
    interface interface-name {
      local-address ip-address;
      remote-address ip-address;
      remote-id id-number;
    }
    label-switched-path lsp-name;
    local-address ip-address;
    remote-address ip-address;
    remote-id id-number;
  }
```


Complete the procedures in the following sections to configure an LMP traffic engineering link:

- Configuring the Local IP Address for Traffic Engineering Links on page 13
- Configuring the Remote IP Address for Traffic Engineering Links on page 13
- Configuring the Remote ID for Traffic Engineering Links on page 14

When you configure a traffic engineering link that contains interfaces for an LMP peer, you must also configure a control channel. However, no control channel is required for a traffic engineering link that contains an LSP. For information about configuring control channels, see "Configuring LMP Peers" on page 14.

Configuring the Local IP Address for Traffic Engineering Links

Use the **local-address** statement to configure the local IP address associated with the traffic engineering link.

We recommend that you configure an IP address subnet for your traffic engineering link addresses that is different from the subnet configured for your physical interfaces. This configuration enables you to identify which addresses are physical and which addresses belong to the traffic engineering link.

To configure the local IP address for the traffic engineering link, include the **local-address** statement:

```
te-link te-link-name {
  interface interface-name {
    local-address ip-address;
  }
  local-address ip-address;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Remote IP Address for Traffic Engineering Links

You need to specify the address of the remote end of the data channel for each traffic engineering link. Use the **remote-address** statement to configure the remote IP address.

We recommend that you configure an IP address subnet for your traffic engineering link addresses that is different from the subnet configured for your physical interfaces. This enables you to identify which addresses are physical and which addresses belong to the traffic engineering link.

To configure the remote IP address for the traffic engineering link, include the **remote-address** statement:

```
te-link te-link-name {
  interface interface-name {
    remote-address ip-address;
  }
  remote-address ip-address;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Remote ID for Traffic Engineering Links

The local ID for the traffic engineering link is automatically assigned by LMP. The port identifier and labels for the interfaces (resources) in the traffic engineering link are also assigned automatically. However, you need to explicitly configure the remote ID for the traffic engineering link and the remote ID traffic engineering link interface. The remote ID for the interface must be based on the post-ID assignment of the peer node. The remote IDs are needed for static mapping of remote labels to local labels.

Before you can obtain the remote IDs for the traffic engineering link and traffic engineering link interface on the peer node, you must first configure the LMP peer, as described in "Configuring LMP Peers" on page 14. Once you have configured the LMP peer, you can obtain the traffic engineering link local ID and interface local ID by issuing the **show link-management te-link** command. Once you have these IDs, you can configure them as the remote IDs on the peer node.

To configure the remote ID for a traffic engineering link and for the traffic engineering link interface, include the **remote-id** statement:

```
te-link te-link-name {
  interface interface-name {
    remote-id id-number;
  }
  remote-id id-number;
}
```

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring LMP Peers

You need to configure network peers for GMPLS. A peer is a network device that your router communicates with when setting up the control and data channels. The peer is often an optical cross-connect (OXC).

To configure an LMP peer name, include the **peer** statement at the **[edit protocols link-management]** hierarchy level:

```
peer peer-name {
  address ip-address;
  control-channel control-channel-interface;
  lmp-control-channel control-channel-interface {
    remote-address ip-address;
  }
  lmp-protocol {
    hello-dead-interval milliseconds;
    hello-interval milliseconds;
    retransmission-interval milliseconds;
    retry-limit number;
    passive;
  }
```



```
    te-link te-link-name;
}
```

The following sections describe how to configure an LMP peer:

Configuring the ID for LMP Peers

To configure the LMP peer ID, include the **address** statement at the **[edit protocols link-management peer *peer-name*]** hierarchy level. The default value for the LMP peer ID is the loopback address.

```
[edit protocols link-management peer peer-name]
address ip-address;
```

Configuring the Interface for Control Channels Between LMP Peers

You must configure one or more control channels between the LMP peers. The control channels must travel across either a point-to-point link or a tunnel.

To configure the interface for the control channel, include the **control-channel** statement at the **[edit protocols link-management peer *peer-name*]** hierarchy level:

```
[edit protocols link-management peer peer-name]
control-channel [ interface-names ];
```

You can configure a generic routing encapsulation (GRE) interface for the control channel. This type of interface does not require a Tunnel PIC.

NOTE: You can configure GRE interfaces only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. For more information, see the *Junos OS Network Interfaces Configuration Guide*.

Configuring the LMP Control Channel Interface for the Peer

In an environment that uses LMP to establish and maintain an LMP control channel between peers, you can configure a number of attributes associated with LMP. To configure the interface to be associated with the LMP control channel for the peer, include the **lmp-control-channel** statement:

lmp-control-channel *control-channel-interface*;

You can configure this statement at the following hierarchy levels:

- **[edit protocols link-management peer *peer-name*]**
- **[edit logical-systems *logical-system-name* protocols link-management peer *peer-name*]**

You can configure a GRE interface for the LMP control channel. This type of interface does not require a Tunnel PIC.

NOTE: You can configure GRE interfaces only for GMPLS control channels. GRE interfaces are not supported or configurable for other applications. For more information, see the *Junos OS Network Interfaces Configuration Guide*.

When this LMP control channel interface comes up, the peers use LMP to negotiate channel parameters and configure the control channel.

The local peer repeatedly sends a Config message to the remote peer. The Config message contains the local control channel ID, the local peer's node ID, a message ID, and a CONFIG object that includes hello message attributes (the hello interval and the hello dead interval).

The channel is activated when the remote peer responds with a ConfigAck message. The remote peer does so only when its own configured hello interval and hello dead interval match the values in the received Config message or the default values. If these values do not match, the remote peer responds with a ConfigNack message. The local peer logs this event and resends the Config message until the message retry limit is reached. When the message retry limit is reached, the local peer logs that event and restarts the configuration process.

Configuring the Remote IP Address for LMP Control Channels

You need to specify the address of the remote end of the LMP control channel.

To configure the remote IP address for the LMP control channel, include the **remote-address** statement:

remote-address *address*;

You can configure this statement at the following hierarchy levels:

- **[edit protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*]**
- **[edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*]**

Configuring Hello Message Intervals for LMP Control Channels

Hello messages are exchanged between LMP peers to maintain the control channel after LMP has activated the control channel. The LMP control channel is considered to be up only when the hello negotiation is successful. Successful negotiation consists of the local peer sending a hello message to the remote peer and receiving a hello message in response.

The LMP peers continue to exchange hello messages after the LMP control channel is up in order to maintain the channel.

The hello interval specifies the interval between periodic hello messages. The hello dead interval specifies how long the local peer waits for a hello response before it declares the LMP control channel to be down. When the channel goes down, the local peer restarts the LMP control channel negotiation and configuration process.

You can specify a hello interval from 150 through 300,000 milliseconds. The default hello interval is 150 milliseconds.

You can specify a hello dead interval from 500 through 300,000 milliseconds. The default hello dead interval is 500 milliseconds.

To configure the attributes for hello messages exchanged between LMP peers, include the **hello-interval** and **hello-dead-interval** statements:

hello-dead-interval *milliseconds*;
hello-interval *milliseconds*;

You can configure these statements at the following hierarchy levels:

- **[edit protocols link-management peer *peer-name* lmp-protocol]**
- **[edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol]**

When an LMP control channel comes up after a successful exchange of hello messages between LMP peers, LMP uses link property correlation to verify the traffic engineering and data link information on both sides of a link. To do so, the local peer sends a LinkSummary message for each traffic engineering link governed by the LMP control channel. The LinkSummary message contains information that characterizes the traffic engineering link and each data link in the traffic engineering link.

The local peer continues sending a LinkSummary message for each link until the remote peer responds with a LinkSummaryAck message or until the message retry limit is reached. When the message retry limit is reached, the local peer logs that event and restarts the link property correlation process.

When the remote peer receives a LinkSummary message, it examines its own link information. If this information agrees with that in the LinkSummary message, the remote peer responds with a LinkSummaryAck message. If the information is different, the remote peer responds with a LinkSummaryNack message.

Controlling Message Exchange for LMP Control Channels

You can configure message attributes that control the exchange of LMP Config and LinkSummary messages. The retransmission interval specifies the interval between resubmitted LMP messages. The retry limit specifies how many times LMP sends a message before restarting the process.

You can specify a retransmission interval from 500 through 300,000 milliseconds. The default retransmission interval is 500 milliseconds.

You can specify a retry limit from 3 through 1000 attempts. The default number of retry attempts is three.

To configure attributes governing the exchange of LMP messages between peers, include the **retransmission-interval** and **retry-limit** statements:

```
retransmission-interval milliseconds;
retry-limit number;
```

You can configure these statements at the following hierarchy levels:

- **[edit protocols link-management peer *peer-name* lmp-protocol]**
- **[edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol]**

Preventing the Local Peer from Initiating LMP Negotiation

You can specify that the local peer does not initiate LMP negotiation. Instead, the local peer waits for the remote peer to configure the LMP control channel.

To configure the local peer to wait for the remote peer to configure the LMP control channel, include the **passive** statement:

```
passive;
```

You can configure this statement at the following hierarchy levels:

- **[edit protocols link-management peer *peer-name* lmp-protocol]**
- **[edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol]**

Associating Traffic Engineering Links with LMP Peers

To specify the name of a traffic engineering link to be associated with this peer, include the **te-link** statement at the **[edit protocols link-management peer *peer-name*]** hierarchy level:

```
[edit protocols link-management peer peer-name]
te-link te-link-name;
```

For information about how to configure a traffic engineering link, see "Configuring LMP Traffic Engineering Links" on page 12.

Disabling the Traffic Engineering Link for LMP Peers

To disable a specific traffic engineering link, include the **disable** statement:

```
disable;
```


You can configure this statement at the following hierarchy levels:

- **[edit protocols link-management te-link *te-link-name*]**
- **[edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*]**

Configuring RSVP and OSPF for LMP Peer Interfaces

After you have configured the LMP peers as described in "Configuring LMP Peers" on page 14, add the peer interfaces to RSVP and OSPF. The peer interface name must match the peer name configured in LMP. Once the peer interfaces are added to the protocols, the traffic engineering link local and remote addresses can be signaled and advertised to peers like any other interface enabled for RSVP and OSPF. These addresses act as virtual interfaces for GMPLS.

NOTE: When adding the virtual peer interfaces to RSVP and OSPF, do not configure the corresponding physical control channel interface in either protocol. If you include the **interface all** statement, you must disable RSVP and OSPF protocols manually on the control channel interface.

To configure peer interfaces in RSVP and OSPF, complete the procedures in the following sections:

- Configuring RSVP Signaling for LMP Peer Interfaces on page 19
- Configuring OSPF Routing for LMP Peer Interfaces on page 19
- Configuring the Hello Interval for LMP Peer Interfaces on page 20

Configuring RSVP Signaling for LMP Peer Interfaces

To configure RSVP signaling for LMP peers, configure the LMP peer interface by including the **peer-interface** statement at the **[edit protocols rsvp]** hierarchy level:

```
[edit protocols rsvp]
peer-interface peer-interface-name {
    (aggregate | no-aggregate);
    authentication-key key;
    disable;
    hello-interval seconds;
    (reliable | no-reliable);
}
```

The statements configured at the **[edit protocols rsvp peer-interface *peer-interface-name*]** hierarchy level have the same functionality as the statements configured at the **[edit protocols rsvp interface *interface-name*]** hierarchy level.

Configuring OSPF Routing for LMP Peer Interfaces

To configure OSPF routing for LMP peers, configure the name of the LMP peer by including the **peer-interface** statement at the **[edit protocols ospf area *area-number*]** hierarchy level:

```
[edit protocols ospf area area-number]
peer-interface peer-interface-name {
  dead-interval seconds;
  disable;
  hello-interval seconds;
  retransmit-interval seconds;
  transit-delay seconds;
}
```

For information about how to configure OSPF statements, see the *Junos OS Routing Protocols Configuration Guide*.

Configuring the Hello Interval for LMP Peer Interfaces

Hello packets are used to indicate to neighboring routers that the peer interface is still up and running. The hello interval must be the same for all routers on a shared logical IP network. You can specify a hello interval from 1 through 255 seconds. The default hello interval is normally 10 seconds. For nonbroadcast networks, the default hello interval is 120 seconds.

To specify how often the router sends hello packets out the peer interface, configure the **hello-interval** statement:

```
hello-interval seconds;
```

You can configure this statement at the following hierarchy levels:

- **[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]**
- **[edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*]**

Configuring MPLS Paths for GMPLS

As part of the configuration for GMPLS, you need to establish an MPLS path for each unique device connected through GMPLS. Configure the traffic engineering link remote address as the address at the **[edit protocols mpls path *path-name*]** hierarchy level. Constrained Shortest Path First (CSPF) is supported so you can choose either the **strict** or **loose** option with the address.

See "LMP Configuration Overview" on page 11 for information about how to obtain a traffic engineering link remote address.

To configure the MPLS path, include the **path** statement at the **[edit protocols mpls]** hierarchy level:

```
[edit protocols mpls]
path path-name {
  next-hop-address (strict | loose);
}
```

For information about how to configure MPLS paths, see Configuring the Ingress Router for MPLS-Signaled LSPs.

Tracing LMP Traffic

To trace LMP protocol traffic, include the **traceoptions** statement at the **[edit protocols link-management]** hierarchy level:

```
[edit protocols link-management]
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

Use the **file** statement to specify the name of the file that receives the output of the tracing operation. All files are placed in the directory **/var/log**.

The following trace flags display the operations associated with the sending and receiving of various LMP messages:

- **all**—Trace all available operations
- **hello-packets**—Trace hello packets on any LMP control channel
- **init**—Output from the initialization messages
- **packets**—Trace all packets other than hello packets on any LMP control channel
- **parse**—Operation of the parser
- **process**—Operation of the general configuration
- **route-socket**—Operation of route socket events
- **routing**—Operation of the routing protocols
- **server**—Server processing operations
- **show**—Servicing operations for **show** commands
- **state**—Trace state transitions of the LMP control channels and traffic engineering links

Each flag can carry one or more of the following flag modifiers:

- **detail**—Provide detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

Configuring MPLS LSPs for GMPLS

To enable the proper GMPLS switching parameters, configure the label-switched path (LSP) attributes that are appropriate for your network connection. The default value for **switching-type** is **psc-1**, which is also appropriate for standard MPLS.

To configure the LSP attributes, include the **lsp-attributes** statement at the **[edit protocols mpls label-switched-path *lsp-name*]** hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name]
```



```
lsp-attributes {
  encoding-type type;
  gpid gpid;
  signal-bandwidth type;
  switching-type type;
}
```

If you include the **no-cspf** statement in the label-switched path configuration, you must also configure primary and secondary paths, or the configuration cannot be committed.

The following sections describe how to configure each of the LSP attributes for a GMPLS LSP:

Configuring the Encoding Type

You need to specify the encoding type of the payload carried by the LSP. It can be any of the following:

- **ethernet**—Ethernet
- **packet**—Packet
- **pdh**—Plesiochronous digital hierarchy (PDH)
- **sonet-sdh**—SONET/SDH

The default value is **packet**.

To configure the encoding type, include the **encoding-type** statement at the **[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]** hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
encoding-type type;
```

Configuring the GPID

You need to specify the type of payload carried by the LSP. The payload is the type of packet underneath the MPLS label. The payload is specified by the generalized payload identifier (GPID).

You can specify the GPID with any of the following values:

- **hdlc**—High-Level Data Link Control (HDLC)
- **ethernet**—Ethernet
- **ipv4**—IP version 4 (default)

- **pos-scrambling-crc-16**—For interoperability with other vendors' equipment
- **pos-no-scrambling-crc-16**—For interoperability with other vendors' equipment
- **pos-scrambling-crc-32**—For interoperability with other vendors' equipment
- **pos-no-scrambling-crc-32**—For interoperability with other vendors' equipment
- **ppp**—Point-to-Point Protocol (PPP)

To configure the GPID, include the **gpid** statement at the **[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]** hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
gpid gpid;
```

Configuring the Signal Bandwidth Type

The signal bandwidth type is the encoding used for path computation and admission control. To configure the signal bandwidth type, include the **signal-bandwidth** statement at the **[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]** hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
signal-bandwidth type;
```

Configuring GMPLS Bidirectional LSPs

Because MPLS and GMPLS use the same configuration hierarchy for LSPs, it is helpful to know which LSP attributes control LSP functionality. Standard MPLS packet-switched LSPs are unidirectional, whereas GMPLS nonpacket LSPs are bidirectional.

If you use the default packet-switching type of **psc-1**, your LSP becomes unidirectional. To enable a GMPLS bidirectional LSP, you must select a non-packet-switching type option, such as **lambda**, **fiber**, or **ethernet**. Include the **switching-type** statement at the **[edit protocols mpls label-switched-path *lsp-name* lsp-attributes]** hierarchy level:

```
[edit protocols mpls label-switched-path lsp-name lsp-attributes]
switching-type (lambda | fiber | ethernet);
```

Allowing Nonpacket GMPLS LSPs to Establish Paths Through Routers Running the Junos OS

By setting the A-bit in the Admin Status object. you can enable nonpacket GMPLS LSPs to establish paths through routers that run Junos. When an ingress router sends an RSVP PATH message with the Admin Status A-bit set, an external device (not a router running the Junos OS) can either perform a Layer 1 path setup test or help bring up an optical cross-connect.

When set, the A-bit in the Admin Status object indicates the administrative down status for a GMPLS LSP. This feature is used specifically by nonpacket GMPLS LSPs. It does not affect control path setup or data forwarding for packet LSPs.

Junos does not distinguish between the control path setup and data path setup. Other nodes along the network path use RSVP PATH signaling using the A-bit in a meaningful way.

To configure the Admin Status object for a GMPLS LSP, include the **admin-down** statement:

```
admin-down;
```

You can include this statement at the following hierarchy levels:

- **[edit protocols mpls label-switched-path *lsp-name*]**
- **[edit logical-systems *logical-system-name* protocols mpls label-switched-path *lsp-name*]**

Gracefully Tearing Down GMPLS LSPs

You can gracefully tear down nonpacket GMPLS LSPs. An LSP that is torn down abruptly, a common process in a packet-switched network, can cause stability problems in nonpacket-switched networks. To maintain the stability of nonpacket-switched networks, it might be necessary to tear down LSPs gracefully.

The following sections describe how to tear down GMPLS LSPs gracefully:

- Temporarily Deleting GMPLS LSPs on page 24
- Permanently Deleting GMPLS LSPs on page 24
- Configuring the Graceful Deletion Timeout Interval on page 25

Temporarily Deleting GMPLS LSPs

You can gracefully tear down a GMPLS LSP using the **clear rsvp session gracefully** command.

This command gracefully tears down an RSVP session for a nonpacket LSP in two passes. In the first pass, the Admin Status object is signaled along the path to the endpoint of the LSP. During the second pass, the LSP is taken down. Using this command, the LSP is taken down temporarily. After the appropriate interval, the GMPLS LSP is resignaled and then reestablished.

The **clear rsvp session gracefully** command has the following properties:

- It only works on the ingress and egress routers of an RSVP session. If used on a transit router, it has the same behavior as the **clear rsvp session** command.
- It only works for nonpacket LSPs. If used with packet LSPs, it has the same behavior as the **clear rsvp session** command.

For more information, see the *Junos OS Routing Protocols and Policies Command Reference*.

Permanently Deleting GMPLS LSPs

When you disable an LSP in the configuration, the LSP is permanently deleted. By configuring the **disable** statement, you can disable a GMPLS LSP permanently. If the LSP being disabled is a nonpacket LSP, then the graceful LSP tear-down procedures that use the Admin Status object are used. If the LSP being disabled is a packet LSP, then the regular signaling procedures for LSP deletion are used.

To disable a GMPLS LSP, include the **disable** statement at any of the following hierarchy levels:

- **[edit protocols mpls label-switched-path *lsp-name*]**—Disable the LSP.
- **[edit protocols link-management** te-link ***te-link-name*]**—Disable a traffic engineering link.
- **[edit protocols link-management** te-link ***te-link-name*** interface ***interface-name*]**—Disable an interface used by a traffic engineering link.

Configuring the Graceful Deletion Timeout Interval

The router that initiates the graceful deletion procedure for an RSVP session waits for the graceful deletion timeout interval to ensure that all routers along the path (especially the ingress and egress routers) have prepared for the LSP to be taken down.

The ingress router initiates the graceful deletion procedure by sending the Admin Status object in the path message with the **D** bit set. The ingress router expects to receive an Resv message with the **D** bit set from the egress router. If the ingress router does not receive this message within the time specified by the graceful deletion timeout interval, it initiates a forced tear-down of the LSP by sending a PathTear message.

To configure the graceful deletion timeout interval, include the **graceful-deletion-timeout** statement at the **[edit protocols rsvp]** hierarchy level. You can configure a time between 1 through 300 seconds. The default value is 30 seconds.

```
graceful-deletion-timeout seconds;
```

You can configure this statement at the following hierarchy levels:

- **[edit protocols rsvp]**
- **[edit logical-systems *logical-system-name* protocols rsvp]**

You can use the **show rsvp version** command to determine the current value configured for the graceful deletion timeout.

CHAPTER 4

Hierarchy of RSVP LSPs Configuration Guidelines

Configuring a Hierarchy of RSVP LSPs

The following sections describe how to configure a hierarchy of RSVP LSPs:

Configuring an RSVP LSP on Ingress Routers

To configure a standard RSVP LSP on the ingress router to be used as the forwarding adjacency LSP, see LSP Configuration Overview. This LSP requires no special configuration to function as a forwarding adjacency LSP.

Configuring Forwarding Adjacencies

A forwarding adjacency is a type of GMPLS traffic engineering link. It requires that you configure local and remote addresses to identify the link. A forwarding adjacency is associated with a specific peer router. You could configure multiple forwarding adjacencies to the same peer router.

To configure a forwarding adjacency, you need to configure the **te-link** statement at the **[edit protocols link-management]** hierarchy level:

```
[edit protocols link-management]
te-link te-link-name {
  label-switched-path lsp-name;
  local-address ip-address;
  remote-address ip-address;
}
```

For more information on how to configure GMPLS traffic engineering links, see "Configuring LMP Traffic Engineering Links" on page 12.

NOTE: Do not configure the control channel for a forwarding adjacency peer router. Configuring a control channel causes the commit operation to fail.

The following sections describe how to configure the **te-link** statement for a forwarding adjacency:

Configuring the Local IP Address for Forwarding Adjacencies

To configure the local IP address for the forwarding adjacency, include the **local-address** statement:

local-address *ip-address*;

For a list of hierarchy levels at which you can include this statement, see the statement summary section for this statement.

Configuring the Remote IP Address for Forwarding Adjacencies

The address of the peer router is the node ID for the forwarding adjacency LSP egress node. You configure this node ID for the forwarding adjacency using the **remote-address** statement:

remote-address *ip-address*;

You can include this statement at the following hierarchy levels:

- **[edit protocols link-management** te-link ***te-link-name*****],**
- **[edit logical-systems *logical-system-name* protocols link-management** te-link ***te-link-name*****]**

Configuring the LSP for Forwarding Adjacencies

To configure a router to function as a forwarding adjacency, use the **label-switched-path** statement and specify the LSP configured in “Configuring a Hierarchy of RSVP LSPs” on page 27:

label-switched-path *label-switched-path-name*;

You can include this statement at the following hierarchy levels:

- **[edit protocols link-management** te-link ***te-link-name*****]**
- **[edit logical-systems *logical-system-name* protocols link-management** te-link ***te-link-name*****]**

Configuring RSVP for Forwarding Adjacencies

For the forwarding adjacency to function properly, RSVP must be made aware of it. Do this by specifying the name of the peer interface corresponding to the link-management peer associated with the forwarding adjacency. Including the **peer-interface** statement at the **[edit protocols rsvp]** hierarchy level enables RSVP to use all of the traffic engineering links configured for that peer. You can also configure RSVP control-plane parameters such as the hello interval and refresh reduction.

To configure RSVP to recognize a forwarding adjacency, include the **peer-interface** statement:

```
peer-interface peer-interface-name {
  disable;
  (aggregate | no-aggregate);
  authentication-key key;
  hello-interval seconds;
  (reliable | no-reliable);
}
```

You can include this statement at the following hierarchy levels:

- **[edit protocols rsvp]**
- **[edit logical-systems *logical-system-name* protocols rsvp]**

For more information on how to configure the **peer-interface** statement, see "Configuring RSVP and OSPF for LMP Peer Interfaces" on page 19.

Advertising Forwarding Adjacencies Using OSPF

You can allow other routers to dynamically signal paths over a forwarding adjacency LSP by configuring OSPF. This configuration is optional.

If you configure OSPF to advertise a forwarding adjacency LSP, the LSP is added to the traffic engineering database on each router in the traffic engineering domain. Because the forwarding adjacency LSP is unidirectional, the corresponding traffic engineering link (forwarding adjacency) is also unidirectional. The forwarding adjacency LSP appears as a standard traffic engineering database half-link to all routers in the traffic engineering domain.

Constrained Shortest Path First (CSPF) performs a bidirectional link check to ensure that traffic can flow in both directions. CSPF checks for a reverse link, either the exact reverse forwarding adjacency or another reverse link. If there is no reverse link from the forwarding adjacency LSP egress router to the forwarding adjacency LSP ingress router, the CSPF check fails.

CSPF might find another parallel reverse link. However, the LSP cannot function properly over the forwarding adjacency unless you have explicitly configured a corresponding forwarding adjacency LSP to handle the traffic flowing in the opposite direction on the forwarding adjacency LSP egress router.

To advertise the traffic engineering properties of a forwarding adjacency to a specific peer router, include the **peer-interface** statement:

```
peer-interface peer-interface-name {
  dead-interval seconds;
  disable;
  hello-interval seconds;
  retransmit-interval seconds;
  transit-delay seconds;
}
```

You can configure this statement at the following hierarchy levels:

- **[edit protocols ospf area *area-name*]**
- **[edit logical-systems *logical-system-name* protocols ospf area *area-name*]**

For more information on how to configure the **peer-interface** statement, see "Configuring RSVP and OSPF for LMP Peer Interfaces" on page 19.

PART 3

Administration

CHAPTER 5

GMPLS Standards and Terminology

Supported GMPLS Standards

The Junos OS substantially supports the following RFCs and Internet drafts, which define standards for Generalized MPLS (GMPLS).

- RFC 3471, *Generalized Multi-Protocol* [sic] *Label Switching (GMPLS) Signaling Functional Description*

  Only the following features are supported:

  - Bidirectional LSPs (upstream label only)
  - Control channel separation
  - Generalized label (suggested label only)
  - Generalized label request (bandwidth encoding only)

- RFC 3473, *Generalized Multi-Protocol* [sic] *Label Switching (GMPLS) Signaling Resource ReserVation* [sic] *Protocol-Traffic Engineering (RSVP-TE) Extensions*

  Only Section 9, "Fault Handling," is supported.

- RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol* [sic] *Label Switching (GMPLS) Traffic Engineering (TE)*
- Internet draft draft-ietf-ccamp-gmpls-routing-09.txt, *Routing Extensions in Support of Generalized Multi-Protocol* [sic] *Label Switching*

  Only interface switching is supported.

- Internet draft draft-ietf-ccamp-gmpls-rsvp-te-ason-02.txt, *Generalized MPLS (GMPLS) RSVP-TE Signalling in support of Automatically Switched Optical Network (ASON)* (expires January 2005)
- Internet draft draft-ietf-ccamp-gmpls-sonet-sdh-08.txt, *Generalized Multi-Protocol* [sic] *Label Switching Extensions for SONET and SDH Control*

  Only S,U,K,L,M-format labels and SONET traffic parameters are supported.

- Internet draft draft-ietf-ccamp-lmp-10.txt, *Link Management Protocol (LMP)*
- Internet draft draft-ietf-ccamp-ospf-gmpls-extensions-12.txt, *OSPF Extensions in Support of Generalized Multi-Protocol* [sic] *Label Switching*

  The following sub-TLV types for the Link type, link, value (TLV) are not supported:

  - Link Local/Remote Identifiers (type 11)
  - Link Protection Type (type 14)
  - Shared Risk Link Group (SRLG) (type 16)

  The features described in Section 2 of the draft, “Implications on Graceful Restart,” are also not supported.

  The Interface Switching Capability Descriptor (type 15) sub-TLV type is implemented, but only for packet switching.
- Internet draft draft-ietf-mpls-bundle-04.txt, *Link Bundling in MPLS Traffic Engineering*

Related Documentation

- Supported LDP Standards
- Supported MPLS Standards
- Supported RSVP Standards
- Accessing Standards Documents on the Internet

GMPLS Terms and Acronyms

F

Forwarding adjacency A forwarding path for sending data between GMPLS-enabled devices.

G

Generalized MPLS (GMPLS) An extension to MPLS that allows data from multiple layers to be switched over label-switched paths (LSPs). GMPLS LSP connections are possible between similar Layer 1, Layer 2, and Layer 3 devices.

GMPLS label Layer 3 identifiers, fiber port, time-division multiplexing (TDM) time slot, or dense wavelength-division multiplexing (DWDM) wavelength of a GMPLS-enabled device used as a next-hop identifier.

GMPLS LSP types The four types of GMPLS LSPs are:

- Fiber-switched capable (FSC)—LSPs are switched between two fiber-based devices, such optical cross-connects (OXCs) that operate at the level of individual fibers.
- Lambda-switched capable (LSC)—LSPs are switched between two DWDM devices, such as such as OXCs that operate at the level of individual wavelengths.
- TDM-switched capable (TDM)—LSPs are switched between two TDM devices, such as SONET ADMs.
- Packet-switched capable (PSC)—LSPs are switched between two packet-based devices, such as routers or ATM switches.

L

Link Management Protocol A protocol used to define a forwarding adjacency between peers and to maintain and allocate resources on the traffic engineering links.

T

Traffic engineering link A logical connection between GMPLS-enabled devices. Traffic engineering links can have addresses or IDs and are associated with certain resources or interfaces. They also have certain attributes (encoding-type, switching capability, bandwidth, and so on). The logical addresses can be routable, although this is not required because they are acting as link identifiers. Each traffic engineering link represents a forwarding adjacency between a pair of devices.

CHAPTER 6

Hierarchy of RSVP LSPs Standards and Terminology

Hierarchy of RSVP LSPs Standard

For more information on how a hierarchy of RSVP LSPs functions, see RFC 4206, *Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)*.

Hierarchy of RSVP LSPs Terminology

F

Forwarding adjacency

A traffic engineering link created by a forwarding adjacency LSP. You can create a forwarding adjacency between two routers in a network by configuring a forwarding adjacency LSP. Forwarding adjacencies can only be statically configured. However, you can configure OSPF to advertise the forwarding adjacency to other routers. When an RSVP LSP traverses a forwarding adjacency, existing MPLS features such as fast reroute continue to function.

Forwarding adjacency LSP

An RSVP LSP used to tunnel other RSVP LSPs; forms the basis for a forwarding adjacency.

CHAPTER 7

Summary of GMPLS Configuration Statements

address

Syntax address *ip-address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name*],
[edit protocols link-management peer *peer-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the ID of the peer.

Default The loopback address is advertised.

Options *ip-address*—IP address of the peer.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the ID for LMP Peers on page 15

control-channel

Syntax control-channel *control-channel-interface*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name*],
[edit protocols link-management peer *peer-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the control channel interface for the peer.

Options ***control-channel-interface***—Name of the control channel interface.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring LMP Peers on page 14

dead-interval

Syntax dead-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number*
peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify how long OSPF and OSPF version 3 (OSPFv3) wait before declaring that a neighboring router is unavailable. This is an interval during which the router receives no hello packets from the neighbor.

Options ***seconds***—Interval to wait.

Range: 1 through 65,535

Default: 40 seconds (four times the hello interval)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP and OSPF for LMP Peer Interfaces on page 19
- **hello-interval (OSPF) on page 43**

disable (GMPLS)

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Disable a traffic engineering link.

Default The configured object is enabled (operational) unless explicitly disabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Disabling the Traffic Engineering Link for LMP Peers on page 18

disable (OSPF Peer Interface)

Syntax disable;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Disable an OSPF peer interface.

Default The configured object is enabled (operational) unless explicitly disabled.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP and OSPF for LMP Peer Interfaces on page 19

hello-dead-interval

Syntax hello-dead-interval *milliseconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in Junos OS Release 8.0.

Description Specify how long the Link Management Protocol (LMP) waits before declaring the control channel to be dead. This is an interval during which the router receives no LMP hello packets from the neighbor on a control that is active or up.

Options ***milliseconds***—Interval to wait before declaring the control channel to be dead.

Range: 500 through 300,000

Default: 500 milliseconds (three times the hello interval)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Hello Message Intervals for LMP Control Channels on page 16
- **hello-interval (LMP) on page 42**

hello-interval (LMP)

Syntax hello-interval *milliseconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in Junos OS Release 8.1.

Description Specify how often the router sends Link Management Protocol (LMP) hello packets.

Options ***milliseconds***—Length of time between hello packets.

Range: 150 through 300,000

Default: 150 milliseconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Hello Message Intervals for LMP Control Channels on page 16
- **hello-dead-interval on page 42**

hello-interval (OSPF)

Syntax hello-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify how often the router sends hello packets out the peer interface. The hello interval must be the same for all routers on a shared logical IP network.

Options *seconds*—Length of time between hello packets.

Range: 1 through 255

Default: 10 seconds; 120 seconds (nonbroadcast networks)

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP and OSPF for LMP Peer Interfaces on page 19
- **dead-interval on page 40**

interface

Syntax interface *interface-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the egress router interface.

Options *interface-name*—Name of the interface to the egress router.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- LMP Configuration Overview on page 11

label-switched-path

Syntax label-switched-path *lsp-name*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name*]

Release Information Statement introduced in Junos OS Release 7.4.

Description Specify the label-switched path (LSP) to be used by the forwarding adjacency.

Options *lsp-name*—Name of the LSP.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Forwarding Adjacencies on page 27

link-management

Syntax link-management { ... }

Hierarchy Level [edit logical-systems *logical-system-name* protocols],
[edit protocols]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable Link Management Protocol (LMP) on the router.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- LMP Configuration Overview on page 11

lmp-control-channel

Syntax

lmp-control-channel *control-channel-interface* {
  remote-address *ip-address*;
}

Hierarchy Level

[edit logical-systems *logical-system-name* protocols link-management peer *peer-name*],
[edit protocols link-management peer *peer-name*]

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Specify the Link Management Protocol (LMP) control channel interface for the peer.

Options

control-channel-interface—Name of the control channel interface.

The remaining statement is described separately in this chapter.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the LMP Control Channel Interface for the Peer on page 15

lmp-protocol

Syntax

lmp-protocol {
  hello-dead-interval *milliseconds*;
  hello-interval *milliseconds*;
  passive;
  retransmission-interval *milliseconds*;
  retry-limit *number*;
}

Hierarchy Level

[edit logical-systems *logical-system-name* protocols link-management peer *peer-name*],
[edit protocols link-management peer *peer-name*]

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Configure attributes of Link Management Protocol (LMP) to establish and maintain the LMP control channel for the peer.

Options

The statements are described separately in this chapter.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring LMP Peers on page 14

local-address

Syntax local-address *ip-address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name* interface *interface-name*],
[edit protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the local IP address associated with the traffic engineering link.

Options *local-address*—Local IP address of the traffic engineering link.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Local IP Address for Traffic Engineering Links on page 13
- Configuring the Local IP Address for Forwarding Adjacencies on page 28

passive

Syntax passive;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in Junos OS Release 8.1.

Description Specify that the router not configure the Link Management Protocol (LMP) control channels but wait for the remote peer to configure the LMP control channels.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Preventing the Local Peer from Initiating LMP Negotiation on page 18

peer

Syntax

```
peer peer-name {
  address ip-address;
  control-channel control-channel-interface;
  lmp-control-channel control-channel-interface;
  lmp-protocol {
    hello-dead-interval milliseconds;
    hello-interval milliseconds;
    passive;
    retransmission-interval milliseconds;
    retry-limit number;
  }
  te-link te-link-name;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols link-management],
[edit protocols link-management]

Release Information

Statement introduced before Junos OS Release 7.4.
lmp-protocol statement and substatements added in Junos OS Release 8.1.

Description

Configure a network peer.

Options

peer-name—Name of the network peer.

The remaining statements are described separately in this chapter.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring LMP Peers on page 14

peer-interface (OSPF)

Syntax

```
peer-interface peer-interface-name {
  dead-interval seconds;
  disable;
  hello-interval seconds;
  retransmit-interval seconds;
  transit-delay seconds;
}
```

Hierarchy Level
[edit logical-systems *logical-system-name* protocols ospf area *area-id*],
[edit protocols ospf area *area-id*]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure the control channel. The peer interface name is the same as the peer interface name configured under LMP.

Options
The options are explained separately.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP and OSPF for LMP Peer Interfaces on page 19
- Advertising Forwarding Adjacencies Using OSPF on page 29
- *Junos OS Routing Protocols Configuration Guide*

remote-address (for LMP Control Channel)

Syntax
remote-address *ip-address*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*],
[edit protocols link-management peer *peer-name* lmp-control-channel *control-channel-interface*]

Release Information
Statement introduced in Junos OS Release 8.1.

Description
Specify the remote IP address for the Link Management Protocol (LMP) control channel interface.

Options
ip-address—Remote IP address mapped to the LMP control channel interface.

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Remote IP Address for LMP Control Channels on page 16

remote-address (for LMP Traffic Engineering)

Syntax remote-address *ip-address*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name* interface *interface-name*],
[edit protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the remote IP address for the traffic engineering link.

Options ***ip-address***—Remote IP address mapped to the traffic engineering link.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Remote IP Address for Traffic Engineering Links on page 13
- Configuring the Remote IP Address for Forwarding Adjacencies on page 28

remote-id

Syntax remote-id *id-number*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name*],
[edit logical-systems *logical-system-name* protocols link-management te-link *te-link-name* interface *interface-name*],
[edit protocols link-management te-link *te-link-name*],
[edit protocols link-management te-link *te-link-name* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the ID assigned to a traffic engineering link or an interface (resource) on the peer node.

Options ***id-number***—ID number for the remote device.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring the Remote ID for Traffic Engineering Links on page 14

retransmission-interval

Syntax retransmission-interval *milliseconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information Statement introduced in Junos OS Release 8.1.

Description Specify how often Link Management Protocol (LMP) sends Config and LinkSummary messages on the LMP control channel.

Options *milliseconds*—Length of time between Config messages.

Range: 500 through 300,000

Default: 500 milliseconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- **retry-limit on page 51**
- Controlling Message Exchange for LMP Control Channels on page 17

retransmit-interval

Syntax retransmit-interval *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify how long the router waits to receive a link-state acknowledgment packet before retransmitting link-state advertisements to a peer interface's neighbors.

Options *seconds*—Interval to wait for a link-state acknowledgment packet.

Range: 1 through 65,535

Default: 5 seconds

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP and OSPF for LMP Peer Interfaces on page 19

retry-limit

Syntax
retry-limit *number*;

Hierarchy Level
[edit logical-systems *logical-system-name* protocols link-management peer *peer-name* lmp-protocol],
[edit protocols link-management peer *peer-name* lmp-protocol]

Release Information
Statement introduced in Junos OS Release 8.1.

Description
Specify how many times the Link Management Protocol (LMP) sends Config and LinkSummary messages on the LMP control channel without receiving an appropriate acknowledgment before it logs a message and restarts the LMP control channel configuration process.

Options
number—Maximum number of times messages are sent without receiving an acknowledgment.

Range: 3 through 1000

Default: 3

Required Privilege Level
routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- **retransmission-interval on page 50**
- Controlling Message Exchange for LMP Control Channels on page 17

te-link

Syntax

```
te-link te-link-name {
  disable;
  interface interface-name {
    disable;
    local-address ip-address;
    remote-address ip-address;
    remote-id id-number;
  }
  local-address ip-address;
  remote-address ip-address;
  remote-id id-number;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols link-management],
[edit logical-systems *logical-system-name* protocols link-management peer *peer-name*],
[edit protocols link-management],
[edit protocols link-management peer *peer-name*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Represent a collection of physical ports or time slots. Assign a traffic engineering link to the specified network peer.

Options

te-link-name—Name of the collection of physical ports or the name of the time slots.

disable—Disable the traffic engineering link or an interface to a traffic engineering link.

The other statements are described separately in this chapter.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring LMP Traffic Engineering Links on page 12

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
  flag flag <flag-modifier> <disable>;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* protocols link-management],
[edit protocols link-management]

Release Information

Statement introduced before Junos OS Release 7.4.
Support for **hello-packets**, **packets**, and **state** flags added in Junos OS Release 8.1.

Description

Trace options for the LMP protocol.

Options

disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as **all**.

filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Range: 2 through 1000

Default: 2 files

If you specify a maximum number of files, you must also include the **size** statement to specify the maximum file size.

flag—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements.

- **all**—Trace all available operations
- **hello-packets**—Trace hello packets on any LMP control channel
- **init**—Output from the initialization messages
- **packets**—Trace all packets other than hello packets on any LMP control channel
- **parse**—Operation of the parser
- **process**—Operation of the general configuration
- **route-socket**—Operation of route socket events
- **routing**—Operation of the routing protocols
- **server**—Server processing operations
- **show**—**show** command servicing operations

- **state**—Trace state transitions of the LMP control channels and traffic engineering links

flag-modifier—(Optional) Modifier for the tracing flag. You can specify one or more of these modifiers:

- **detail**—Provide detailed trace information
- **receive**—Packets being received
- **send**—Packets being transmitted

no-world-readable—(Optional) Prevent all users from reading the log file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches this size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

If you specify a maximum file size, you must also include the **files** statement to specify the maximum number of files.

world-readable—(Optional) Enable log file access for all users.

Required Privilege Level

routing and trace—To view this statement in the configuration.
routing-control and trace-control—To add this statement to the configuration.

Related Documentation

- Tracing LMP Traffic on page 21
- *Junos OS Network Management Configuration Guide*

transit-delay

Syntax transit-delay *seconds*;

Hierarchy Level [edit logical-systems *logical-system-name* protocols ospf area *area-number* peer-interface *peer-interface-name*],
[edit protocols ospf area *area-number* peer-interface *peer-interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set the estimated time required to transmit a link-state update on the peer interface. When calculating this time, you should account for transmission and propagation delays.

Options ***seconds***—Estimated time for transmitting the link-state update.

Range: 1 through 65,535

Default: 1 second

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring RSVP and OSPF for LMP Peer Interfaces on page 19

PART 4

Index

Index

I

L

M

N

O

P

R

S

