Ethernet Ring Protection Switching

Published: 2013-02-14

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

Ethernet Ring Protection Switching

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 Figures

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.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series
- J Series

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 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`

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes 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*
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; 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

Ethernet Ring Protection Switching

Ethernet Ring Protection Switching Overview

Ethernet ring protection switching (ERPS) helps achieve high reliability and network stability. Links in the ring will never form loops that fatally affect the network operation and services availability. The basic idea of an Ethernet ring is to use one specific link to protect the whole ring. This special link is called a *ring protection link (RPL)*. If no failure happens in other links of the ring, the RPL blocks the traffic and is not used. The RPL is controlled by a special node called an *RPL owner*. There is only one RPL owner in a ring. The RPL owner is responsible for blocking traffic over the RPL. Under ring failure conditions, the RPL owner is responsible for unblocking traffic over the RPL. A ring failure results in protection switching of the RPL traffic. An automation protocol suite (APS) protocol is used to coordinate the protection actions over the ring. Protection switching blocks traffic on the failed link and unblocks the traffic on the RPL. When the failure clears, revertive protection switching blocks traffic over the RPL and unblocks traffic on the link on which the failure is cleared.

The following standards provide detailed information on Ethernet ring protection switching:

- IEEE 802.1Q - 1998
- IEEE 802.1D - 2004
- IEEE 802.1Q - 2003
- Draft ITU-T Recommendation G.8032/Y.1344, *Ethernet Ring protection switching*
- ITU-T Y.1731, *OAM functions and mechanisms for Ethernet-based networks*

For additional information on configuring Ethernet ring protection switching on EX Series switches, see Example: Configuring Ethernet Ring Protection Switching on EX Series Switches.

For additional information on configuring Ethernet ring protection switching on MX Series routers, see the *Layer 2 Configuration Guide* for a complete example of Ethernet rings and information about STP loop avoidance and prevention.

Related Documentation

- Understanding Ethernet Ring Protection Switching Functionality on page 4
- Configuring Ethernet Ring Protection Switching on page 11
- Example: Ethernet Ring Protection Switching Configuration on MX Routers on page 12
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Junos® OS Ethernet Interfaces

Understanding Ethernet Ring Protection Switching Functionality

Acronyms

The following acronyms are used in the discussion about Ethernet ring protection switching:

- MA—Maintenance association
- MEP—Maintenance association end point
- OAM—Connectivity fault management daemon
- FDB—MAC forwarding database
- STP—Spanning Tree Protocol
- RAPS—Ring automatic protection switching
- WTR—Wait to restore
- RPL—Ring protection link

Ring Nodes

Multiple nodes are used to form a ring. For each ring node. There are two different node types:

- Normal node—The node has no special role on the ring.
- RPL owner node—The node owns the RPL and blocks or unblocks traffic over the RPL. This node also initiates the RAPS message.

Ring Node States

There are three different states for each node of a specific ring:

- init—Not a participant of a specific ring.
- idle—No failure on the ring; the node is performing normally. For a normal node, traffic is unblocked on both ring ports. For the RPL owner, traffic is blocked on the ring port that connects to the RPL and unblocked on the other ring port.
- protection—A failure occurred on the ring. For normal node, traffic is blocked on the ring port that connects to the failing link and unblocked on working ring ports. For the RPL owner, traffic is unblocked on both ring ports if they connect to non-failure links.

There can be only one RPL owner for each ring. The user configuration must guarantee this, because the APS protocol cannot check this.

Failure Detection

Ethernet ring operation depends on quick and accurate failure detection. The failure condition *signal failure (SF)* is supported. For SF detection, an Ethernet continuity check MEP must be configured for each ring link. For fast protection switching, a 10-ms transmission period for this MEP group is supported. OAM monitors the MEP group's MA and reports SF or SF clear events to the Ethernet ring control module. For this MEP group, the action profile must be configured to update the interface device IFF_LINKDOWN flag. OAM updates the IFF_LINKDOWN flag to notify the Ethernet ring control module.

Logical Ring

This feature currently supports only the physical ring, which means that two adjacent nodes of a ring must be physically connected and the ring must operate on the physical interface, not the VLAN.

FDB Flush

When ring protection switching occurs, normally an *FDB flush* should be executed. The Ethernet ring control module (or, on the switch, the ERPS configuration) should use the same mechanism as the STP to trigger the FDB flush. The Ethernet ring control module controls the ring port physical interface's default STP index to execute the FDB flush.

Traffic Blocking and Forwarding

Ethernet ring control uses the same mechanism as the STP to control forwarding or discarding of user traffic. The Ethernet ring control module sets the ring port physical interface default STP index state to forwarding or discarding in order to control user traffic.

RAPS Message Blocking and Forwarding

The router or switch treats the ring automatic protection switching (RAPS) message the same as it treats user traffic for forwarding RAPS messages between two ring ports. The ring port physical interface default STP index state also controls forwarding RAPS messages between the two ring ports. Other than forwarding RAPS messages between the two ring ports, as shown in Figure 1 on page 6, the system also needs to forward the RAPS message between the CPU (Ethernet ring control module) and the ring port. This type of forwarding does not depend on the ring port physical interfaces' STP index state. The RAPS message is always sent by the router or switch through the ring ports, as shown in Figure 2 on page 6. A RAPS message received from a discarding ring port is sent to the Ethernet ring control module, but is not sent to the other ring port.

Figure 1: Protocol Packets from the Network to the Router

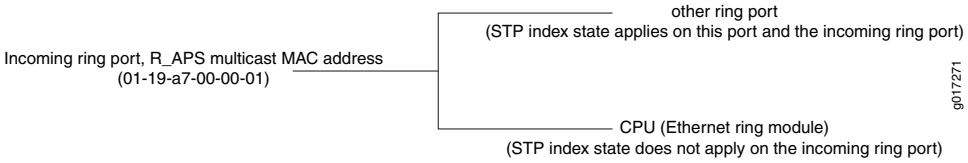
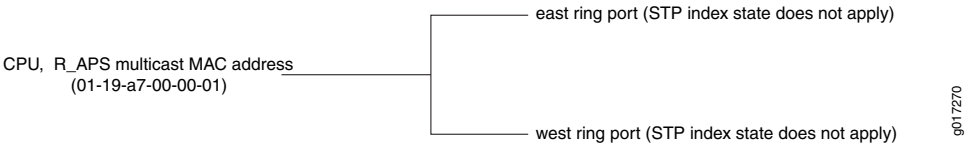


Figure 2: Protocol Packets from the Router or Switch to the Network



Juniper Networks EX Series switches and Juniper Networks MX Series routers use different methods to achieve these routes.

The switches use forwarding database entries to direct the RAPS messages. The forwarding database entry (keyed by the RAPS multicast address and VLAN) has a composite next hop associated with it—the composite next hop associates the two ring interfaces with the forwarding database entry and uses the split horizon feature to prevent sending the packet out on the interface that it is received on. This is an example of the forwarding database entry relating to the RAPS multicast MAC (a result of the **show ethernet-switching table detail** command):

```
VLAN: v1, Tag: 101, MAC: 01:19:a7:00:00:01, Interface: ERP
Interfaces:          ge-0/0/9.0, ge-0/0/3.0
Type: Static
Action: Mirror
Nexthop index: 1333
```

The routers use an implicit filter to achieve ERP routes. Each implicit filter binds to a bridge domain. Therefore, the east ring port control channel and the west ring port control channel of a particular ring instance must be configured to the same bridge domain. For each ring port control channel, a filter term is generated to control RAPS message forwarding. The filter number is the same as the number of bridge domains that contain the ring control channels. If a bridge domain contains control channels from multiple rings, the filter related to this bridge domain will have multiple terms and each term will relate to a control channel. The filter has command parts and control-channel related parts, as follows:

- Common terms:
  - term 1: if [Ethernet type is not OAM Ethernet type (0x8902)
    ] { accept packet }
  - term 2: if [source MAC address belongs to this bridge]
    { drop packet, our packet loop through the ring and come back
    to home}
  - term 3: if [destination is the RAPS PDU multicast address(0x01,0x19,0xa7,
    0x00,0x00,0x01] AND[ring port STP status is DISCARDING]
    { send to CPU }
- Control channel related terms:
  - if [destination is the RAPS PDU multicast address(0x01,0x19,0xa7,0x00,0x00,
    0x01] AND[ring port STP status is FORWARDING] AND [Incoming interface
    IFL equal to control channel IFL]
    { send packet to CPU and send to the other ring port }
    default term: accept packet.

Dedicated Signaling Control Channel

For each ring port, a dedicated signaling control channel with a dedicated VLAN ID must be configured. In Ethernet ring configuration, only this control logical interface is configured and the underlying physical interface is the physical ring port. Each ring requires that two control physical interfaces be configured. These two logical interfaces must be configured in a bridge domain for routers (or the same VLAN for switches) in order to forward RAPS protocol data units (PDUs) between the two ring control physical interfaces. If the router control channel logical interface is not a trunk port, only control logical interfaces will be configured in ring port configuration. If this router control channel logical interface is a trunk port, in addition to the control channel logical interfaces, a dedicated VLAN ID must be configured for routers. For EX Series switches, always specify either a VLAN name or VLAN ID for all links.

RAPS Message Termination

The RAPS message starts from the originating node, travels through the entire ring, and terminates in the originating node unless a failure is present in the ring. The originating node must drop the RAPS message if the source MAC address in the RAPS message belongs to itself. The source MAC address is the node's node ID.

Multiple Rings

The Ethernet ring control module supports multiple rings in each node (two logical interfaces are part of each ring). However, interconnection of multiple rings is not supported in this release. The interconnection of two rings means that two rings may share the same link or share the same node.

Node ID

For each node in the ring, a unique *node ID* identifies each node. The node ID is the node's MAC address.

For routers only, you can configure this node ID when configuring the ring on the node or automatically select an ID such as STP. In most cases, you will not configure this and the router will select a node ID, like STP does. It should be the manufacturing MAC address. The ring node ID should not be changed, even if you change the manufacturing MAC address. Any MAC address can be used if you make sure each node in the ring has a different node ID. The node ID on EX Series switches is selected automatically and is not configurable.

Bridge Domains with the Ring Port (MX Series Routers Only)

On the routers, the protection group is seen as an abstract logical port that can be configured to any bridge domain. Therefore, if you configure one ring port or its logical interface in a bridge domain, you must configure the other related ring port or its logical interface to the same bridge domain. The bridge domain that includes the ring port acts as any other bridge domain and supports the IRB Layer 3 interface.

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Configuring Ethernet Ring Protection Switching on page 11
- Example: Ethernet Ring Protection Switching Configuration on MX Routers on page 12
- Junos® OS Ethernet Interfaces
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

PART 2

Configuration

CHAPTER 2

Ethernet Ring Protection Switching

Configuring Ethernet Ring Protection Switching

The inheritance model follows:

```
protection-group {
  ethernet-ring ring-name (
    node-id mac-address;
    ring-protection-link-owner;
    east-interface {
      control-channel channel-name {
      ring-protection-link-end;
    }
    west-interface {
      node-id mac-address;
      control-channel channel-name {
      ring-protection-link-end;
    }
    data-channel {
      vlan number;
    }
    guard-interval number;
    restore-interval number;
  }
}
```

For each ring, a protection group must be configured. There may be several rings in each node, so there should be multiple protection groups corresponding to the related Ethernet rings.

Three interval parameters (**restore-interval**, **guard-interval**, and **hold-interval**) can be configured at the protection group level. These configurations are global configurations and apply to all Ethernet rings if the Ethernet ring doesn't have a more specific configuration for these values. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Understanding Ethernet Ring Protection Switching Functionality on page 4

Example: Ethernet Ring Protection Switching Configuration on MX Routers

This example describes how to configure Ethernet ring protection switching on an MX Series router:

Requirements

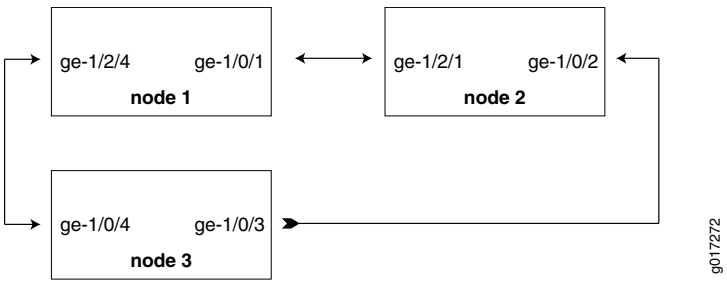
This example uses the following hardware and software components:

- Router node 1 running Junos OS with two Gigabit Ethernet interfaces.
- Router node 2 running Junos OS with two Gigabit Ethernet interfaces.
- Router node 3 running Junos OS with two Gigabit Ethernet interfaces.

Ethernet Ring Overview and Topology

This section describes a configuration example for a three-node ring. The ring topology is shown in Figure 3 on page 12.

Figure 3: Example of a Three-Node Ring Topology



The configuration in this section is only for the RAPS channel. The bridge domain for user traffic is the same as the normal bridge domain. The only exception is if a bridge domain includes a ring port, then it must also include the other ring port of the same ring.

Configuring a Three-Node Ring

To configure Ethernet Ring Protection Switching on a three-node ring, perform these tasks:

Configuring Ethernet Ring Protection Switching on a Three-Node Ring

Step-by-Step Procedure

1. **Configuring Node 1**

```
interfaces {
   ge-1/0/1 {
      vlan-tagging;
      encapsulation flexible-ethernet-services;
      unit 1 {
         encapsulation vlan-bridge;
         vlan-id 100;
      }
   }
   ge-1/2/4 {
      vlan-tagging;
      encapsulation flexible-ethernet-services;
      unit 1 {
         encapsulation vlan-bridge;
         vlan-id 100;
         }
      }
   }
   bridge-domains {
      bd1 {
         domain-type bridge;
         interface ge-1/2/4.1;
         interface ge-1/0/1.1;
         }
      }
   protocols {
      protection-group {
         ethernet-ring pg101 {
            node-id 00:01:01:00:00:01;
            ring-protection-link-owner;
            east-interface {
               control-channel ge-1/0/1.1;
               ring-protection-link-end;
               }
            west-interface {
               control-channel ge-1/2/4.1;
               }
            }
         }
      }
   protocols {
      oam {
         ethernet {
            connectivity-fault-management {
               action-profile rmep-defaults {
                  default-action {
                     interface-down;
                     }
                  }
               maintenance-domain d1 {
                  level 0;
```

```
                maintenance-association 100 {
                  mep 1 {
                    interface ge-1/0/1;
                    remote-mep 2 {
                      action-profile rmep-defaults;
                      }
                    }
                  }
                }
              maintenance-domain d2 {
                level 0;
                maintenance-association 100 {
                  mep 1 {
                    interface ge-1/2/4;
                    remote-mep 2 {
                      action-profile rmep-defaults;
                      }
                    }
                  }
                }
              }
            }
          }
        }
      }
    }
```

2. **Configuring Node 2**

```
interfaces {
  ge-1/0/2 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
      encapsulation vlan-bridge;
      vlan-id 100;
    }
  }

  ge-1/2/1 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
      encapsulation vlan-bridge;
      vlan-id 100;
    }
  }
}

bridge-domains {
  bd1 {
    domain-type bridge;
    interface ge-1/2/1.1;
    interface ge-1/0/2.1;
  }
}
```

```
protocols {
  protection-group {
    ethernet-ring pg102 {
      east-interface {
        control-channel ge-1/0/2.1;
      }
      west-interface {
        control-channel ge-1/2/1.1;
      }
    }
  }
}
```

```
protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        action-profile rmep-defaults {
          default-action {
            interface-down;
          }
        }
        maintenance-domain d1 {
          level 0;
          maintenance-association 100 {
            mep 2 {
              interface ge-1/2/1;
              remote-mep 1 {
                action-profile rmep-defaults;
              }
            }
          }
        }
        maintenance-domain d3 {
          level 0;
          maintenance-association 100 {
            mep 1 {
              interface ge-1/0/2;
              remote-mep 2 {
                action-profile rmep-defaults;
              }
            }
          }
        }
      }
    }
  }
}
```

3. **Configuring Node 3**

```
interfaces {
  ge-1/0/4 {
    vlan-tagging;
    encapsulation flexible-ethernet-services;
    unit 1 {
```

```
        encapsulation vlan-bridge;
        vlan-id 100;
      }
    }

    ge-1/0/3 {
      vlan-tagging;
      encapsulation flexible-ethernet-services;
      unit 1 {
        encapsulation vlan-bridge;
        vlan-id 100;
      }
    }
}

bridge-domains {
  bd1 {
    domain-type bridge;
    interface ge-1/0/4.1;
    interface ge-1/0/3.1;
  }
}


protocols {
  protection-group {
    ethernet-ring pg103 {
      east-interface {
        control-channel ge-1/0/3.1;
      }
      west-interface {
        control-channel ge-1/0/4.1;
      }
    }
  }
}


protocols {
  oam {
    ethernet {
      connectivity-fault-management {
        action-profile rmep-defaults {
          default-action {
            interface-down;
          }
        }
        maintenance-domain d2 {
          level 0;
          maintenance-association 100 {
            mep 2 {
              interface ge-1/0/4;
              remote-mep 1 {
                action-profile rmep-defaults;
              }
            }
```

```
            }
          }
          maintenance-domain d3 {
            level 0;
            maintenance-association 100 {
              mep 2 {
                interface ge-1/0/3;
                remote-mep 1 {
                  action-profile rmep-defaults;
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Examples: Ethernet RPS Output

This section provides output examples based on the configuration shown in "Example: Ethernet Ring Protection Switching Configuration on MX Routers" on page 12. The show commands used in these examples can help verify configuration and correct operation.

Normal Situation—RPL Owner Node

If the ring has no failure, the **show** command will have the following output for Node 1:

```
user@node1> show protection-group ethernet-ring aps

Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg101               NR             No        Yes

Originator  Remote Node ID
Yes
```

```
user@node1> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg101

Interface    Control Channel  Forward State  Ring Protection Link End
ge-1/0/1     ge-1/0/1.1       discarding     Yes
ge-1/2/4     ge-1/2/4.1       forwarding     No

Signal Failure  Admin State
Clear          IFF ready
Clear          IFF ready
```

```
user@node1> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg101            idle         NR-RB         Yes

Restore Timer  Quard Timer  Operation state
disabled       disabled    operational
```

```
user@node1> show protection-group ethernet-ring statistics group-name pg101
Ethernet Ring statistics for PG pg101
RAPS sent                        : 1
RAPS received                    : 0
Local SF happened:               : 0
Remote SF happened:              : 0
NR event happened:               : 0
NR-RB event happened:            : 1
```

Normal Situation—Other Nodes

For Node 2 and Node 3, the outputs should be the same:

```
user@node2> show protection-group ethernet-ring aps
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg102               NR             No        Yes

Originator  Remote Node ID
No          00:01:01:00:00:01
```

```
user@node2> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg102

Interface    Control Channel  Forward State  Ring Protection Link End
ge-1/2/1     ge-1/2/1.1       forwarding     No
ge-1/0/2     ge-1/0/2.1       forwarding     No

Signal Failure  Admin State
Clear          IFF ready
Clear          IFF ready
```

```
user@node2> show protection-group ethernet-ring node-state
```

```
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg102            idle         NR-RB         No

Restore Timer  Quard Timer  Operation state
disabled       disabled     operational
```

```
user@node2> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg101
RAPS sent                       : 0
RAPS received                   : 1
Local SF happened:              : 0
Remote SF happened:             : 0
NR event happened:              : 0
NR-RB event happened:           : 1
```

Failure Situation—RPL Owner Node

If the ring has a link failure between Node 2 and Node 3, the **show** command will have the following outputs for Node 1:

```
user@node1> show protection-group ethernet-ring aps
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg101               SF             NO        No

Originator  Remote Node ID
No          00:01:02:00:00:01
```

```
user@node1> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg101

Interface    Control Channel  Forward State  Ring Protection Link End
ge-1/0/1     ge-1/0/1.1       forwarding     Yes
ge-1/2/4     ge-1/2/4.1       forwarding     No

Signal Failure  Admin State
Clear           IFF ready
Clear           IFF ready
```

```
user@node1> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg101            protected    SF            Yes

Restore Timer  Quard Timer  Operation state
disabled       disabled     operational
```

```
user@node1> show protection-group ethernet-ring statistics group-name pg101
Ethernet Ring statistics for PG pg101
RAPS sent                       : 1
RAPS received                   : 1
Local SF happened:              : 0
Remote SF happened:             : 1
NR event happened:              : 0
NR-RB event happened:           : 1
```

Failure Situation—Other Nodes

For Node 2 and Node 3, the outputs should be the same:

```
user@node2> show protection-group ethernet-ring aps
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg102               SF             No        No

Originator  Remote Node ID
Yes         00:00:00:00:00:00
```

```
user@node2> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg102

Interface    Control Channel  Forward State  Ring Protection Link End
ge-1/2/1     ge-1/2/1.1       forwarding     No
ge-1/0/2     ge-1/0/2.1       discarding     No

Signal Failure  Admin State
Clear           IFF ready
set             IFF ready
```

```
user@node2> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg102             idle        NR-RB         No

Restore Timer  Quard Timer  Operation state
disabled       disabled     operational
```

```
user@node2> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg101
RAPS sent                        : 1
RAPS received                    : 1
Local SF happened:               : 1
Remote SF happened:              : 0
NR event happened:               : 0
NR-RB event happened:            : 1
```

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Understanding Ethernet Ring Protection Switching Functionality on page 4
- Configuring Ethernet Ring Protection Switching on page 11
- Junos® OS Ethernet Interfaces

CHAPTER 3

Network Interfaces Configuration Statements and Hierarchy

[edit interfaces] Hierarchy Level

The statements at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level can also be configured at the **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]** hierarchy level.

NOTE: The accounting-profile statement is an exception to this rule. The **accounting-profile** statement can be configured at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level, but it cannot be configured at the **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]** hierarchy level.

```
interfaces {
    traceoptions {
        file filename <files number> <match regular-expression> <size size> <world-readable |
            no-world-readable> ;
        flag flag <disable>;
    }
    interface-name {
        accounting-profile name;
        aggregated-ether-options {
            (flow-control | no-flow-control);
            lacp {
                (active | passive);
                link-protection {
                    disable;
                (revertive | non-revertive);
                periodic interval;
                system-priority priority;
            }
            link-protection;
```

```
    link-speed speed;
    (loopback | no-loopback);
    mc-ae{
      chassis-id chassis-id;
      mc-ae-id mc-ae-id;
      mode (active-active | active-standby);
      redundancy-group group-id;
      status-control (active | standby);
    }
    minimum-links number;
    source-address-filter {
      mac-address;
    }
    (source-filtering | no-source-filtering);
  }
  aggregated-sonet-options {
    link-speed speed | mixed;
    minimum-links number;
  }
  atm-options {
    cell-bundle-size cells;
    ilmi;
    linear-red-profiles profile-name {
      high-plp-max-threshold percent;
      low-plp-max-threshold percent;
      queue-depth cells high-plp-threshold percent low-plp-threshold percent;
    }
    mpls {
      pop-all-labels {
        required-depth number;
      }
    }
    pic-type (atm1 | atm2);
    plp-to-clp;
    promiscuous-mode {
      vpi vpi-identifier;
    }
    scheduler-maps map-name {
      forwarding-class class-name {
        epd-threshold cells plp1 cells;
        linear-red-profile profile-name;
        priority (high | low);
        transmit-weight (cells number | percent number);
      }
      vc-cos-mode (alternate | strict);
    }
    use-null-cw;
      vpi vpi-identifier {
      maximum-vcs maximum-vcs;
      oam-liveness {
        down-count cells;
        up-count cells;
      }
      oam-period (seconds | disable);
      shaping {
```

```
            (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
              burst length);
            queue-length number;
          }
        }
      }
      clocking clock-source;
      data-input (system | interface interface-name);
      dce;
      serial-options {
        clock-rate rate;
        clocking-mode (dce | internal | loop);
        control-polarity (negative | positive);
        cts-polarity (negative | positive);
        dcd-polarity (negative | positive);
        dce-options {
          control-signal (assert | de-assert | normal);
          cts (ignore | normal | require);
          dcd (ignore | normal | require);
          dsr (ignore | normal | require);
          dtr signal-handling-option;
          ignore-all;
          indication (ignore | normal | require);
          rts (assert | de-assert | normal);
          tm (ignore | normal | require);
        }
        dsr-polarity (negative | positive);
        dte-options {
          control-signal (assert | de-assert | normal);
          cts (ignore | normal | require);
          dcd (ignore | normal | require);
          dsr (ignore | normal | require);
          dtr signal-handling-option;
          ignore-all;
          indication (ignore | normal | require);
          rts (assert | de-assert | normal);
          tm (ignore | normal | require);
        }
        dtr-circuit (balanced | unbalanced);
        dtr-polarity (negative | positive);
        encoding (nrz | nrzi);
        indication-polarity (negative | positive);
        line-protocol protocol;
        loopback mode;
        rts-polarity (negative | positive);
        tm-polarity (negative | positive);
        transmit-clock invert;
      }
      description text;
      dialer-options {
        pool pool-name <priority priority>;
      }
      disable;
      ds0-options {
        bert-algorithm algorithm;
        bert-error-rate rate;
```

```
    bert-period seconds;
    byte-encoding (nx56 | nx64);
    fcs (16 | 32);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback payload;
    start-end-flag (filler | shared);
  }
  e1-options {
    bert-error-rate rate;
    bert-period seconds;
    fcs (16 | 32);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (local | remote);
    start-end-flag (filler | shared);
    timeslots time-slot-range;
  }
  e3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    framing feet;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (16 | 32);
    framing (g.751 | g.832);
    idle-cycle-flag (filler | shared);
    invert-data;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag (filler | shared);
    (unframed | no-unframed);
  }
  encapsulation type;
  es-options {
    backup-interface es-fpc/pic/port;
  }
  fastether-options {
    802.3ad aex;
    (flow-control | no-flow-control);
    ignore-l3-incompletes;
    ingress-rate-limit rate;
    (loopback | no-loopback);
    mpls {
      pop-all-labels {
        required-depth number;
      }
    }
    source-address-filter {
      mac-address;
    }
    (source-filtering | no-source-filtering);
  }
  flexible-vlan-tagging;
```

```
gigether-options {
  802.3ad ae x;
  (asynchronous-notification | no-asynchronous-notification);
  (auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
    local-interface-offline>;
  auto-reconnect seconds;
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  (loopback | no-loopback);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  no-auto-mdix;
  source-address-filter {
    mac-address;
  }
  (source-filtering | no-source-filtering);
  ethernet-switch-profile {
    (mac-learn-enable | no-mac-learn-enable);
    tag-protocol-id [ tpids ];
    ethernet-policer-profile {
      input-priority-map {
        ieee802.1p premium [ values ];
      }
      output-priority-map {
        classifier {
          premium {
            forwarding-class class-name {
              loss-priority (high | low);
            }
          }
        }
      }
      policer cos-policer-name {
        aggregate {
          bandwidth-limit bps;
          burst-size-limit bytes;
        }
        premium {
          bandwidth-limit bps;
          burst-size-limit bytes;
        }
      }
    }
  }
}
(gratuitous-arp-reply | no-gratuitous-arp-reply);
hold-time up milliseconds down milliseconds;
ima-group-options {
  differential-delay number;
  frame-length (32 | 64 | 128 | 256);
  frame-synchronization {
    alpha number;
    beta number;
```

```
      gamma number;
    }
    minimum-links number;
    symmetry (symmetrical-config-and-operation |
      symmetrical-config-asymmetrical-operation);
    test-procedure {
      ima-test-start;
      ima-test-stop;
      interface name;
      pattern number;
      period number;
    }
    transmit-clock (common | independent);
    version (1.0 |1.1);
  }
  ima-link-options group-id group-id;
  interface-set interface-set-name {
    interface ethernet-interface-name {
      (unit unit-number | vlan-tags-outer vlan-tag);
    }
    interface interface-name {
      (unit unit-number);
    }
  }
  isdn-options {
    bchannel-allocation (ascending | descending);
    calling-number number;
    pool pool-name <priority priority>;
    spid1 spid-string;
    spid2 spid-string;
    static-tei-val value;
    switch-type (att5e | etsi | ni1 | ntdms100 | ntt);
    t310 seconds;
    tei-option (first-call | power-up);
  }
  keepalives <down-count number> <interval seconds> <up-count number>;
  link-mode mode;
  lmi {
    lmi-type (ansi | itu | c-lmi);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
  }
  lsq-failure-options {
    no-termination-request;
    [ trigger-link-failure interface-name ];
  }
  mac mac-address;
  mlfr-uni-nni-bundle-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
```

```
    drop-timeout milliseconds;
    fragment-threshold bytes;
    cisco-interoperability send-lip-remove-link-for-link-reject;
    hello-timer milliseconds;
    link-layer-overhead percent;
    lmi-type (ansi | itu | c-lmi);
    minimum-links number;
    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 seconds;
    t392 seconds;
    yellow-differential-delay milliseconds;
}
modem-options {
    dialin (console | routable);
    init-command-string initialization-command-string;
}
mtu bytes;
multi-chassis-protection {
    peer a.b.c.d {
        interfaceinterface-name;
        }
    }
multiservice-options {
    (core-dump | no-core-dump);
    (syslog | no-syslog);
}
native-vlan-id number;
no-gratuitous-arp-request;
no-keepalives;
no-partition {
    interface-type type;
}
no-vpivci-swapping;
otn-options {
    fec (efec | gfec | none);
    (laser-enable | no-laser-enable);
    (line-loopback | no-line-loopback);
    pass-thru;
    rate (fixed-stuff-bytes | no-fixed-stuff-bytes | pass-thru);
    transmit-payload-type number;
    trigger (oc-lof | oc-lom | oc-los | oc-wavelength-lock | odu-ais | odu-bbe-th | odu-bdi
        | odu-es-th | odu-lck | odu-oci | odu-sd | odu-ses-th | odu-ttim | odu-uas-th |
        opu-ptm | otu-ais | otu-bbe-th | otu-bdi | otu-es-th | otu-fec-deg | otu-fec-exe |
        otu-iae | otu-sd | otu-ses-th | otu-ttim | otu-uas-th);
    tti;
}
optics-options {
    wavelength nm;
    alarm alarm-name {
        (syslog | link-down);
    }
    warning warning-name {
```

```
      (syslog | link-down);
    }
  }
  partition partition-number oc-slice oc-slice-range interface-type type;
  timeslots time-slot-range;
  passive-monitor-mode;
  per-unit-scheduler;
  ppp-options {
    chap {
      access-profile name;
      default-chap-secret name;
      local-name name;
      passive;
    }
    compression {
      acfc;
      pfc;
    }
    dynamic-profile profile-name;
    no-termination-request;
    pap {
      access-profile name;
      local-name name;
      local-password password;
      compression;
    }
  }
  psn-vcipsn-vci-identifier;
  psn-vpipsn-vpi-identifier;
  receive-bucket {
    overflow (discard | tag);
    rate percentage;
    threshold bytes;
  }
  redundancy-options {
    priority sp-fpc/pic/port;
    secondary sp-fpc/pic/port;
    hot-standby;
  }
  satop-options {
    payload-size n;
  }
  schedulers number;
  serial-options {
    clock-rate rate;
    clocking-mode (dce | internal | loop);
    control-polarity (negative | positive);
    cts-polarity (negative | positive);
    dcd-polarity (negative | positive);
    dce-options {
      control-signal (assert | de-assert | normal);
      cts (ignore | normal | require);
      dcd (ignore | normal | require);
      dsr (ignore | normal | require);
      dtr signal-handling-option;
      ignore-all;
```

```
      indication (ignore | normal | require);
      rts (assert | de-assert | normal);
      tm (ignore | normal | require);
    }
    dsr-polarity (negative | positive);
    dte-options {
      control-signal (assert | de-assert | normal);
      cts (ignore | normal | require);
      dcd (ignore | normal | require);
      dsr (ignore | normal | require);
      dtr signal-handling-option;
      ignore-all;
      indication (ignore | normal | require);
      rts (assert | de-assert | normal);
      tm (ignore | normal | require);
    }
    dtr-circuit (balanced | unbalanced);
    dtr-polarity (negative | positive);
    encoding (nrz | nrzi);
    indication-polarity (negative | positive);
    line-protocol protocol;
    loopback mode;
    rts-polarity (negative | positive);
    tm-polarity (negative | positive);
    transmit-clock invert;
  }
  services-options {
    inactivity-timeout seconds;
    open-timeout seconds;
    session-limit {
      maximum number;
      rate new-sessions-per-second;
      }
      syslog {
      host hostname {
        facility-override facility-name;
        log-prefix prefix-number;
        services priority-level;
      }
    }
  }
  shdsl-options {
    annex (annex-a | annex-b);
    line-rate line-rate;
    loopback (local | remote);
    snr-margin {
      current margin;
      snext margin;
    }
  }
  sonet-options {
    aggregate asx;
    aps {
      advertise-interval milliseconds;
      annex-b;
      authentication-key key;
```

```
        fast-aps-switch;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        preserve-interface;
        protect-circuit group-name;
        request;
        revert-time seconds;
        switching-mode (bidirectional | unidirectional);
        working-circuit group-name;
    }
    bytes {
        c2 value;
        e1-quiet value;
        f1 value;
        f2 value;
        s1 value;
        z3 value;
        z4 value;
    }
    fcs (16 | 32);
    loopback (local | remote);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    path-trace trace-string;
    (payload-scrambler | no-payload-scrambler);
    rfc-2615;
    trigger {
        defect ignore;
        hold-time up milliseconds down milliseconds;
    }
    vtmapping (itu-t | klm);
    (z0-increment | no-z0-increment);
}
speed (10m | 100m | 1g | oc3 | oc12 | oc48);
stacked-vlan-tagging;
switch-options {
    switch-port port-number {
        (auto-negotiation | no-auto-negotiation);
        speed (10m | 100m | 1g);
        link-mode (full-duplex | half-duplex);
    }
}
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout value;
    byte-encoding (nx56 | nx64);
    crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);
    crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);
```

```
    fcs (16 | 32);
    framing (esf | sf);
    idle-cycle-flag (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
    start-end-flag (filler | shared);
    timeslots time-slot-range;
  }
  t3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout feet;
    (cbit-parity | no-cbit-parity);
    compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate
      value>;
    fcs (16 | 32);
    (feac-loop-respond | no-feac-loop-respond);
    idle-cycle-flag value;
    (long-buildout | no-long-buildout);
    (loop-timing | no-loop-timing);
    loopback (local | payload | remote);
    (mac | no-mac);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag (filler | shared);
  }
  traceoptions {
    flag flag <flag-modifier> <disable>;
  }
  transmit-bucket {
    overflow discard;
    rate percentage;
    threshold bytes;
  }
  (traps | no-traps);
  unidirectional;
  vlan-tagging;
  vlan-vci-tagging;
  unit logical-unit-number {
    accept-source-mac {
      mac-address mac-address {
        policer {
          input cos-policer-name;
          output cos-policer-name;
        }
      }
    }
    accounting-profile name;
    advisory-options {
      downstream-rate rate;
      upstream-rate rate;
    }
    allow-any-vci;
```

```
atm-scheduler-map (map-name | default);
backup-options {
  interface interface-name;
}
bandwidth rate;
cell-bundle-size cells;
clear-dont-fragment-bit;
compression {
  rtp {
    f-max-period number;
    maximum-contexts number <force>;
    queues [ queue-numbers ];
    port {
      minimum port-number;
      maximum port-number;
    }
  }
}
compression-device interface-name;
copy-tos-to-outer-ip-header;
demux-destination family;
demux-source family;
demux-options {
  underlying-interface interface-name;
}
description text;
interface {
  l2tp-interface-id name;
  (dedicated | shared);
}
dialer-options {
  activation-delay seconds;
  callback;
  callback-wait-period time;
  deactivation-delay seconds;
  dial-string [ dial-string-numbers ];
  idle-timeout seconds;
  incoming-map {
    caller (caller-id | accept-all);
    initial-route-check seconds;
    load-interval seconds;
    load-threshold percent;
    pool pool-name;
    redial-delay time;
    watch-list {
      [ routes ];
    }
  }
}
disable;
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
  activation-priority priority;
  bearer-bandwidth-limit kilobits-per-second;
```

```
}
encapsulation type;
epd-threshold cells plp1 cells;
fragment-threshold bytes;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {
   (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
   inner-tag-protocol-id tpid;
   inner-vlan-id number;
   tag-protocol-id tpid;
   vlan-id number;
}
interleave-fragments;
inverse-arp;
layer2-policer {
   input-policer policer-name;
   input-three-color policer-name;
   output-policer policer-name;
   output-three-color policer-name;
}
link-layer-overhead percent;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multilink-max-classes number;
multipoint;
oam-liveness {
   down-count cells;
   up-count cells;
}
oam-period (seconds | disable);
output-vlan-map {
   (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
   inner-tag-protocol-id tpid;
   inner-vlan-id number;
   tag-protocol-id tpid;
   vlan-id number;
}
passive-monitor-mode;
peer-unit unit-number;
plp-to-clp;
point-to-point;
ppp-options {
   chap {
      access-profile name;
      default-chap-secret name;
      local-name name;
      passive;
   }
   compression {
      acfc;
      pfc;
      pap;
      default-pap-password password;
      local-name name;
```

```
      local-password password;
      passive;
    }
    dynamic-profile profile-name;
    lcp-max-conf-req number;
    lcp-restart-timer milliseconds;
    loopback-clear-timer seconds;
    ncp-max-conf-req number;
    ncp-restart-timer milliseconds;
  }
  pppoe-options {
    access-concentrator name;
    auto-reconnect seconds;
    (client | server);
    service-name name;
    underlying-interface interface-name;
  }
  proxy-arp;
  service-domain (inside | outside);
  shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
      burst length);
    queue-length number;
  }
  short-sequence;
  transmit-weight number;
  (traps | no-traps);
  trunk-bandwidth rate;
  trunk-id number;
  tunnel {
    backup-destination address;
    destination address;
    key number;
    routing-instance {
      destination routing-instance-name;
    }
    source source-address;
    ttl number;
  }
  vci vpi-identifier.vci-identifier;
  vci-range start start-vci end end-vci;
  vpi vpi-identifier;
  vlan-id number;
  vlan-id-list [vlan-id vlan-id–vlan-id];
  vlan-id-range number-number;
  vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
  vlan-tags-outer tpid.vlan-id inner-list [vlan-id vlan-id–vlan-id];
  family family {
    accounting {
      destination-class-usage;
      source-class-usage {
        direction;
      }
    }
    access-concentrator name;
    address address {
```

```
    destination address;
}
bundle ml-fpc/pic/port | ls-fpc/pic/port);
duplicate-protection;
dynamic-profile profile-name;
filter {
    group filter-group-number;
    input filter-name;
    input-list {
        [ filter-names ];
        output filter-name;
    }
    output-list {
        [ filter-names ];
    }
}
ipsec-sa sa-name;
keep-address-and-control;
max-sessions number;
max-sessions-vsa-ignore;
mtu bytes;
multicast-only;
negotiate-address;
no-redirects;
policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}
primary;
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check {
    fail-filter filter-name;
    mode loose;
}
sampling {
    direction;
}
service {
    input {
        service-set service-set-name <service-filter filter-name>;
        post-service-filter filter-name;
    }
    output {
        service-set service-set-names <service-filter filter-name>;
    }
}
service-name-table table-name;
short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
    maximum-seconds>;
targeted-broadcast {
    forward-and-send-to-re;
    forward-only;
```

```
        }
        (translate-discard-eligible | no-translate-discard-eligible);
        (translate-fecn-and-becn | no-translate-fecn-and-becn);
        translate-plp-control-word-de;
        unnumbered-address interface-name <destination address destination-profile
          profile-name | preferred-source-address address>;
        address address {
          arp ip-address (mac | multicast-mac) mac-address <publish>;
          broadcast address;
          destination address;
          destination-profile name;
          eui-64;
          multipoint-destination address (dlci dlci-identifier | vci vci-identifier);
          multipoint-destination address {
            epd-threshold cells plp1 cells;
            inverse-arp;
            oam-liveness {
              up-count cells;
              down-count cells;
            }
            oam-period (seconds | disable);
            shaping {
              (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained
                rate burst length);
              queue-length number;
            }
            vci vpi-identifier.vci-identifier;
          }
          preferred;
          primary;
          (vrrp-group | vrrp-inet6-group) group-number {
            (accept-data | no-accept-data);
            advertise–interval seconds;
            authentication-type authentication;
            authentication-key key;
            fast-interval milliseconds;
            (preempt | no-preempt) {
              hold-time seconds;
            }
            priority-number number;
            track {
              priority-cost seconds;
              priority-hold-time interface-name {
                bandwidth-threshold bits-per-second {
                  priority;
                }
                interface priority;
              }
              route ip-address/mask routing-instance instance-name priority-cost cost;
            }
            virtual-address [ addresses ];
          }
        }
      }
    }
  }
```

```
}
```

Related Documentation

- *Junos OS Hierarchy and RFC Reference*
- Junos® OS Ethernet Interfaces
- Junos® OS Network Interfaces

[edit logical-systems] Hierarchy Level

The following lists the statements that can be configured at the **[edit logical-systems]** hierarchy level that are also documented in this manual. For more information about logical systems, see the Logical Systems Configuration Guide.

```
logical-systems logical-system-name {
  interfaces interface-name {
    unit logical-unit-number {
      accept-source-mac {
        mac-address mac-address {
          policer {
            input cos-policer-name;
            output cos-policer-name;
          }
        }
      }
      allow-any-vci;
      atm-scheduler-map (map-name | default);
      bandwidth rate;
      backup-options {
        interface interface-name;
      }
      cell-bundle-size cells;
      clear-dont-fragment-bit;
      compression {
        rtp {
          f-max-period number;
          port {
            minimum port-number;
            maximum port-number;
          }
          queues [ queue-numbers ];
        }
      }
      compression-device interface-name;
      description text;
      interface {
        l2tp-interface-id name;
        (dedicated | shared);
      }
      dialer-options {
        activation-delay seconds;
        deactivation-delay seconds;
        dial-string [ dial-string-numbers ];
        idle-timeout seconds;
        initial-route-check seconds;
```

```
    load-threshold number;
    pool pool;
    remote-name remote-callers;
    watch-list {
      [ routes ];
    }
  }
  disable;
  dlci dlci-identifier;
  drop-timeout milliseconds;
  dynamic-call-admission-control {
    activation-priority priority;
    bearer-bandwidth-limit kilobits-per-second;
  }
  encapsulation type;
  epd-threshold cells plp1 cells;
  fragment-threshold bytes;
  input-vlan-map {
    inner-tag-protocol-id;
    inner-vlan-id;
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-push | swap-swap);
    tag-protocol-id tpid;
    vlan-id number;
  }
  interleave-fragments;
  inverse-arp;
  layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    output-three-color policer-name;
  }
  link-layer-overhead percent;
  minimum-links number;
  mrru bytes;
  multicast-dlci dlci-identifier;
  multicast-vci vpi-identifier.vci-identifier;
  multilink-max-classes number;
  multipoint;
  oam-liveness {
    up-count cells;
    down-count cells;
  }
  oam-period (seconds | disable);
  output-vlan-map {
    inner-tag-protocol-id;
    inner-vlan-id;
    (pop | pop-pop | pop-swap | push | push-push | swap | swap-swap);
    tag-protocol-id tpid;
    vlan-id number;
  }
  passive-monitor-mode;
  peer-unit unit-number;
  plp-to-clp;
  point-to-point;
  ppp-options {
```

```
    chap {
      access-profile name;
      default-chap-secret name;
      local-name name;
      passive;
    }
    compression {
      acfc;
      pfc;
      }
    }
    dynamic-profile profile-name;
    pap {
      default-pap-password password;
      local-name name;
      local-password password;
      passive;
    }
  }
  proxy-arp;
  service-domain (inside | outside);
  shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
      burst length);
    queue-length number;
  }
  short-sequence;
  transmit-weight number;
  (traps | no-traps);
  trunk-bandwidth rate;
  trunk-id number;
  tunnel {
    backup-destination address;
    destination address;
    key number;
    routing-instance {
      destination routing-instance-name;
    }
    source source-address;
    ttl number;
  }
  vci vpi-identifier.vci-identifier;
  vlan-id number;
  vlan-id-list [vlan-id vlan-id–vlan-id]
  vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
  vlan-tags outer tpid.vlan-id inner-list [vlan-id vlan-id–vlan-id]
  vpi vpi-identifier;
  family family {
    accounting {
      destination-class-usage;
      source-class-usage {
        direction;
      }
    }
    bundle interface-name;
    filter {
```

```
    group filter-group-number;
    input filter-name;
    input-list {
      [ filter-names ];
    }
    output filter-name;
    output-list {
      [ filter-names ];
    }
  }
  ipsec-sa sa-name;
  keep-address-and-control;
  mtu bytes;
  multicast-only;
  no-redirects;
  policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
  }
  primary;
  proxy inet-address address;
  receive-options-packets;
  receive-ttl-exceeded;
  remote (inet-address address | mac-address address);
  rpf-check <fail-filter filter-name> {
    <mode loose>;
  }
  sampling {
    direction;
  }
  service {
    input {
      service-set service-set-name <service-filter filter-name>;
      post-service-filter filter-name;
    }
    output {
      service-set service-set-name <service-filter filter-name>;
    }
  }
  (translate-discard-eligible | no-translate-discard-eligible);
  (translate-fecn-and-becn | no-translate-fecn-and-becn);
  unnumbered-address interface-name destination address destination-profile
    profile-name;
  address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    multipoint-destination address (dlci dlci-identifier | vci vci-identifier);
    multipoint-destination address {
      epd-threshold cells plp1 cells;
      inverse-arp;
      oam-liveness {
        up-count cells;
```

```
            down-count cells;
          }
          oam-period (seconds | disable);
          shaping {
            (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained
              rate burst length);
            queue-length number;
          }
          vci vpi-identifier.vci-identifier;
        }
        preferred;
        primary;
        (vrrp-group | vrrp-inet6-group) group-number {
          (accept-data | no-accept-data);
          advertise–interval seconds;
          authentication-type authentication;
          authentication-key key;
          fast-interval milliseconds;
          (preempt | no-preempt) {
            hold-time seconds;
          }
          priority-number number;
          track {
            priority-cost seconds;
            priority-hold-time interface-name {
              interface priority;
              bandwidth-threshold bits-per-second {
                priority;
              }
            }
            route ip-address/mask routing-instance instance-name priority-cost cost;
          }
        }
        virtual-address [ addresses ];
      }
    }
  }
}
```

Related Documentation

- *Junos OS Hierarchy and RFC Reference*
- Junos® OS Ethernet Interfaces
- Junos® OS Network Interfaces

[edit protocols protection-group] Hierarchy Level

```
ethernet-ringring-name {
  east-interface {
    control-channel channel-name {
      vlan number;
    }
  }
  guard-interval number;
```

```
    node-id mac-address;
    restore-interval number;
    ring-protection-link-owner;
    west-interface {
      control-channel channel-name {
        vlan number;
      }
    }
  }
```

Related Documentation

- *Junos OS Hierarchy and RFC Reference*
- Junos® OS Ethernet Interfaces
- Junos® OS Network Interfaces

CHAPTER 4

Statement Summary

control-channel

Syntax

```
control-channel channel-name {
    vlan vlan-id;
}
```

Hierarchy Level [edit protocols protection-group ethernet-ring *name* (east-interface | west-interface)]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure the Ethernet RPS control channel logical interface to carry the RAPS PDU. The related physical interface is the physical ring port.

Options

vlan ***vlan-id***—If the control channel logical interface is a trunk port, then a dedicated **vlan** ***vlan-id*** defines the dedicated VLAN channel to carry the RAPS traffic. Only configure the ***vlan-id*** when the control channel logical interface is the trunk port.

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

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

data-channel

Syntax

```
data-channel {
  vlan number;
}
```

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name*]

Release Information Statement introduced in Junos OS Release 10.2.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description For Ethernet ring protection, configure a data channel to define a set of VLAN IDs that belong to a ring instance.

VLANs specified in the data channel use the same topology used by the ERPS PDU in the control channel. Therefore, if a ring interface is blocked in the control channel, all traffic in the data channel is also blocked on that interface.

Options **vlan *number***—Specify (by VLAN ID) one or more VLANs that belong to a ring instance.

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

Related Documentation

- Ethernet Ring Protection Using Ring Instances for Load Balancing
- Example: Configuring Load Balancing Within Ethernet Ring Protection for MX Series Routers
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

east-interface

Syntax

```
east-interface {
  node-id mac-address;
  control-channel channel-name {
  interface-none
  ring-protection-link-end;
}
```

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name*]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Define one of the two interface ports for Ethernet ring protection, the other being defined by the **west-interface** statement at the same hierarchy level. The interface must use the control channel's logical interface name. The control channel is a dedicated VLAN channel for the ring port.

EX Series switches do not use the node-id statement--the node ID is automatically configured on the switches using the MAC address.

NOTE: **Always configure this port first, before configuring the west-interface statement.**

NOTE: **The Node ID is not configurable on EX Series switches. The node ID is automatically configured using the MAC address.**

The statements are explained separately.

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

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- west-interface on page 54
- ethernet-ring on page 46
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

ethernet-ring

Syntax

```
ethernet-ring ring-name {
  control-vlan (vlan-id | vlan-name);
  data-channel {
    vlan number
  }
  east-interface {
    control-channel channel-name {
      vlan number;
    }
  }
  guard-interval number;
  node-id mac-address;
  restore-interval number;
  ring-protection-link-owner;
  west-interface {
    control-channel channel-name {
      vlan number;
    }
  }
}
```

Hierarchy Level [edit protocols protection-group]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description For Ethernet PICs on MX Series routers or for EX Series switches, , specify the Ethernet ring in an Ethernet ring protection switching configuration.

Options *ring-name*—Name of the Ethernet protection ring.

The remaining statements are explained separately.

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

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

fast-aps-switch

Syntax fast-aps-switch;

Hierarchy Level [edit interfaces *interface-name* sonet-options aps]

Release Information Statement introduced in Junos OS Release 12.1.

Description (M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only) Reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits.

NOTE:

- Configuring this statement reduces the APS switchover time only when the Layer 2 circuit encapsulation type for the interface receiving traffic from a Layer 2 circuit neighbor is SAToP.
- When the **fast-aps-switch** statement is configured in revertive APS mode, you must configure an appropriate value for revert time to achieve reduction in APS switchover time.
- To prevent the logical interfaces in the data path from being shut down, configure appropriate hold-time values on all the interfaces in the data path that support TDM.
- The **fast-aps-switch** statement cannot be configured when the APS **annex-b** option is configured.
- The interfaces that have the **fast-aps-switch** statement configured cannot be used in virtual private LAN service (VPLS) environments.

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

Related Documentation
- Reducing APS Switchover Time in Layer 2 Circuits

guard-interval

Syntax guard-interval *number*;

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name*]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description When a link goes down, the ring protection link (RPL) activates. When the downed link comes back up, the RPL link receives notification, restores the link, and waits for the restore interval before issuing another block on the same link. This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

Options *number*—Guard timer interval, in milliseconds.
Range: 10 through 2000 ms
Default: 500 ms

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

Related Documentation
- Ethernet Ring Protection Switching Overview on page 3
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

hold-interval (Protection Group)

Syntax hold-interval *number*;

Hierarchy Level [edit protocols protection-group ethernet-ring *name*]

Release Information Statement introduced in Junos OS Release 9.4.

Description Specify the hold-off timer interval *for all rings* in 100 millisecond (ms) increments.

Options *number*—Hold-timer interval, in milliseconds.
Range: 0 through 10,000 ms
Default: 100 ms

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

Related Documentation
- Ethernet Ring Protection Switching Overview on page 3

node-id

Syntax node-id *mac-address*;

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name*]

Release Information Statement introduced in Junos OS Release 9.4.

Description For EX Series switches, node-id is not configurable.

For MX Series routers, optionally specify the MAC address of a node in the protection group. If this statement is not included, the router assigns the node's MAC address.

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

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3

protection-group

Syntax

```
protection-group {
    ethernet-ringring-name {
      control-vlan (vlan-id | vlan-name);
      data-channel {
        vlan number
      }
      east-interface {
        control-channel channel-name {
          vlan number;
        }
      }
      guard-interval number;
      node-id mac-address;
      restore-interval number;
      ring-protection-link-owner;
      west-interface {
        control-channel channel-name {
          vlan number;
        }
      }
    }
  control-vlan (vlan-id | vlan-name);
      east-interface {
        node-id mac-address;
        control-channel channel-name {
        interface-none
        ring-protection-link-end;
      }
    }
      control-channel channel-name {
        vlan number;
      }
    }
    data-channel {
      vlan number
    }
    guard-interval number;
    node-id mac-address;
    restore-interval number;
    ring-protection-link-owner;
      west-interface {
        node-id mac-address;
        control-channel channel-name {
        interface-none
        ring-protection-link-end;
      }
      control-channel channel-name {
        vlan number;
      }
    }
  }
  guard-interval number;
```

```
    restore-interval number;
    traceoptions {
      file filename <no-stamp> <world-readable | no-world-readable> <replace> <size size>;
      flag flag;
    }
}
```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure Ethernet ring protection switching.

The statements are explained separately. All statements apply to MX Series routers. EX Series switches do not assign **node-id** and use **control-vlan** instead of **control-channel**.

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

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- Example: Configuring Load Balancing Within Ethernet Ring Protection for MX Series Routers
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

restore-interval

Syntax restore-interval *number*;

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name*]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configures the number of minutes that the node does not process any Ethernet ring protection (ERP) protocol data units (PDUs).. This configuration is a global configuration and applies to all Ethernet rings if the Ethernet ring does not have a more specific configuration for this value. If no parameter is configured at the protection group level, the global configuration of this parameter uses the default value.

Options *number*—Specify the restore interval.
Range: 5 through 12 minutes

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

Related Documentation
- Ethernet Ring Protection Switching Overview on page 3
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

ring-protection-link-end

Syntax ring-protection-link-end;

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name* (east-interface | west-interface)]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Specify that the port is one side of a ring protection link (RPL) by setting the RPL end flag.

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

Related Documentation
- Ethernet Ring Protection Switching Overview on page 3
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

ring-protection-link-owner

Syntax ring-protection-link-owner;

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name*]

Release Information Statement introduced in Junos OS Release 9.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Specify the ring protection link (RPL) owner flag in the Ethernet protection ring. Include this statement only once for each ring (only one node can function as the RPL owner).

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

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3

west-interface

Syntax

```
west-interface {
  node-id mac-address;
  control-channel channel-name {
  interface-none
  ring-protection-link-end;
}
```

Hierarchy Level [edit protocols protection-group ethernet-ring *ring-name*]

Release Information Statement introduced in Junos OS Release 9.5.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Define one of the two interface ports for Ethernet ring protection, the other being defined by the **east-interface** statement at the same hierarchy level. The interface must use the control channel's logical interface name. The control channel is a dedicated VLAN channel for the ring port.

NOTE: **Always configure this port second, after configuring the east-interface statement.**

The statements are explained separately.

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

Related Documentation

- Ethernet Ring Protection Switching Overview on page 3
- Ethernet Ring Protection Using Ring Instances for Load Balancing
- east-interface on page 45
- ethernet-ring on page 46
- Example: Configuring Ethernet Ring Protection Switching on EX Series Switches
- Configuring Ethernet Ring Protection Switching (CLI Procedure)

PART 3

Administration

CHAPTER 5

Monitoring Commands

show protection-group ethernet-ring aps

Syntax **show protection-group ethernet-ring aps**

Release Information Command introduced in Junos OS Release 9.4.
Command introduced in Junos OS Release 12.1 for EX Series switches.

Description Display the status of the Automatic Protection Switching (APS) and Ring APS (RAPS) messages on an Ethernet ring.

Options This command has no options.

Required Privilege Level view

Related Documentation

- show protection-group ethernet-ring data-channel on page 60
- show protection-group ethernet-ring interface on page 62
- show protection-group ethernet-ring node-state on page 65
- show protection-group ethernet-ring statistics on page 68
- show protection-group ethernet-ring vlan on page 71

List of Sample Output

show protection-group ethernet-ring aps (EX Switches) on page 59
show protection-group ethernet-ring aps (Owner Node, Normal Operation on MX Routers) on page 59
show protection-group ethernet-ring aps (Ring Node, Normal Operation on MX Routers) on page 59
show protection-group ethernet-ring aps (Owner Node, Failure Condition on MX Routers) on page 59
show protection-group ethernet-ring aps (Ring Node, Failure Condition on MX Routers) on page 59

Output Fields Table 3 on page 58 lists the output fields for the **show protection-group ethernet-ring aps** command. Output fields are listed in the approximate order in which they appear.

Table 3: show protection-group ethernet-ring aps Output Fields

Field Name	Field Description
Ethernet Ring Name	Name configured for the Ethernet ring.
Request/State	Status of the Ethernet ring RAPS messages. • **NR**—Indicates there is no request for APS on the ring. • **SF**—Indicates there is a signal failure on the ring.
No Flush	State of the ring flushing: **No** (normal) or **Yes** (failure).
Ring Protection Link Blocked	Blocking on the ring protection link: **Yes** or **No**.

Table 3: show protection-group ethernet-ring aps Output Fields *(continued)*

Field Name	Field Description
Originator	Whether this node is the ring originator: **Yes** or **No**.
Remote Node ID	Identifier (in MAC address format) of the remote node.

Sample Output

show protection-group ethernet-ring aps (EX Switches)

```
user@switch>> show protection-group ethernet-ring aps
Ring Name    Request/state  No Flush  RPL Blocked  Originator  Remote Node ID
erp1         NR             no        yes          no          00:1F:12:30:B8:81
```

Sample Output

show protection-group ethernet-ring aps (Owner Node, Normal Operation on MX Routers)

```
user@host> show protection-group ethernet-ring aps
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg101               NR             No        Yes

Originator  Remote Node ID
Yes
```

show protection-group ethernet-ring aps (Ring Node, Normal Operation on MX Routers)

```
user@host> show protection-group ethernet-ring aps
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg102               NR             No        Yes

Originator  Remote Node ID
No          00:01:01:00:00:01
```

show protection-group ethernet-ring aps (Owner Node, Failure Condition on MX Routers)

```
user@host> show protection-group ethernet-ring aps
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg101               SF             No        No

Originator  Remote Node ID
No          00:01:02:00:00:01
```

show protection-group ethernet-ring aps (Ring Node, Failure Condition on MX Routers)

```
user@host> show protection-group ethernet-ring aps
Ethernet Ring Name  Request/state  No Flush  Ring Protection Link Blocked
pg102               SF             No        Yes

Originator  Remote Node ID
Yes         00:00:00:00:00:00
```

show protection-group ethernet-ring data-channel

Syntax

show protection-group ethernet-ring data-channel
<brief | detail>
<group-name *group-name*>

Release Information

Command introduced in Junos OS Release 10.2.

Description

On MX Series routers, display data channel information for all Ethernet ring protection groups or for a specific Ethernet ring protection group.

Options

brief | detail—(Optional) Display the specified level of output.

group-name—(Optional) Protection group for which to display statistics. If you omit this optional field, all protection group statistics for configured groups will be displayed.

Required Privilege Level

view

Related Documentation

- show protection-group ethernet-ring aps on page 58
- show protection-group ethernet-ring interface on page 62
- show protection-group ethernet-ring node-state on page 65
- show protection-group ethernet-ring statistics on page 68
- show protection-group ethernet-ring vlan on page 71

List of Sample Output

show protection-group ethernet-ring data-channel on page 61

Output Fields

Table 4 on page 60 lists the output fields for the **show protection-group ethernet-ring data-channel** command. Output fields are listed in the approximate order in which they appear.

Table 4: show protection-group ethernet-ring data-channel Output Fields

Field Name	Field Description
Interface	Name of the interface configured for the Ethernet ring.
STP index	The Spanning Tree Protocol (STP) index number used by each interface in an Ethernet ring. The STP index controls the forwarding behavior for a set of VLANs on a data channel on an Ethernet ring port. For multiple Ethernet ring instances on an physical ring port, there are multiple STP index numbers. Different ring instances will have different STP index numbers and may have different forwarding behavior.
Forward State	Forwarding state on the Ethernet ring. • **fowarding**—Indicates packets are being forwarded. • **discarding**—Indicates packets are being discarded.

Sample Output

show protection-group ethernet-ring data-channel

```
user@host> show protection-group ethernet-ring data-channel
Ethernet ring data channel information for protection group pg301
Interface    STP index        Forward State
ge-1/0/3     71               forwarding
ge-1/0/4     82               forwarding

Ethernet ring data channel information for protection group pg302
Interface    STP index        Forward State
ge-1/0/3     52               forwarding
ge-1/0/4     91               forwarding
```

show protection-group ethernet-ring interface

Syntax **show protection-group ethernet-ring interface**

Release Information Command introduced in Junos OS Release 9.4.

Description Displays the status of the Automatic Protection Switching (APS) interfaces on an Ethernet ring.

Options This command has no options.

Required Privilege Level view

Related Documentation

- show protection-group ethernet-ring data-channel on page 60
- show protection-group ethernet-ring aps on page 58
- show protection-group ethernet-ring node-state on page 65
- show protection-group ethernet-ring statistics on page 68
- show protection-group ethernet-ring vlan on page 71

List of Sample Output

show protection-group ethernet-ring interface (EX Series Switch Owner Node) on page 63
show protection-group ethernet-ring interface (Owner Node MX Series Router) on page 63
show protection-group ethernet-ring interface (EX Series Switch Ring Node) on page 63
show protection-group ethernet-ring interface (MX Series Router Ring Node) on page 63

Output Fields Table 5 on page 62 lists the output fields for both the EX Series switch and the MX Series router **show protection-group ethernet-ring interface** commands. Output fields are listed in the approximate order in which they appear.

Table 5: MX Series Routers show protection-group ethernet-ring interface Output Fields

Field Name	Field Description
Ethernet ring port parameters for protection group *group-name*	Output is organized by configured protection group.
Interface	Physical interfaces configured for the Ethernet ring.
Control Channel	(MX Series router only) Logical unit configured on the physical interface. • **NR**—Indicates there is no request for APS on the ring. • **SF**—Indicates there is a signal failure on the ring.
Forward State	State of the ring forwarding on the interface: **discarding** or **forwarding**.

Table 5: MX Series Routers show protection-group ethernet-ring interface Output Fields *(continued)*

Field Name	Field Description
Ring Protection Link End	Whether this interface is the end of the ring: **Yes** or **No**.
Signal Failure	Whether there a signal failure exists on the link: **Clear** or **Set**.
Admin State	State of the interface: For EX switches, **ready**, **ifl ready**, or **waiting**. For MX routers, **IFF ready** or **IFF disabled**.

Sample Output

show protection-group ethernet-ring interface (EX Series Switch Owner Node)

```
user@host> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg101

Interface      Forward State  RPL End  Signal Failure  Admin State

ge-0/0/3.0     discarding     Yes        Clear          ready
ge-0/0/9.0     forwarding     No         Clear          ready
```

show protection-group ethernet-ring interface (Owner Node MX Series Router)

```
user@host> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg101

Interface    Control Channel  Forward State  Ring Protection Link End
ge-1/0/1     ge-1/0/1.1       discarding     Yes
ge-1/2/4     ge-1/2/4.1       forwarding     No

Signal Failure  Admin State
Clear          IFF ready
Clear          IFF ready
```

show protection-group ethernet-ring interface (EX Series Switch Ring Node)

```
user@host> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg102

Ethernet ring port parameters for protection group pg101

Interface      Forward State  RPL End  Signal Failure  Admin State

ge-0/0/3.0     discarding     Yes        Clear          ready
ge-0/0/9.0     forwarding     No         Clear          ready
```

show protection-group ethernet-ring interface

```
user@host> show protection-group ethernet-ring interface
Ethernet ring port parameters for protection group pg102
```

(MX Series Router Ring Node)

```
Interface    Control Channel  Forward State  Ring Protection Link End
ge-1/2/1     ge-1/2/1.1       forwarding     No
ge-1/0/2     ge-1/0/2.1       forwarding     No

Signal Failure  Admin State
Clear          IFF ready
Clear          IFF ready
```

show protection-group ethernet-ring node-state

Syntax **show protection-group ethernet-ring node-state**

Release Information Command introduced in Junos OS Release 9.4.
Command introduced in Junos OS Release 12.1 for EX Series switches.

Description Display the status of the Automatic Protection Switching (APS) nodes on an Ethernet ring.

Options This command has no options.

Required Privilege Level view

Related Documentation

- show protection-group ethernet-ring data-channel on page 60
- show protection-group ethernet-ring aps on page 58
- show protection-group ethernet-ring interface on page 62
- show protection-group ethernet-ring statistics on page 68
- show protection-group ethernet-ring vlan on page 71

List of Sample Output

show protection-group ethernet-ring node-state (EX Series Switch) on page 66
show protection-group ethernet-ring node-state (Owner Node, Normal Operation on MX Series Router) on page 66
show protection-group ethernet-ring node-state (Ring Node, Normal Operation on MX Series Router) on page 66
show protection-group ethernet-ring node-state (Owner Node, Failure Condition on MX Series Router) on page 66
show protection-group ethernet-ring node-state (Ring Node, Failure Condition on MX Series Router) on page 66

Output Fields Table 6 on page 65 lists the output fields for the **show protection-group ethernet-ring node-state** command. Output fields are listed in the approximate order in which they appear.

Table 6: show protection-group ethernet-ring node-state Output Fields

Field Name	Field Description
Ring Name	Name configured for the Ethernet ring.
APS State	State of the Ethernet ring APS. • **idle**—Indicates there is no APS on the ring. • **protected**—Indicates there is a protection switch on the ring.

Table 6: show protection-group ethernet-ring node-state Output Fields *(continued)*

Field Name	Field Description
Event	Events on the ring. • **NR-RB**—Indicates there is no APS request and the ring link is blocked on the ring owner node. • **NR**—Indicates there is no APS request on the ring non-owner nodes. • **SF**—Indicates there is signal failure on a node link.
Ring Protection Link Owner	Whether this node is the ring owner: **Yes** or **No**.
Restore Timer (WTR Timer)	Restoration timer: **Enabled** or **Disabled**.
Guard Timer	Guard timer: **Enabled** or **Disabled**.
Operational State	State of the node: **Operational** or **Non-operational**.

Sample Output

show protection-group ethernet-ring node-state (EX Series Switch)

```
user@switch> show protection-group ethernet-ring node-state
Ring Name APS State Event RPL Owner WTR Timer Guard Timer Op State
erp1   idle      NR-RB    yes    disabled     disabled         operational
```

show protection-group ethernet-ring node-state (Owner Node, Normal Operation on MX Series Router)

```
user@host> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg101            idle         NR-RB         Yes

Restore Timer  Guard Timer  Operation state
disabled       disabled     operational
```

show protection-group ethernet-ring node-state (Ring Node, Normal Operation on MX Series Router)

```
user@host> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg102            idle         NR-RB         No

Restore Timer  Guard Timer  Operation state
disabled       disabled     operational
```

show protection-group ethernet-ring node-state (Owner Node, Failure Condition on MX Series Router)

```
user@host> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg101            protected    SF           Yes

Restore Timer  Guard Timer  Operation state
disabled       disabled     operational
```

show protection-group ethernet-ring

```
user@host> show protection-group ethernet-ring node-state
Ethernet ring    APS State    Event         Ring Protection Link Owner
pg102            idle         NR-RB         No
```

node-state (Ring Node, Failure Condition on MX Series Router)

```
Restore Timer  Quard Timer  Operation state
disabled       disabled     operational
```

show protection-group ethernet-ring statistics

Syntax **show protection-group ethernet-ring statistics <group-name *group-name*>**

Release Information Command introduced in Junos OS Release 9.4.
Command introduced in Junos OS Release 12.1 for EX Series switches.

Description Display statistics regarding Automatic Protection Switching (APS) protection groups on an Ethernet ring.

Options **group-name**—Protection group for which to display statistics. In you omit this optional field, all protection group statistics for configured groups will be displayed.

Required Privilege Level view

Related Documentation

- show protection-group ethernet-ring data-channel on page 60
- show protection-group ethernet-ring aps on page 58
- show protection-group ethernet-ring node-state on page 65
- show protection-group ethernet-ring interface on page 62
- show protection-group ethernet-ring vlan on page 71

List of Sample Output

show protection-group ethernet-ring statistics (EX Switch) on page 69
show protection-group ethernet-ring statistics (Owner Node, Normal Operation on MX Router) on page 69
show protection-group ethernet-ring statistics (Ring Node, Normal Operation on MX Router) on page 69
show protection-group ethernet-ring statistics (Owner Node, Failure Condition on MX Router) on page 69
show protection-group ethernet-ring statisitics (Ring Node, Failure Condition on MX Router) on page 69

Output Fields Table 7 on page 68 lists the output fields for the **show protection-group ethernet-ring statistics** command. Output fields are listed in the approximate order in which they appear.

Table 7: show protection-group ethernet-ring statistics Output Fields

Field Name	Field Description
Ethernet Ring Statistics for PG	Name of the protection group for which statistics are displayed.
RAPS sent	Number of Ring Automatic Protection Switching (RAPS) messages sent. (On MX Series switches only)
RAPS received	Number of RAPS messages received. (On MX Series switches only)

Table 7: show protection-group ethernet-ring statistics Output Fields *(continued)*

Field Name	Field Description
Local SF	Number of times a signal failure (SF) has occurred locally.
Remote SF	Number of times a signal failure (SF) has occurred anywhere else on the ring.
NR event	Number of times a No Request (NR) event has occurred on the ring.
NR-RB event	Number of times a No Request, Ring Blocked (NR-RB) event has occurred on the ring.

Sample Output

show protection-group ethernet-ring statistics (EX Switch)

```
user@switch> show protection-group ethernet-ring statistics
Ring Name Local SF Remote SF NR Event NR-RB Event
erp1       2       1       2        3
```

show protection-group ethernet-ring statistics (Owner Node, Normal Operation on MX Router)

```
user@host> show protection-group ethernet-ring statistics group-name pg101
Ethernet Ring statistics for PG pg101
RAPS sent                       : 1
RAPS received                   : 0
Local SF happened:              : 0
Remote SF happened:             : 0
NR event happened:              : 0
NR-RB event happened:           : 1
```

show protection-group ethernet-ring statistics (Ring Node, Normal Operation on MX Router)

```
user@host> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg102
RAPS sent                       : 0
RAPS received                   : 1
Local SF happened:              : 0
Remote SF happened:             : 0
NR event happened:              : 0
NR-RB event happened:           : 1
```

show protection-group ethernet-ring statistics (Owner Node, Failure Condition on MX Router)

```
user@host> show protection-group ethernet-ring statistics group-name pg101
Ethernet Ring statistics for PG pg101
RAPS sent                       : 1
RAPS received                   : 1
Local SF happened:              : 0
Remote SF happened:             : 1
NR event happened:              : 0
NR-RB event happened:           : 1
```

show protection-group ethernet-ring statisitics (Ring Node, Failure

```
user@host> show protection-group ethernet-ring statistics group-name pg102
Ethernet Ring statistics for PG pg102
RAPS sent                       : 1
RAPS received                   : 1
```

Condition on MX Router)

```
Local SF happened:              : 1
Remote SF happened:             : 0
NR event happened:              : 0
NR-RB event happened:           : 1
```

show protection-group ethernet-ring vlan

Syntax

show protection-group ethernet-ring vlan
<brief | detail>
<group-name *group-name*>

Release Information

Command introduced in Junos OS Release 10.2.

Description

On MX Series routers, display all data channel logical interfaces and the VLAN IDs controlled by a ring instance data channel.

Options

brief | detail—(Optional) Display the specified level of output.

group-name—(Optional) Protection group for which to display statistics. In you omit this optional field, all protection group statistics for configured groups will be displayed.

Required Privilege Level

view

Related Documentation

- show protection-group ethernet-ring aps on page 58
- show protection-group ethernet-ring data-channel on page 60
- show protection-group ethernet-ring interface on page 62
- show protection-group ethernet-ring node-state on page 65
- show protection-group ethernet-ring statistics on page 68

List of Sample Output

show protection-group ethernet-ring vlan on page 72
show protection-group ethernet-ring vlan brief on page 72
show protection-group ethernet-ring vlan detail on page 72
show protection-group ethernet-ring vlan group-name vkm01 on page 72

Output Fields

Table 8 on page 71 lists the output fields for the **show protection-group ethernet-ring vlan** command. Output fields are listed in the approximate order in which they appear.

Table 8: show protection-group ethernet-ring vlan Output Fields

Field Name	Field Description
Interface	Name of the interface configured for the Ethernet protection ring.
Vlan	Name of the VLAN associated with the interface configured for the Ethernet protection ring.
STP index	The Spanning Tree Protocol (STP) index number used by each interface in an Ethernet ring. The STP index controls the forwarding behavior for a set of VLANs on a data channel on an Ethernet ring port. For multiple Ethernet ring instances on an physical ring port, there are multiple STP index numbers. Different ring instances will have different STP index numbers and may have different forwarding behavior.

Table 8: show protection-group ethernet-ring vlan Output Fields *(continued)*

Field Name	Field Description
Bridge Domain	Name of the bridge domain that is associated with the VLAN configured for the Ethernet protection ring.

Sample Output

show protection-group ethernet-ring vlan

```
user@host> show protection-group ethernet-ring vlan
Ethernet ring IFBD parameters for protection group vkm01

Interface    Vlan    STP Index   Bridge Domain
ge-2/0/8     100     130         default-switch/bd100
ge-2/0/4     100     126         default-switch/bd100
```

show protection-group ethernet-ring vlan brief

```
user@host> show protection-group ethernet-ring vlan brief
Ethernet ring IFBD parameters for protection group vkm01

Interface    Vlan    STP Index   Bridge Domain
ge-2/0/8     100     130         default-switch/bd100
ge-2/0/4     100     126         default-switch/bd100
```

show protection-group ethernet-ring vlan detail

```
user@host> show protection-group ethernet-ring vlan detail
Ethernet ring IFBD parameters for protection group vkm01

Interface name                : ge-2/0/8
Vlan                          : 100
STP index                     : 130
Bridge Domain                 : default-switch/bd100
Interface name                : ge-2/0/4
Vlan                          : 100
STP index                     : 126
Bridge Domain                 : default-switch/bd100
```

show protection-group ethernet-ring vlan group-name vkm01

```
user@host> show protection-group ethernet-ring vlan vkm01
Ethernet ring IFBD parameters for protection group vkm01

Interface    Vlan    STP Index   Bridge Domain
ge-2/0/8     100     130         default-switch/bd100
ge-2/0/4     100     126         default-switch/bd100
```

CHAPTER 6

Command Summary

Ethernet Interface Operational Mode Commands

Table 9 on page 73 summarizes the command-line interface (CLI) commands that you can use to monitor and troubleshoot aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces. Commands are listed in alphabetical order.

Table 9: Ethernet Interface Operational Mode Commands

Task	Command
Clear dynamic VLAN interfaces.	clear auto-configuration interfaces
Clear a specified dynamic agent circuit identifier (ACI) interface set configured on the router. You can clear only those ACI interface sets that have no subscriber interface members.	clear auto-configuration interfaces interface-set
Clear Link Aggregation Control Protocol (LACP) statistics.	clear lacp statistics
Clear Link Aggregation Control Protocol (LACP) timeout entries.	clear lacp timeouts
Clear learned MAC addresses from the hardware and MAC database. Static MAC addresses are not cleared.	clear interfaces mac-database
Clear statistics that are collected for every MAC address, including policer statistics, on a given physical or logical interface.	clear interfaces mac-database statistics
Clear statistics that are collected for interface sets.	clear interfaces interface-set statistics
Clear the existing continuity measurement and restart counting the operational uptime.	clear oam ethernet connectivity-fault-management continuity-measurement

Table 9: Ethernet Interface Operational Mode Commands *(continued)*

Task	Command
Clear ITU-T Y.1731 Ethernet frame delay measurement (ETH-DM) delay statistics and ETH-DM frame counts. (MX Series routers)	clear oam ethernet connectivity-fault-management delay-statistics
Clear Operation, Administration, and Management (OAM) and connectivity fault management (CFM) linktrace database information.	clear oam ethernet connectivity-fault-management linktrace path-database
Clear all loss statistics maintained by CFM for a given maintenance domain and maintenance association.	clear oam ethernet connectivity-fault-management loss-statistics
Clear connectivity-fault-management policer statistics.	clear oam ethernet connectivity-fault-management policer
Clear all statistics maintained by CFM. (Routers that support IEEE 802.1ag OAM CFM) In addition, for interfaces that support ITU-T Y.1731 Ethernet frame delay measurement (ETH-DM), also clear any ETH-DM statistics and frame counts for CFM maintenance association end points (MEPs).	clear oam ethernet connectivity-fault-management statistics
Clear Operation, Administration, and Management (OAM) link fault management state information and restart the link discovery process on Ethernet interfaces.	clear oam ethernet link-fault-management state
Clear Operation, Administration, and Management (OAM) statistics link fault management statistics for Ethernet interfaces.	clear oam ethernet link-fault-management statistics
Clear the statistics for all Ethernet ring protection groups or a specific Ethernet ring protection group.	clear protection-group ethernet-ring statistics
Check the reachability of a remote IEEE 802.1ag OAM maintenance association end point (MEP) or maintenance association intermediate point (MIP).	ping ethernet
Manually rebalance the subscribers on an aggregated Ethernet bundle with targeted distribution enabled.	request interface rebalance (Aggregated Ethernet for Subscriber Management)
Manually revert egress traffic from the designated backup link to the designated primary link of an aggregated Ethernet interface for which link protection is enabled, or manually switch egress traffic from the primary link to the backup link.	request interface (revert | switchover) (Aggregated Ethernet Link Protection)
Force LACP link switchover.	request lacp link-switchover

Table 9: Ethernet Interface Operational Mode Commands *(continued)*

Task	Command
Clear the lockout, force switch, manual switch, exercise, and wait-to-restore states.	request protection-group ethernet-aps clear
Test if APS is operating correctly.	request protection-group ethernet-aps exercise
Force traffic to switch from the active path to the alternate path.	request protection-group ethernet-aps force-switch
Lock the protection path, forcing the use of the working path.	request protection-group ethernet-aps lockout
Force traffic to switch from the active path to the alternate path.	request protection-group ethernet-aps manual-switch
Display status information about aggregated Fast Ethernet or Gigabit Ethernet router interfaces.	show interfaces (Aggregated Ethernet)
	show interfaces (far-end-interval)
Display status information about Fast Ethernet interfaces.	show interfaces (Fast Ethernet)
Display status information about the specified Gigabit Ethernet interface.	show interfaces (Gigabit Ethernet)
Display status information about 10-Gigabit Ethernet router interfaces.	show interfaces (10-Gigabit Ethernet)
Display IPv6 interface statistics for IPv6 traffic traversing through the IQ2 and IQ2E PICs on standalone T640 routers and on T640 routers in a TX Matrix or in a TXP Matrix. Display IPv6 interface statistics for IPv6 traffic traversing through the IQ2 PICs on M10i and M120 routers. Display IPv6 interface statistics for IPv6 traffic traversing through the IQ2E PICs on M10i, M120, and M320 routers.	show interfaces extensive
Display information about Gigabit Ethernet or 10-Gigabit Ethernet router interface sets.	show interfaces interface-set (Ethernet Interface Set)
Display information about Gigabit Ethernet or 10-Gigabit Ethernet router interface set queues.	show interfaces interface-set queue
Display the transceiver temperature, laser bias current, laser output power, receive optical power, and related alarms for 10-Gigabit Ethernet dense wavelength-division multiplexing (DWDM) interfaces.	show interfaces diagnostics optics (Gigabit Ethernet, 10-Gigabit Ethernet, and 100 Gigabit Ethernet)

Table 9: Ethernet Interface Operational Mode Commands *(continued)*

Task	Command
Display information about integrated routing and bridging interfaces.	show interfaces irb
Display status information about the distribution of subscribers on different links in an aggregated Ethernet bundle.	show interfaces targeting (Aggregated Ethernet for Subscriber Management)
Display Link Aggregation Control Protocol (LACP) information for aggregated, Fast Ethernet, or Gigabit Ethernet router interfaces.	show lacp interfaces
Display Link Aggregation Control Protocol (LACP) statistics.	show lacp statistics
Display Link Aggregation Control Protocol timeout entries.	show lacp timeouts
Display MAC address information for Gigabit Ethernet router interfaces.	show interfaces mac-database (Gigabit Ethernet)
Display information on a specified interface that is part of a multichassis link aggregation configuration.	show interfaces mc-ae
Display ETH-DM statistics for CFM MEPs. (MX Series routers, Ethernet DPCs).	show oam ethernet connectivity-fault-management delay-statistics
Display IEEE 802.1ag OAM connectivity fault management forwarding state information for Ethernet interfaces.	show oam ethernet connectivity-fault-management forwarding-state
Display OAM connectivity fault management information for Ethernet interfaces. For interfaces that support ETH-DM, also display any ETH-DM frame counts when the **detail** or **extensive** option is included. In all other cases, ETH-DM frame counts are zero.	show oam ethernet connectivity-fault-management interfaces
Display OAM connectivity fault management linktrace path database information.	show oam ethernet connectivity-fault-management linktrace path-database
Display OAM connectivity fault management maintenance association end point (MEP) database information. For interfaces that support ETH-DM, also display any ETH-DM frame counts. In all other cases, ETH-DM frame counts are zero.	show oam ethernet connectivity-fault-management mep-database

Table 9: Ethernet Interface Operational Mode Commands *(continued)*

Task	Command
Display ETH-DM statistics and frame counts for CFM MEPs. (MX Series routers, Ethernet DPCs)	show oam ethernet connectivity-fault-management mep-statistics
Display ETH-LM statistics for on-demand mode only.	show oam ethernet connectivity-fault-management loss-statistics
Display information about maintenance intermediate points (MIPs) for the Ethernet OAM 802.1ag standard for connectivity fault management (CFM).	show oam ethernet connectivity-fault-management mip
Display OAM connectivity fault management path database information for hosts configured with MEP.	show oam ethernet connectivity-fault-management path-database
Displays connectivity-fault-management policer statistics.	show oam ethernet connectivity-fault-management policer
Display OAM Ethernet Virtual Connection (EVC) information for hosts configured with Ethernet Local Management Interface (E-LMI). (MX series only)	show oam ethernet evc
Display OAM fault management statistics for Ethernet interfaces.	show oam ethernet link-fault-management
Display OAM Ethernet Local Management Interface status information for an LMI configured interface. (MX series only)	show oam ethernet lmi
Display OAM Ethernet Local Management Interface statistics for an LMI configured interface. (MX series only)	show oam ethernet lmi statistics
Display protection group Ethernet ring Automatic Protection Switching (APS).	show protection-group ethernet-ring aps
Display data channel information for all Ethernet ring protection groups or for a specific Ethernet ring protection group.	show protection-group ethernet-ring data-channel
Display protection group Ethernet ring interfaces.	show protection-group ethernet-ring interface
Display protection group Ethernet ring nodes.	show protection-group ethernet-ring node-state
Display protection group Ethernet ring statistics.	show protection-group ethernet-ring statistics

Table 9: Ethernet Interface Operational Mode Commands *(continued)*

Task	Command
Display all data channel logical interfaces and the VLAN IDs controlled by a ring instance data channel.	show protection-group ethernet-ring vlan
Trace the path between two Ethernet OAM end points.	traceroute ethernet

PART 4

Troubleshooting

CHAPTER 7

Ethernet

traceroute ethernet

Syntax

traceroute ethernet (*mac-address* | *mep-id*)
maintenance-association *ma-name*
maintenance-domain *md-name*
ttl *value*
<**wait** *seconds*>

Release Information

Command introduced in Junos OS Release 9.0.
mep-id option introduced in Junos OS Release 9.1.

Description

Triggers the linktrace protocol to trace the route between two maintenance points. The result of the traceroute protocol is stored in the path database. To display the path database, use the **show oam ethernet connectivity-fault-management path-database** command.

Before using the traceroute command, you can verify the remote MEP's MAC address using the **show oam ethernet connectivity-fault-management path-database** command.

Options

mac-address—Destination unicast MAC address of the remote maintenance point.

mep-id—MEP identifier of the remote maintenance point. The range of values is 1 through 8191.

maintenance-association ***ma-name***—Specifies an existing maintenance association from the set of configured maintenance associations.

maintenance-domain ***md-name***—Specifies an existing maintenance domain from the set of configured maintenance domains.

ttl ***value***—Number of hops to use in the linktrace request. The range is 1 to 255 hops. The default is 4.

wait ***seconds***—(Optional) Maximum time to wait for a response to the traceroute request. The range is 1 to 255 seconds. The default is 5.

Required Privilege Level

network

List of Sample Output

traceroute ethernet on page 83

Output Fields

Table 10 on page 82 lists the output fields for the **traceroute ethernet** command. Output fields are listed in the approximate order in which they appear.

Table 10: traceroute ethernet Output Fields

Field Name	Field Description
Linktrace to	MAC address of the destination maintenance point.
Interface	Local interface used to send the linktrace message (LTM).

Table 10: traceroute ethernet Output Fields *(continued)*

Field Name	Field Description
Maintenance Domain	Maintenance domain specified in the traceroute command.
Level	Maintenance domain level configured.
Maintenance Association	Maintenance association specified in the traceroute command.
Local Mep	The local maintenance end point identifier.
Transaction Identifier	4-byte identifier maintained by the MEP. Each LTM uses a transaction identifier. The transaction identifier is maintained globally across all Maintenance Domains. Use the transaction identifier to match an incoming linktrace response (LTR), with a previously sent LTM.
Hop	Sequential hop count of the linktrace path.
TTL	Number of hops remaining in the linktrace message. The time to live (TTL) is decremented at each hop.
Source MAC address	MAC address of the 802.1ag maintenance point that is sending the linktrace message.
Next-hop MAC address	MAC address of the 802.1ag node that is the next hop in the LTM path.

Sample Output

traceroute ethernet

```
user@host> traceroute ethernet maintenance-domain md1 maintenance-association ma1
00:90:69:7e:01:ff
Linktrace to 00:01:02:03:04:05, Interface : ge-5/0/0.0
       Maintenance Domain: MD1, Level: 7
       Maintenance Association: MA1, Local Mep: 1

       Hop     TTL      Source MAC address        Next hop MAC address
       Transaction Identifier:100001
       1       63       00:00:aa:aa:aa:aa         00:00:bb:bb:bb:bb
       2       62       00:00:bb:bb:bb:bb         00:00:cc:cc:cc:cc
       3       61       00:00:cc:cc:cc:cc         00:01:02:03:04:05
       4       60       00:01:02:03:04:05         00:00:00:00:00:00
```

CHAPTER 8

Interface Diagnostics

Interface Diagnostics

You can use two diagnostic tools to test the physical layer connections of interfaces: loopback testing and bit error rate test (BERT) testing. Loopback testing enables you to verify the connectivity of a circuit. BERT testing enables you to identify poor signal quality on a circuit. This section contains the following topics:

Configuring Loopback Testing

Loopback testing allows you to verify the connectivity of a circuit. You can configure any of the following interfaces to execute a loopback test: Aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, E1, E3, *N*xDS0, serial, SONET/SDH, T1, and T3.

The physical path of a network data circuit usually consists of segments interconnected by devices that repeat and regenerate the transmission signal. The transmit path on one device connects to the receive path on the next device. If a circuit fault occurs in the form of a line break or a signal corruption, you can isolate the problem by using a loopback test. Loopback tests allow you to isolate segments of the circuit and test them separately.

To do this, configure a *line loopback* on one of the routers. Instead of transmitting the signal toward the far-end device, the line loopback sends the signal back to the originating router. If the originating router receives back its own data link layer packets, you have verified that the problem is beyond the originating router. Next, configure a line loopback farther away from the local router. If this originating router does not receive its own data link layer packets, you can assume the problem is on one of the segments between the local router and the remote router's interface card. In this case, the next troubleshooting step is to configure a line loopback closer to the local router to find the source of the problem.

There are several types of loopback testing supported by the Junos OS, as follows:

- DCE local—Loops packets back on the local DCE.
- DCE remote—Loops packets back on the remote DCE.

- Local—Useful for troubleshooting physical PIC errors. Configuring local loopback on an interface allows transmission of packets to the channel service unit (CSU) and then to the circuit toward the far-end device. The interface receives its own transmission, which includes data and timing information, on the local router's PIC. The data received from the CSU is ignored. To test a local loopback, issue the **show interfaces *interface-name*** command. If PPP keepalives transmitted on the interface are received by the PIC, the **Device Flags** field contains the output **Loop-Detected**.
- Payload—Useful for troubleshooting the physical circuit problems between the local router and the remote router. A payload loopback loops data only (without clocking information) on the remote router's PIC. With payload loopback, overhead is recalculated.
- Remote—Useful for troubleshooting the physical circuit problems between the local router and the remote router. A remote loopback loops packets, including both data and timing information, back on the remote router's interface card. A router at one end of the circuit initiates a remote loopback toward its remote partner. When you configure a remote loopback, the packets received from the physical circuit and CSU are received by the interface. Those packets are then retransmitted by the PIC back toward the CSU and the circuit. This loopback tests all the intermediate transmission segments.

Table 11 on page 86 shows the loopback modes supported on the various interface types.

Table 11: Loopback Modes by Interface Type

Interface	Loopback Modes	Usage Guidelines
Aggregated Ethernet, Fast Ethernet, Gigabit Ethernet	Local	Configuring Ethernet Loopback Capability
Circuit Emulation E1	Local and remote	Configuring E1 Loopback Capability
Circuit Emulation T1	Local and remote	Configuring T1 Loopback Capability
E1 and E3	Local and remote	Configuring E1 Loopback Capability and Configuring E3 Loopback Capability
*N*xDS0	Payload	Configuring Channelized E1 IQ and IQE Interfaces, Configuring T1 and NxDS0 Interfaces, Configuring Channelized OC12/STM4 IQ and IQE Interfaces (SONET Mode), Configuring Channelized STM1 IQ and IQE Interfaces, and Configuring Channelized T3 IQ Interfaces
Serial (V.35 and X.21)	Local and remote	Configuring Serial Loopback Capability
Serial (EIA-530)	DCE local, DCE remote, local, and remote	Configuring Serial Loopback Capability
SONET/SDH	Local and remote	Configuring SONET/SDH Loopback Capability

Table 11: Loopback Modes by Interface Type *(continued)*

Interface	Loopback Modes	Usage Guidelines
T1 and T3	Local, payload, and remote	Configuring T1 Loopback Capability and Configuring T3 Loopback Capability See also Configuring the T1 Remote Loopback Response

To configure loopback testing, include the **loopback** statement:

loopback *mode*;

You can include this statement at the following hierarchy levels:

- **[edit interfaces** *interface-name* **aggregated-ether-options]**
- **[edit interfaces** *interface-name* **ds0-options]**
- **[edit interfaces** *interface-name* **e1-options]**
- **[edit interfaces** *interface-name* **e3-options]**
- **[edit interfaces** *interface-name* **fastether-options]**
- **[edit interfaces** *interface-name* **gigether-options]**
- **[edit interfaces** *interface-name* **serial-options]**
- **[edit interfaces** *interface-name* **sonet-options]**
- **[edit interfaces** *interface-name* **t1-options]**
- **[edit interfaces** *interface-name* **t3-options]**

Interface Diagnostics

BERT allows you to troubleshoot problems by checking the quality of links. You can configure any of the following interfaces to execute a BERT when the interface receives a request to run this test: E1, E3, T1, T3; the channelized DS3, OC3, OC12, and STM1 interfaces; and the channelized DS3 IQ, E1 IQ, and OC12 IQ interfaces.

A BERT test requires a line loop to be in place on either the transmission devices or the far-end router. The local router generates a known bit pattern and sends it out the transmit path. The received pattern is then verified against the sent pattern. The higher the bit error rate of the received pattern, the worse the noise is on the physical circuit. As you move the position of the line loop increasingly downstream toward the far-end router, you can isolate the troubled portion of the link.

To configure BERT, you must configure the duration of the test, the bit pattern to send on the transmit path, and the error rate to monitor when the inbound pattern is received.

To configure the duration of the test, the pattern to send in the bit stream, and the error rate to include in the bit stream, include the **bert-period**, **bert-algorithm**, and **bert-error-rate** statements, respectively, at the **[edit interfaces** *interface-name interface-type*-**options]** hierarchy level:

[edit interfaces *interface-name interface-type*-options]
bert-algorithm *algorithm*;
bert-error-rate *rate*;
bert-period *seconds*;

By default, the BERT period is 10 seconds. You can configure the BERT period to last from 1 through 239 seconds on some PICs and from 1 through 240 seconds on other PICs.

rate is the bit error rate. This can be an integer from 0 through 7, which corresponds to a bit error rate from 10^{-0} (1 error per bit) to 10^{-7} (1 error per 10 million bits).

algorithm is the pattern to send in the bit stream. For a list of supported algorithms, enter a **?** after the **bert-algorithm** statement; for example:

```
[edit interfaces t1-0/0/0 t1-options]

user@host# set bert-algorithm ?
Possible completions:
  pseudo-2e11-o152     Pattern is 2^11 -1 (per O.152 standard)
  pseudo-2e15-o151     Pattern is 2^15 - 1 (per O.152 standard)
  pseudo-2e20-o151     Pattern is 2^20 - 1 (per O.151 standard)
  pseudo-2e20-o153     Pattern is 2^20 - 1 (per O.153 standard)
        ...
```

For specific hierarchy information, see the individual interface types.

NOTE: The 4-port E1 PIC supports only the following algorithms:

```
pseudo-2e11-o152     Pattern is 2^11 -1 (per O.152 standard)
pseudo-2e15-o151     Pattern is 2^15 - 1 (per O.151 standard)
pseudo-2e20-o151     Pattern is 2^20 - 1 (per O.151 standard)
pseudo-2e23-o151     Pattern is 2^23 (per O.151 standard)
```

When you issue the help command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.

NOTE: The 12-port T1/E1 Circuit Emulation (CE) PIC supports only the following algorithms:

```
all-ones-repeating   Repeating one bits
all-zeros-repeating  Repeating zero bits
alternating-double-ones-zeros  Alternating pairs of ones and zeros
alternating-ones-zeros  Alternating ones and zeros
pseudo-2e11-o152     Pattern is 2^11 -1 (per O.152 standard)
pseudo-2e15-o151     Pattern is 2^15 - 1 (per O.151 standard)
pseudo-2e20-o151     Pattern is 2^20 - 1 (per O.151 standard)
pseudo-2e7           Pattern is 2^7 - 1
pseudo-2e9-o153      Pattern is 2^9 - 1 (per O.153 standard)
repeating-1-in-4     1 bit in 4 is set
repeating-1-in-8     1 bit in 8 is set
repeating-3-in-24    3 bits in 24 are set
```

When you issue the help command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.

NOTE: The IQE PICs support only the following algorithms:

```
all-ones-repeating   Repeating one bits
all-zeros-repeating  Repeating zero bits
alternating-double-ones-zeros  Alternating pairs of ones and zeros
alternating-ones-zeros  Alternating ones and zeros
pseudo-2e9-o153      Pattern is 2^9  -1 (per O.153 (511 type) standard)
pseudo-2e11-o152     Pattern is 2^11 -1 (per O.152 and O.153 (2047 type)
 standards)
pseudo-2e15-o151     Pattern is 2^15 -1 (per O.151 standard)
pseudo-2e20-o151     Pattern is 2^20 -1 (per O.151 standard)
pseudo-2e20-o153     Pattern is 2^20 -1 (per O.153 standard)
pseudo-2e23-o151     Pattern is 2^23 -1 (per O.151 standard)
repeating-1-in-4     1 bit in 4 is set
repeating-1-in-8     1 bit in 8 is set
repeating-3-in-24    3 bits in 24 are set
```

When you issue the help command from the CLI, all BERT algorithm options are displayed, regardless of the PIC type, and no commit check is available. Unsupported patterns for a PIC type can be viewed in system log messages.

NOTE: BERT is supported on the PDH interfaces of the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP and the DS3/E3 MIC. The following BERT algorithms are supported:

```
all-ones-repeating            Repeating one bits
all-zeros-repeating           Repeating zero bits
alternating-double-ones-zeros Alternating pairs of ones and zeros
alternating-ones-zeros        Alternating ones and zeros
repeating-1-in-4              1 bit in 4 is set
repeating-1-in-8              1 bit in 8 is set
repeating-3-in-24             3 bits in 24 are set
pseudo-2e9-o153               Pattern is 2^9 - 1 (per 0.153 standard)
pseudo-2e11-o152              Pattern is 2^11 - 1 (per 0.152 standard)
pseudo-2e15-o151              Pattern is 2^15 - 1 (per 0.151 standard)
pseudo-2e20-o151              Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e20-o153              Pattern is 2^20 - 1 (per 0.153 standard)
pseudo-2e23-o151              Pattern is 2^23 (per 0.151 standard)
```

Table 12 on page 90 shows the BERT capabilities for various interface types.

Table 12: BERT Capabilities by Interface Type

Interface	T1 BERT	T3 BERT	Comments
12-port T1/E1 Circuit Emulation	Yes (ports 0–11)		• Limited algorithms
4-port Channelized OC3/STM1 Circuit Emulation	Yes (port 0–3)		• Limited algorithms
E1 or T1	Yes (port 0–3)	Yes (port 0–3)	• Single port at a time • Limited algorithms
E3 or T3	Yes (port 0–3)	Yes (port 0–3)	• Single port at a time
Channelized OC12	N/A	Yes (channel 0–11)	• Single channel at a time • Limited algorithms • No bit count
Channelized STM1	Yes (channel 0–62)	N/A	• Multiple channels • Only one algorithm • No error insert • No bit count
Channelized T3 and Multichannel T3	Yes (channel 0–27)	Yes (port 0–3 on channel 0)	• Multiple ports and channels • Limited algorithms for T1 • No error insert for T1 • No bit count for T1

These limitations do not apply to channelized IQ interfaces. For information about BERT capabilities on channelized IQ interfaces, see Channelized IQ and IQE Interfaces Properties.

Starting and Stopping a BERT Test

Before you can start the BERT test, you must disable the interface. To do this, include the **disable** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
disable;
```

After you configure the BERT properties and commit the configuration, begin the test by issuing the **test interface *interface-name interface-type*-bert-start** operational mode command:

```
user@host> test interface interface-name interface-type-bert-start
```

The test runs for the duration you specify with the **bert-period** statement. If you wish to terminate the test sooner, issue the **test interface *interface-name interface-type*-bert-stop** command:

```
user@host> test interface interface-name interface-type-bert-stop
```

For example:

```
user@host> test interface t3-1/2/0 t3-bert-start
user@host> test interface t3-1/2/0 t3-bert-stop
```

To view the results of the BERT test, issue the **show interfaces extensive | find BERT** command:

```
user@host> show interfaces interface-name extensive | find BERT
```

For more information about running and evaluating the results of the BERT procedure, see the Junos OS Operational Mode Commands.

NOTE: To exchange BERT patterns between a local router and a remote router, include the **loopback remote** statement in the interface configuration at the remote end of the link. From the local router, issue the **test interface** command.

Example: Configuring Bit Error Rate Testing

Configure a BERT test on a T3 interface. In this example, the run duration lasts for 120 seconds. The configured error rate is 0, which corresponds to a bit error rate of 10^{-0} (1 error per bit). The configured bit pattern of **all-ones-repeating** means that every bit the interface sends is a set to a value of 1.

```
[edit interfaces]
t3-1/2/0 {
    t3-options {
        bert algorithm all-ones-repeating;
        bert-error-rate 0;
        bert-period 120;
```

```
    }
}
```

PART 5

Index

Index

R

S

T

W