JUNIPER NETWORKS

Junos® OS

SONET/SDH Interfaces Configuration Guide

Release
11.4

Published: 2011-11-14

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

Junos® OS SONET/SDH Interfaces Configuration Guide
Release 11.4

Revision History
November 2011—R1 Junos® OS 11.4

The information in this document is current as of the date listed in the revision history.

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.

Abbreviated Table of Contents

Table of Contents

List of Figures

List of Tables

About This Guide

This preface provides the following guidelines for using the *Junos® OS SONET/SDH Interfaces Configuration Guide*:

Junos Documentation and Release Notes

For a list of related Junos documentation, see http://www.juniper.net/techpubs/software/junos/ .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos 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/ .

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books .

Objectives

This guide provides an overview of the network interfaces features of the JUNOS Software and describes how to configure these properties on the routing platform.

NOTE: For additional information about the Junos OS—either corrections to or information that might have been omitted from this guide—see the software release notes at http://www.juniper.net/ .

Audience

This guide is designed for network administrators who are configuring and monitoring a Juniper Networks M Series, MX Series, T Series, EX Series, or J Series router or switch.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

Supported Routing Platforms

For the features described in this manual, the JUNOS Software currently supports the following routing platforms:

- J Series
- M Series

- MX Series
- T Series

Using the Indexes

This reference contains two indexes: a complete index that includes topic entries, and an index of statements and commands only.

In the index of statements and commands, an entry refers to a statement summary section only. In the complete index, the entry for a configuration statement or command contains at least two parts:

- The primary entry refers to the statement summary section.
- The secondary entry, *usage guidelines*, refers to the section in a configuration guidelines chapter that describes how to use the statement or command.

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

```
system {
    scripts {
        commit {
            file ex-script.xsl;
        }
    }
}
interfaces {
    fxp0 {
        disable;
```

```
        unit 0 {
          family inet {
            address 10.0.0.1/24;
          }
        }
      }
    }
```

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

Table 1 on page xix 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 xix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub** <**default-metric** *metric*>**;**

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

Convention	Description	Examples
| (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 postsales 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/
- 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, visit us at http://www.juniper.net/support/requesting-support.html

PART 1

SONET/SDH Interfaces Configuration Statements Overview

CHAPTER 1

SONET/SDH Interfaces Configuration Statements and Hierarchy

The following interfaces hierarchy listings show the complete configuration statement hierarchy for the indicated hierarchy levels, listing all possible configuration statements within the indicated hierarchy levels, and showing their level in the configuration hierarchy. When you are configuring the Junos OS, your current hierarchy level is shown in the banner on the line preceding the **user@host#** prompt.

This section contains the following topics:

[edit chassis] Hierarchy Level

```
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
    sonet {
      device-count number;
    }
  }
  channel-group number {
    ethernet {
      device-count number;
    }
    fpc slot-number{
      pic pic-number {
        adaptive-services{
          service-package (layer-2 | layer-3);
        }
        aggregate-ports;
        atm-cell-relay-accumulation;
        atm-l2circuit-mode (aal5 | cell | trunk trunk);
        ce1 {
          e1 link-number {
```

```
            channel-group group-number;
            timeslots time-slot-range;
          }
        }
        channelization;
        ct1 {
          t1 link-number {
            channel-group group-number;
            timeslots time-slot-range;
          }
        }
        ct3 {
          port port-number {
            t1 link-number {
              channel-group group-number;
              timeslots time-slot-range;
            }
          }
          framing sdh;
        }
        max-queues-per-interface number;
        mlfr-uni-nni-bundles num-intf;
        no-concatenate;
        shdsl {
          pic-mode (1-port-atm | 2-port-atm);
        }
        vtmapping (klm | itu-t);
      }
    }
    fpc slot-number{
    pic pic-number{
      egress-policer-overhead bytes;
        ingress-policer-overhead bytes;
      }
    }
  }
```

[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 aex;
    (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;
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;
}
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;
    }
  }
  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;
      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 | 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 Configuration Guide*
- *Junos OS Network Interfaces Configuration Guide*

[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 *Junos OS Routing Protocols 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 Configuration Guide*
- *Junos OS Network Interfaces Configuration Guide*

PART 2

Configuring SONET/SDH Interfaces

CHAPTER 2

Configuring SONET/SDH Interfaces

SONET/SDH Interfaces Overview

Synchronous Digital Hierarchy (SDH) is a CCITT standard for a hierarchy of optical transmission rates. Synchronous Optical Network (SONET) is a USA standard that is largely equivalent to SDH. Both are widely used methods for very high speed transmission of voice and data signals across the numerous world-wide fiber-optic networks.

SDH and SONET use light-emitting diodes or lasers to transmit a binary stream of light-on and light-off sequences at a constant rate. At the far end optical sensors convert the pulses of light back to electrical representations of the binary information.

In wavelength-division multiplexing (WDM), light at several different wavelengths (colors to a human eye) is transmitted on the same fiber segment, greatly increasing the throughput of each fiber cable.

In dense wavelength-division multiplexing (DWDM), many optical data streams at different wavelengths are combined into one fiber.

The basic building block of the SONET/SDH hierarchy in the optical domain is an OC1; in the electrical domain, it is an STS-1. An OC1 operates at 51.840 Mbps. OC3 operates at 155.520 Mbps.

A SONET/SDH stream can consist of discrete lower-rate traffic flows that have been combined using time-division multiplexing (TDM) techniques. This method is useful, but a portion of the total bandwidth is consumed by the TDM overhead. When a SONET/SDH stream consists of only a single, very high speed payload, it is referred to as operating in concatenated mode. A SONET/SDH interface operating in this mode has a "c" added to the rate descriptor. For example, a concatenated OC48 interface is referred to as OC48c.

SONET and SDH traffic streams exhibit very few differences in behavior that are significant to Juniper Networks SONET/SDH interfaces; in general, this chapter uses *SONET/SDH* to indicate behavior that is identical for the two standards. However, there is one important difference that requires you to configure the interface specifically for SONET or SDH mode. That difference is in the setting of two bits (the ss-bits) in the pointer. SONET equipment ignores these bits, but SDH equipment uses them to distinguish a VC-4 payload from other types. When configured in SDH mode, Juniper Networks SONET/SDH PICs set the ss-bits to **s1s0 2** (binary 10). For more information, see the *Junos OS System Basics Configuration Guide*.

CAUTION: To extend the life of the laser, when a SONET/SDH PIC is not being actively used with any valid links, take the PIC offline until you are ready to establish a link to another device. To do this, issue the **request chassis pic offline fpc-slot** *slot-number* **pic-slot** *slot-number* operational mode command:

user@host> request chassis pic offline fpc-slot *slot-number* **pic-slot** *slot-number*

After you have connected the PIC to another device, bring the PIC back online by issuing the **request chassis pic online fpc-slot** *slot-number* **pic-slot** *slot-number* operational mode command.

user@host> request chassis pic online fpc-slot *slot-number* **pic-slot** *slot-number*

For information about taking a PIC offline or online, see the **request chassis pic offline** command and the **request chassis pic online** command in the *Junos OS System Basics and Services Command Reference*.

Configuring SONET/SDH Physical Interface Properties

To configure SONET/SDH physical interface properties, include the **sonet-options** statement at the **[edit interfaces** *interface-name***]** hierarchy level:

```
[edit interfaces so-fpc/pic/port]
framing (sdh | sonet);
sonet-options {
  aggregate asx;
  aps {
    advertise-interval milliseconds;
    annex-b
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
```

```
        neighbor address;
        paired-group group-name;
        protect-circuit group-name;
        request;
        revert-time seconds;
        switching-mode (bidirectional | unidirectional);
        working-circuit group-name;
      }
      bytes {
        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;
        defect hold-time up milliseconds down milliseconds;
      }
    }
    vtmapping (itu-t | klm);
    (z0-increment | no-z0-increment);
    speed (oc3 | oc12 | oc48);
```

Note that when you configure SONET/SDH OC48 interfaces for channelized (multiplexed) mode (by including the **no-concatenate** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level), the **bytes f1** statement has no effect. Currently, the **bytes e1-quiet** statement is ignored if you include it in the configuration. The **bytes f2**, **bytes z3**, **bytes z4**, and **path-trace** options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3. When using **no-concatenate**, you must specify a channel. For more information, see the *Junos OS System Basics Configuration Guide*.

For DS3 channels on a channelized OC12 interface, the **bytes f1**, **bytes f2**, **bytes z3**, and **bytes z4** options have no effect. The **bytes s1** option is supported only for channel 0; it is ignored if configured on channels 1 through 11. The **bytes s1** value configured on channel 0 applies to all channels on the interface.

You can also include some of the statements in the **sonet-options** statement to set SONET/SDH parameters on ATM interfaces.

You can configure the following SONET/SDH physical interface properties:

Configuring SONET/SDH Framing

The 4-port OC48 PIC with SFP installed, the next-generation SONET/SDH PICs with SFP, the 4-port OC192 PIC on M Series, MX Series, and T Series routers, the SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP on MX Series routers, and the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP on MX Series routers support SONET or SDH framing on a per-port basis. This functionality allows you to mix SONET and SDH modes on interfaces on a single PIC or MIC. You can use the **framing** statement to configure incoming SDH links from Europe and outgoing SONET links to the US on the same PIC or MIC. Traffic flowing through other ports of the same PIC or MIC will not be affected.

When you change SONET/SDH mode on a port, only the port's framing type is changed. The PIC or MIC does not go offline.

To configure framing on a per-port basis, include the **framing** (**sdh** | **sonet**) statement at the **[edit interfaces so-*fpc/pic/port*]** hierarchy level:

```
[edit interfaces]
so-fpc/pic/port {
  framing (sdh | sonet);
}
```

NOTE: Per-port framing configuration is applicable for SONET interfaces in concatenated mode (default mode) only. When you configure a PIC or MIC to operate in nonconcatenated mode, the individual channels inherit framing configuration from the **[edit chassis fpc *number* pic *number* framing (sonet | sdh)]** hierarchy level.

NOTE: Automatic Protection Switching (APS) is used by SONET add/drop multiplexers (ADMs) to protect against circuit failures. If APS is configured, and you do not change the SONET/SDH mode on both the working and protection port, APS support will not function properly. Both the working and protection ports must have the same mode configuration.

To view interface information, use the operational mode command **show interfaces so-*fpc/pic/port***.

Configuring SONET/SDH Interface Speed

You can configure the speed of SONET/SDH interfaces on next-generation SONET/SDH Type 1 and Type 2 PICs with SFP. The speed you select is dependent upon whether the PIC is in concatenated or nonconcatenated mode. In concatenated mode, the bandwidth of the interface is in a single channel. In nonconcatenated mode, the PIC operates in channelized (multiplexed) mode.

Table 3 on page 31 shows the mode combinations for the next-generation SONET/SDH Type 1 PICs with SFP.

Table 3: Type 1 PIC Mode Combinations

PIC	Mode	Speed Configuration	Default Mode
2-port OC3	2xOC3 concatenated	*fpc/pic*/0 speed oc3	Concatenated
4-port OC3	1xOC12 concatenated	*fpc/pic*/0 speed oc12	
	1xOC12 nonconcatenated	*fpc/pic*/0:0 speed oc3	Nonconcatenated
	4xOC3 concatenated	*fpc/pic/port* speed oc3	Concatenated
1-port OC12	1xOC12 concatenated	*fpc/pic*/0 speed oc12	Concatenated
	1xOC12 nonconcatenated	*fpc/pic*/0:0 speed oc3	Nonconcatenated
	1xOC3 concatenated	*fpc/pic*/0 speed oc3	

Table 4 on page 32 shows the mode combinations for the next-generation SONET/SDH Type 2 PICs with SFP.

Table 4: Type 2 PIC Mode Combinations

PIC	Mode	Speed Configuration	Default Mode
1-port OC48	1xOC48 concatenated	*fpc/pic*/0 speed oc48	Concatenated
	1xOC48 nonconcatenated	*fpc/pic*/0:0 speed oc12	Nonconcatenated
	1xOC12 concatenated	*fpc/pic*/0 speed oc12	
	1xOC12 nonconcatenated	*fpc/pic*/0 0 speed oc3	
	1xOC3 concatenated	*fpc/pic*/0 speed oc3	
4-port OC12	1xOC48 concatenated	*fpc/pic*/0 speed oc48	
	1xOC48 nonconcatenated	*fpc/pic*/0:0 speed	Nonconcatenated
	1xOC12 nonconcatenated	*fpc/pic*/0 speed oc3	
	4xOC12 concatenated	*fpc/pic/port* speed oc3|oc12	Concatenated
4-port OC3	1xOC12 concatenated	*fpc/pic*/0 speed oc12	
	1xOC12 nonconcatenated	*fpc/pic*/0:0 speed oc3	Nonconcatenated
	4xOC3 concatenated	*fpc/pic/port* speed oc3	Concatenated

By default, SONET/SDH PICs operate in concatenated mode. To specify interface speed in concatenated mode, include the **speed** statement with options at the **[edit interfaces so-*fpc/pic/port*]** hierarchy level:

```
[edit interfaces so-fpc/pic/port
speed (oc3 | oc12 | oc48);
```

For example, each port of 4-port OC12 PIC can be configured to be in OC3 or OC12 speed independently when this PIC is in 4xOC12 concatenated mode.

To specify interface speed in nonconcatenated mode, include the **speed** statement at the **[edit interfaces so-*fpc/pic/port.channel*]** hierarchy level:

```
[edit interfaces so-fpc/pic/port.channel]
speed (oc3 | oc12);
```

To configure the PIC to operate in channelized (multiplexed) mode, include the **no-concatenate** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level.

NOTE: On SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP and Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, you cannot set the interface speed at the **[edit interfaces]** hierarchy level. To enable the speed on these MICs, you need to set the port speed at the **[edit chassis fpc *slot-number* pic *pic-number* port *port-number*]** hierarchy level.

For more information about using the **non-concatenate** statement, see the *Junos OS System Basics Configuration Guide*.

Configuring SONET/SDH Rate-Selectability

You can configure rate-selectability on the SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP and Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP by specifying the port speed. To specify the port speed, include the **speed** statement at the **[edit chassis fpc *slot-number* pic *pic-number* port *port-number*]** hierarchy level:

```
[edit chassis fpc slot-number pic pic-number port port-number]
speed (oc12-stm4 | oc3-stm1 | oc48-stm16);
```

By default, rate-selectability is enabled on the SONET/SDH OC3/STM1 (Multi-Rate) MICs with **oc3-stm1** speed.

To disable the rate-selectability on the 8-port SONET/SDH OC3/STM1 (Multi-Rate) MIC, include the **no-multi-rate** statement with options at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level.

NOTE: You cannot disable the rate-selectability on the 4-port SONET/SDH OC3/STM1(Multi-Rate) MIC and the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP.

Table 5 on page 33 shows the port speed restrictions on the SONET/SDH OC3/STM1 (Multi-Rate) MICs.

Table 5: Port Speed Restrictions for SONET/SDH OC3/STM1 (Multi-Rate) MICs

Mode\MIC Name	8-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP	4-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP
Rate-selectable Mode	• Only the first two ports (0–1) can be configured for **oc48-stm16** speed. • All eight ports can be configured for **oc3-stm1** or **oc12-stm4** speed. • Total available bandwidth is 8.75 Gbps.	• Only the first port (0) can be configured for **oc48-stm16** speed. • All four ports can be configured for **oc3-stm1** or **oc12-stm4** speed. • Total available bandwidth is 4.375 Gbps.
Non-rate-selectable Mode	• Only the first four ports (0–3) are available and set to **oc48-stm16** speed. • Total available bandwidth is 10 Gbps.	This mode is not available on this MIC.

All ports of the 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP can be configured as channelized OC3/channelized STM1. However, only four ports (ports 0, 1, 2, and 3) can be configured as channelized OC12/channelized STM4. Table 6 on page 34 and Table 7 on page 34 indicate the port configuration restrictions of the 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP.

Table 6: OC12/STM4 Port Configuration Restrictions on MIC-3D-8CHOC3-4CHOC12

Ports Configured as OC3/STM1	Ports Available for OC12/STM4 Configuration
None	0, 1, 2, and 3
0 or 4	1, 2, and 3
1 or 5	0, 2, and 3
2 or 6	0, 1, and 3
3 or 7	0, 1, and 2

Table 7: OC3/STM1 Port Configuration Restrictions on MIC-3D-8CHOC3-4CHOC12

Ports Configured as OC12/STM4	Ports Available for OC3/STM1 Configuration
None	All ports (0 through 7)
0	All ports except port 4
1	All ports except port 5
2	All ports except port 6
3	All ports except port 7

All ports of the 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP can be configured as channelized OC3/channelized STM1. However, only two ports (ports 0 and 1) can be configured as channelized OC12/channelized STM4. Table 8 on page 34 and Table 9 on page 35 indicate the port configuration restrictions of the 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP.

Table 8: OC12/STM4 Port Configuration Restrictions on MIC-3D-4CHOC3-2CHOC12

Ports Configured as OC3/STM1	Ports Available for OC12/STM4 Configuration
None	0 and 1
0 or 2	1
1 or 3	0

Table 9: OC3/STM1 Port Configuration Restrictions on MIC-3D-4CHOC3-2CHOC12

Ports Configured as OC12/STM4	Ports Available for OC12/STM4 Configuration
None	All ports (0 through 3)
0	All ports except 2
1	All ports except 3

Configuring SONET/SDH Header Byte Values

To configure values in SONET/SDH header bytes, include the **bytes** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
bytes {
    c2 value;
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
}
```

You can configure the following SONET/SDH header bytes:

- **c2**—Path signal label SONET/SDH overhead byte. SONET/SDH frames use the C2 byte to indicate the contents of the payload inside the frame. SONET/SDH interfaces use the C2 byte to indicate whether the payload is scrambled. For the c2 byte, ***value*** can be from **0** through **255**. The default value is **0xCF**.
- **e1-quiet**—Default idle byte sent on the orderwire SONET/SDH overhead bytes. The router does not support the orderwire channel, and hence sends this byte continuously.
- **f1**, **f2**, **z3**, **z4**—SONET/SDH overhead bytes. For these bytes, ***value*** can be from **0** through **255**. The default value is **0x00**.
- **s1**—Synchronization message SONET/SDH overhead byte. This byte is normally controlled as a side effect of the system reference clock configuration and the state of the external clock coming from an interface if the system reference clocks have been configured to use an external reference. For the s1 byte, ***value*** can be from **0** through **255**.

Table 10 on page 35 displays Junos OS framing bytes for several specific speeds.

Table 10: SONET/SDH Framing Bytes for Specific Speeds

Overhead Bytes	STM4	STM16	STM64	OC12	OC48	OC192
A1	F6	F6	F6	F6	F6	F6

Table 10: SONET/SDH Framing Bytes for Specific Speeds *(continued)*

Overhead Bytes	STM4	STM16	STM64	OC12	OC48	OC192
A2	28	28	28	28	28	28
C1	—	—	—	1..12	1..48	1..192
H1/H2	6A0A	6A0A	6A0A	620A	620A	620A
Z0	01/CC	01/CC	01/CC	—	—	—
Concatenated mode	93FF	93FF	93FF	93FF	93FF	93FF

When you configure SONET/SDH header bytes, note the following:

- The C2 byte is the path signal label. If the C2 byte value on an interface does not match the C2 byte value on the remote interface, the path label mismatch (PLM-P) or unequipped (UNEQ-P) alarm might occur.
- When you configure SONET/SDH OC48 interfaces for channelized (multiplexed) mode (by including the **no-concatenate** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level), the **bytes f1** statement has no effect.
- Currently, the **bytes e1-quiet** statement is ignored if you include it in the configuration.
- The **bytes f2**, **bytes z3**, **bytes z4**, and **path-trace** options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.
- For DS3 channels on a channelized OC12 interface, the **bytes f1, bytes f2, bytes z3,** and **bytes z4** options have no effect.
- The **bytes s1** option is supported only for channel 0; it is ignored if configured on channels 1 through 11. The **bytes s1** value configured on channel 0 applies to all channels on the interface.
- Embedded operations channel (EOC) D1, D2, and D3 bytes are not supported.
- For channelized OC12 IQE and channelized OC48 IQE PICs with SFPs:
  - Only C2 (Path signal label) and S1 byte setting is supported.
  - Following header bytes are not supported. The router will syslog an INFO message if a command for an unsupported header byte is received.

    F1—Section user channel byte

    F2—Path user channel byte

    Z3, Z4—SONET/SDH overhead bytes

    E1—quiet default idle byte

  - The following header bytes are supported on the SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP.

Z0, F1—Section user channel bytes

K1, K2, S1— Line user channel bytes

G1, F2, Z3, Z4, C2, E1—Path user channel bytes

- The following header bytes are supported on the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP.

  Z0, F1—Section user channel bytes

  S1— Line user channel bytes

  G1, F2, Z3, Z4, C2, E1—Path user channel bytes

Configuring an Incrementing STM ID

When configured in SDH framing mode, SONET/SDH interfaces on a Juniper Networks router might not interoperate with some older versions of ADMs or regenerators that require an incrementing STM ID.

Current SDH standards specify a set of 3*n* overhead bytes in an STM*n* that includes the J0 section trace byte. The rest are essentially unused (spare Z0) and contain hexadecimal values (0x01, 0xCC, 0xCC ... 0xCC). The older version of the standard specified that the same set of bytes should contain an incrementing sequence: 1, 2, 3, ..., 3*n*. Their use was still unspecified although they might have been used to assist in frame alignment. You can configure an incrementing STM ID to enable your Juniper Networks router to interoperate with older equipment that relies on these bytes for frame alignment.

The STM identifier has a precise definition in the SDH specifications. In ITU-T Recommendation G.707, *Network node interface for the synchronous digital hierarchy (SDH)* (03/96), Section 9.2.2.2.

You can explicitly configure an incrementing STM ID rather than a static one in the SDH overhead by including the **z0-increment** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level. You should include this statement only for SDH mode; do not use it for SONET mode.

```
[edit interfaces so-fpc/pic/port sonet-options]
z0-increment;
```

To explicitly disable incrementing of the STM ID, include the following statement:

```
[edit interfaces so-fpc/pic/port sonet-options]
no-z0-increment;
```

Configuring the SONET/SDH Frame Checksum

By default, SONET/SDH interfaces use a 16-bit frame checksum. You can configure a 32-bit checksum, which provides more reliable packet verification. However, some older equipment might not support 32-bit checksums.

To configure a 32-bit checksum, include the **fcs** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
fcs 32;
```

To return to the default 16-bit frame checksum, delete the **fcs 32** statement from the configuration:

```
[edit]
user@host# delete interfaces so-fpc/pic/port sonet-options fcs 32
```

To explicitly configure a 16-bit checksum, include the **fcs** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
fcs 16;
```

On a channelized OC12 interface, the **sonet-options fcs** statement is not supported. To configure the frame checksum sequence (FCS) on each DS3 channel, you must include the **t3-options fcs** statement in the configuration for each channel.

Configuring Channelized IQ and IQE SONET/SDH Loop Timing

By default, internal clocking (line timing) is used on channelized IQ and IQE interfaces. To configure SONET/SDH or DS3-level clocking, include the **loop-timing** statement:

```
loop-timing;
```

To explicitly configure the default line timing, include the **no-loop-timing** statement in the configuration:

```
no-loop-timing;
```

You can include these statements at the following hierarchy levels:

- **[edit interfaces ct3-*fpc/pic/port* t3-options]**
- **[edit interfaces stm1-*fpc/pic/port* sonet-options]**

The **loop-timing** and **no-loop-timing** statements apply only to E1 and T1 interfaces you configure on channelized IQ and IQE PICs. If you attempt to include these statements on any other interface type, they are ignored.

For all channelized IQ and IQE PICs, the **clocking** statement is supported on all channels. To configure clocking on individual interfaces, include the **clocking** statement at the **[edit interfaces *type-fpc/pic/port*:*channel*]** hierarchy level. If you do not include the **clocking** statement, the individual interfaces use internal clocking by default.

For more information, see Configuring the Clock Source and Clock Sources on Channelized Interfaces.

Configuring SONET/SDH Loopback Capability

To configure loopback capability on a SONET/SDH interface, include the **loopback** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
loopback (local | remote);
```

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.

For more information about configuring BERT, see Interface Diagnostics. For more information about using operational mode commands to test interfaces, see the *Junos OS System Basics and Services Command Reference*.

To turn off the loopback capability, remove the **loopback** statement from the configuration:

```
[edit]
user@host# delete interfaces so-fpc/pic/port sonet-options loopback
```

For channel 0 on channelized interfaces only, you can include the **loopback** statement at the **[edit interfaces *interface-name interface-type*-options]** hierarchy level. The loopback setting configured for channel 0 applies to all channels on the channelized interface. The **loopback** statement is ignored if you include it at this hierarchy level in the configuration of other channels. To configure loopbacks on individual channels, you must include the ***channel-type*-options loopback** statement in the configuration for each channel. This allows each channel to be put in loopback mode independently.

For example, for DS3 channels on a channelized OC12 interface, the **sonet-options loopback** statement is supported only for channel 0; it is ignored if included in the configuration for channels 1 through 11. The SONET/SDH loopback configured for channel 0 applies to all 12 channels equally. To configure loopbacks on the individual DS3 channels, you must include the **t3-options loopback** statement in the configuration for each channel. This allows each DS3 channel can be put in loopback mode independently.

You can determine whether there is an internal problem or an external problem by checking the error counters in the output of the **show interface *interface-name* extensive** command:

```
user@host> show interfaces so-fpc/pic/port extensive
```

Example: Configuring SONET/SDH Loopback Capability

To determine whether a problem is internal or external, loop packets on both the local and the remote router. To do this, include the **no-keepalives** and **encapsulation cisco-hdlc** statements at the **[edit interfaces *interface-name*]** hierarchy level, and the **loopback local** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level. With this configuration, the link stays up, so you can loop ping packets to a remote router. The **loopback local** statement causes the interface to loop within the PIC just before the data reaches the transceiver.

```
[edit interfaces]
so-1/0/0 {
    no-keepalives;
    encapsulation cisco-hdlc;
    sonet-options {
        loopback local;
    }
    unit 0 {
        family inet {
```

```
            address 10.100.100.1/24;
        }
    }
}
```

Configuring the SONET/SDH Path Trace Identifier

The SONET/SDH *path trace identifier* is a text string that identifies the circuit. If the string contains spaces, enclose it in quotation marks.

By default, the Junos OS uses the router and interface names for the path trace identifier. Depending on the router and interface names, the default path trace identifier might be longer then 16 bytes. The SDH standards define a maximum 16-byte path trace. For this reason, the default path trace identifier might be truncated in SDH mode. You can prevent the path trace identifier from being truncated in SDH mode by configuring a path trace identifier that is under 16-bytes long. In SONET mode, a path trace identifier can be up to 64-bytes long.

For DS3 channels on a channelized OC12 interface, you can configure a unique path trace for each of the 12 channels. Each path trace can be up to 16 bytes. For channels on a channelized OC12 intelligent queuing (IQ and IQE) interface, each path trace can be up to 64 bytes.

To configure a path trace identifier, include the **path-trace** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces interface-name sonet-options]
path-trace trace-string;
```

A common convention is to use the circuit identifier as the path trace identifier.

To display the local router's path trace identifier, issue the **show interfaces** command on the remote router.

Configuring SONET/SDH HDLC Payload Scrambling

SONET/SDH HDLC payload scrambling, which is enabled by default, provides better link stability. Both sides of a connection must either use or not use scrambling.

NOTE: HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling, because the Junos OS rejects configurations that have both features enabled. For more information, see "Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces" on page 63.

On a channelized OC12 interface, the **sonet-options payload-scrambler** statement is ignored. To configure scrambling on the DS3 channels on the interface, include the **t3-options payload-scrambler** statement in the configuration for each DS3 channel.

To disable HDLC payload scrambling, include the **no-payload-scrambler** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
no-payload-scrambler;
```

To return to the default, that is, to re-enable payload scrambling, delete the **no-payload-scrambler** statement from the configuration:

```
[edit]
user@host# delete interfaces so-fpc/pic/port sonet-options no-payload-scrambler
```

To explicitly enable payload scrambling, include the **payload-scrambler** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
payload-scrambler;
```

Configuring SONET/SDH RFC 2615 Support

RFC 2615, *PPP over SONET/SDH*, requires certain C2 header byte and FCS settings that vary from the default values configured in accordance with RFC 1619 (the previous version of RFC 2615). The newer values are optimized for stronger error detection, especially when combined with payload scrambling at higher bit rate links.

Table 11 on page 41 shows the older (RFC 1619) and newer (RFC 2615) values, together with the Juniper Networks default values.

Table 11: SONET/SDH Default Settings

Value	RFC 1619	Default	RFC 2615
SONET/SDH C2 header byte	0XCF	0XCF	0X16
Frame checksum (bit)	16	16	32
Payload scrambling	n/a	Enabled	Enabled

To enable support for the RFC 2615 features, include the **rfc-2615** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options]
rfc-2615;
```

Configuring SONET/SDH Defect Triggers to Be Ignored

A trigger is a defect alarm that causes a physical interface to be marked down. By default, all defects are honored with no hold time. For SONET/SDH and ATM over SONET/SDH interfaces only, you can configure individual triggers to ignore a defect, honor a defect, and apply up and down hold timers to the defect.

Table 12 on page 41 lists the defects you can configure.

Table 12: SONET/SDH and ATM Active Alarms and Defects

Alarm	Description
Physical	

Table 12: SONET/SDH and ATM Active Alarms and Defects *(continued)*

Alarm	Description
pll	Phase-locked loop out of lock
lol	Loss of light
Section	
lof	Loss of frame
los	Loss of signal
Line	
ais-l	Alarm indication signal—line
rfi-l	Remote failure indication—line
ber-sd	Bit error rate defect-signal degrade
ber-sf	Bit error rate fault-signal fail
Path	
ais-p	Alarm indication signal—path
locd (ATM only)	Loss of cell delineation
lop-p	Loss of pointer—path
plm-p	Payload label mismatch
rfi-p	Remote failure indication—path
uneq-p	Path unequipped

To configure defects to be ignored, include the **trigger** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces interface-name sonet-options]
trigger {
  defect ignore;
}
```

If you configure a defect to be ignored, that defect does not contribute to the interface being marked down or up.

After you configure a defect to be ignored, the Junos OS reevaluates the state of the defect on the interface. If the defect is outstanding and has caused the interface to be marked down, the interface is marked up.

When you configure a trigger on a low-level defect—for example, an LOS—only the low-level defect is affected. Higher-level defects that might result from the lower-level defect are not affected by the low-level trigger configuration. Therefore, you must configure higher-level defects as well.

Configuring SONET/SDH Defect Hold Times

By default, an interface is marked down as soon as a defect is detected, and is marked up as soon as the defect is absent. You might want to apply hold times to defects for the following reasons:

- To prevent route flaps from happening before a defect has been outstanding for a longer period than would be expected for an Automatic Protection Switching (APS) cutover
- To reduce the number of interface transitions

NOTE: On M Series and T Series routers with Channelized SONET IQ PICs and Channelized SONET IQE PICs, the SONET defect alarm trigger **hold-time** statement is not supported.

When you apply a “down” hold time to a defect, the defect must be present for at least the hold-time period before the interface is marked down. When you apply an “up” hold time to a defect, the defect must remain absent for at least the hold-time period before the interface is marked up, assuming no other defect is outstanding.

When you configure hold timers and the interface goes from up to down, the interface transition is not advertised to the rest of the system until the interface has remained down for the hold-time period. Similarly, when an interface goes from down to up, the interface transition is not advertised until the interface has remained up for the hold-time period.

To configure hold timers, include the **hold-time** statement at the **[edit interfaces *interface-name* sonet-options trigger *defect*]** hierarchy level:

```
[edit interfaces interface-name sonet-options trigger defect]
hold-time up milliseconds down milliseconds;
```

The time can be a value from 1 through 65,534 milliseconds.

When you configure defect hold times, you should note the following:

- You can configure an up hold time, a down hold time, or both.
- Each interface on a SONET/SDH PIC controls certain aspects of the SONET/SDH overhead. For example, when you configure an OC48 PIC to be nonconcatenated, four interfaces are created. Each interface has its own path overhead. However, all four path interfaces share the same physical, section, and line overhead. This means the following:
  - Each interface’s path trigger configuration is honored.

- The physical, section, and line trigger configuration for the primary interface (**so-*fpc/pic/slot*:0**) is applied to all four interfaces.

Therefore, if you configure the **so-*fpc/pic/slot*:0** interface to have a hold time for the LOS trigger, when an LOS event occurs, all four interfaces remain up until the trigger expires, and then all four interfaces are marked down.

- The hold timers on the SONET/SDH defects are applied in addition to any other hold timers you configure on the interface. For example, if an interface is up and you configure a SONET/SDH trigger down hold time of 100 milliseconds and an interface down hold time of 250 milliseconds, when the SONET/SDH defect occurs, the SONET/SDH trigger timer starts. After 100 milliseconds, assuming the defect is still present, the SONET/SDH defect starts the 250 millisecond down timer. After this has expired and again assuming the defect is still outstanding, the interface will be marked down. For more information about interface hold timers, see Damping Interface Transitions.
- Some defects are reported through a periodic poll (once every second). For these defects, there could be up to one second lost before the defect is detected and the hold timer is started. The hold timer expires in precisely the amount of time configured. At that point, the existence of the defect is checked again and the interface is marked up or down accordingly. These defects are as follows:
  - lol
  - pll
  - ber-sf
  - ber-sd
- We recommend the following settings:
  - Configure SONET/SDH defect timers on no more than 64 interfaces per FPC.
  - Configure a combined up hold time and down hold time for a SONET/SDH defect to be at least 100 milliseconds.

Example: Configuring SONET/SDH Defects to Be Ignored

Prevent an LOS from bringing down an interface. An LOS can lead to the following defects:

- AIS-L
- LOF
- PLL
- RFI-L
- RFI-P

```
[edit interfaces sonet-options trigger]
ais-l ignore;
lof ignore;
los ignore;
pll ignore;
```

```
rfi-l ignore;
rfi-p ignore;
```

Configuring Virtual Tributary Mapping

You can configure virtual tributary mapping to use KLM mode or ITU-T mode. By default, virtual tributary mapping uses KLM mode.

For the Channelized STM1 IQ and IQE PICs, you can configure virtual tributary mapping by including the **vtmapping** statement at the **[edit interfaces cau4-*fpc/pic/port* sonet-options]** hierarchy level:

```
[edit interfaces cau4-fpc/pic/port sonet-options]
vtmapping (klm | itu-t);
```

For the STM1 PIC, you can configure virtual tributary mapping by including the **vtmapping** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level:

```
[edit chassis fpc slot-number pic pic-number]
vtmapping (klm | itu-t);
```

Configuring Channelized STM1 Interfaces lists the KLM mappings used by the Channelized STM1-to-E1 PIC interfaces.

Configuring APS and MSP

Automatic Protection Switching (APS) is used by SONET add/drop multiplexers (ADMs) to protect against circuit failures. The Junos implementation of APS allows you to protect against circuit failures between an ADM and one or more routers, and between multiple interfaces in the same router. When a circuit or router fails, a backup immediately takes over.

NOTE: For SDH interfaces, the Junos OS supports multiplex section protection (MSP). You configure MSP with the same CLI statements you use to configure APS.

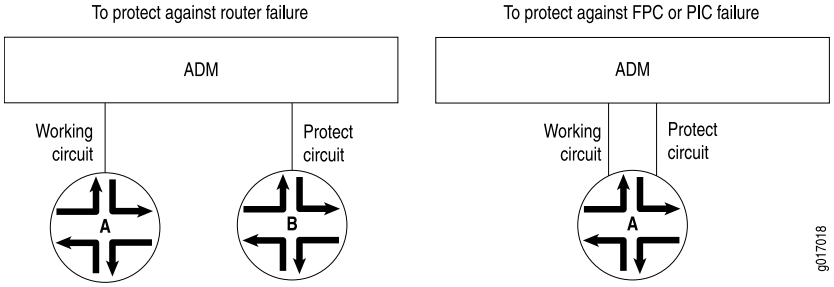
The Junos OS supports APS 1+1 switching, either revertive or nonrevertive mode, and bidirectional mode only (although you can configure interoperation with line-terminating equipment [LTE] provisioned for unidirectional mode). The Junos OS does not transmit identical data on the working and protect circuits, as the APS specification requires for 1+1 switching, but this causes no operational impact.

For DS3 channels on a channelized OC12 interface, you can configure APS on channel 0 only. If you configure APS on channels 1 through 11, it is ignored.

With APS and MSP, you configure two circuits, a *working circuit* and a *protect circuit*. Normally, traffic is carried on the working circuit (that is, the working circuit is the active circuit), and the protect circuit is disabled. If the working circuit fails or degrades, or if the working router fails, the ADM and the protect router switch the traffic to the protect circuit, and the protect circuit becomes the active circuit.

To configure APS or MSP, you configure a working and a protect circuit, as shown in Figure 1 on page 46. To protect against a router failure, you connect two routers to the ADM, configuring one of them as the working router and the second as the protect router. To protect against a PIC or FPC failure, you connect one router to the ADM through both the working and protect circuits, configuring one of the PICs or FPCs as the working circuit and the second as the protect circuit.

Figure 1: APS/MSP Configuration Topologies



To configure APS or MSP, include the **aps** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces interface-name sonet-options]
aps {
  advertise-interval milliseconds;
  annex-b
  authentication-key key;
  force;
  hold-time milliseconds;
  lockout;
  neighbor address;
  paired-group group-name;
  protect-circuit group-name;
  request;
  revert-time seconds;
  switching-mode (bidirectional | unidirectional);
  working-circuit group-name;
}
```

This section includes the following topics:

- Configuring APS Load Sharing Between Circuit Pairs on page 58
- Example: Configuring APS Load Sharing Between Circuit Pairs on page 59

NOTE: This implementation of APS is not supported on Layer 2 circuits. For Layer 2 circuits, configure APS by including the **protect-interface** statement. You can include this statement at the following hierarchy levels:

- **[edit logical-systems *logical-system-name* protocols l2circuit neighbor *neighbor-id* interface *interface-name*]**
- **[edit protocols l2circuit neighbor *neighbor-id* interface *interface-name*]**

For more information and a configuration example, see the *Junos OS VPNs Configuration Guide*.

When configuring the APS **annex-b** option, the APS options *must* be configured as follows:

- **switching-mode** *cannot* be uni-directional
- **revert-time** *cannot* be configured
- **lockout** is allowed to be configured
- **wait-to-restore-time** is allowed *only* when Annex-B is configured
- **protect-circuit** *must* be configured
- **working-circuit** *must* be configured

Configuring Basic APS Support

To set up a basic APS configuration, configure one interface to be the working circuit and a second to be the protect circuit. If you are using APS to protect against router failure, configure one interface on each router. If you are using APS to protect against FPC failure, configure two interfaces on the router, one on each FPC.

For each working–protect circuit pair, configure the following:

- Group name—Creates the association between the two circuits. Configure the same group name for both the working and protect routers.
- Authentication key—You configure this on both interfaces. Configure the same key for both the working and protect routers.
- Address of the other interface on the other router—If you are configuring one router to be the working router and a second to be the protect router, you must configure the address of the remote interface. You configure this on one or both of the interfaces.

The address you specify for the neighbor must never be routed through the interface on which APS is configured, or instability will result. APS neighbor only applies to inter-router configurations. We strongly recommend that you directly connect the working and protect

routers and that you configure the interface address of this shared network as the neighbor address.

The working and protect configurations on the routers must match the circuit configurations on the ADM; that is, the working router must be connected to the ADM's working circuit and the protect router must be connected to the protect circuit.

To set up a basic APS configuration, include the following statements at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

On the Working Circuit

```
[edit interfaces so-fpc/pic/port sonet-options]
aps {
  working-circuit group-name;
  authentication-key key;
  neighbor address; # Include if protect circuit is on a different router
}
```

On the Protect Circuit

```
aps {
  protect-circuit group-name;
  authentication-key key;
  neighbor address; # Include if working circuit is on a different router
}
```

Example: Configuring Basic APS Support

Configure Router A to be the working router and Router B to be the protect router.

On Router A (the Working Router)

```
[edit interfaces so-6/1/1 sonet-options]
aps {
  working-circuit San-Jose;
  authentication-key " $9$B2612345" ;
}
```

On Router B (the Protect Circuit)

```
[edit interfaces so-0/0/0 sonet-options]
aps {
  protect-circuit San-Jose;
  authentication-key " $9$B2612345" ;
  neighbor 192.168.1.2;# Address of Router A on the link between A and B
}
```

On a Single Platform, One Interface as the Working Circuit and Another Interface as the Protect Circuit

```
[edit interfaces so-2/1/1 sonet-options]
aps {
  working-circuit bayward;
  authentication-key blarney;
}
[edit interfaces so-3/0/2 sonet-options]
aps {
  protect-circuit bayward;
  authentication-key blarney;
}
```

Configuring Container Interfaces

The Junos OS supports container interfaces for APS on SONETlinks. Physical interfaces and logical interfaces remain up on switchover, and their APS parameters are auto-copied

from the container interface to the member links. See Container Interfaces Overview for more information.

Container interfaces support the following features:

- Cisco HDLC or PPP encapsulation methods.
- Unpaired groups.
- Bidirectional APS.
- Non-container and container-based APS on the same system.
- Use of any combination of (nonchannelized) SONET interfaces installed on the same router.

To configure a container interface, you must first create the number of container devices that you require. You can create up to a maximum of 128 container interfaces per router using the **device-count** statement at the **[edit chassis container-devices]** hierarchy level. You can create more container interfaces later if required, up to 128 (total). The resulting container interfaces are designated sequentially from **ci0** up to a maximum of **ci127**, depending on the **device-count** ***number*** specified. SONET interfaces can be assigned to any container interface **ci*n***.

To configure each container interface, you must assign two SONET interfaces (**so-*fpc/pic/port***) using the **container-list ci*n*** statement, and specify the **member-interface-speed** ***speed*** and **container-options** for each SONET interface.

Within each of the two SONET interfaces' container options, you must set one container-type as **primary** (corresponding to an APS working circuit) and the other as **standby** (corresponding to an APS protect circuit). For each SONET interface, you can also use the **allow-configuration-override** statement to allow the physical configuration of a member link to override the container configuration.

The following configuration steps are required:

1. Specify the total number of container interfaces (up to 128) to create using the **device-count** ***number*** statement at the **[edit chassis container-devices]** hierarchy level:

   ```
   [edit chassis container-devices]
   user@host# set device-count number
   ```

2. Configure the container interface parameters for a specified container **ci*n*** as follows:

   a. Specify the container interface using the numbered identifier **ci*n***:

      ```
      [edit interfaces]
      user@host# edit cin
      ```

   b. Specify the container interface encapsulation as **cisco-hdlc** or **ppp**:

      ```
      [edit interfaces cin]
      user@host# set encapsulation (cisco-hdlc | ppp)
      ```

   c. Specify the container options **container-type** as **aps**; a SONET interface is required for APS selection:

```
[edit interfaces ci0]
user@host# set container-options container-type aps
```

d. Specify the container interface **member-interface type** as **sonet**:

```
[edit interfaces ci0]
user@host# set interfaces ci0 container-options member-interface-type sonet
```

e. Specify the container **member-interface-speed** ***speed*** to match the specified installed SONET interface links; the available values are ***OC3, OC12, OC48, OC192, OC768,*** or ***mixed***. The **member-interface-speed** ***speed*** statement setting applies to all SONET member interfaces of the specified container **ci0**.

```
[edit interfaces ci0]
user@host# set interfaces ci0 container-options member-interface-type sonet
  member-interface-speed speed
```

f. Specify the container interface's unit number, family, IP address, and mask:

```
[edit interfaces ci0]
user@host# set interfaces ci0 unit number family inet address ip-address/mask
```

3. Configure each of the required two SONET interfaces as follows:

a. Specify the SONET interfaces and their container options; including the **container-list**, identified by its **ci0**.

b. Specify the **container-type** as ***primary*** (corresponding to an APS working-circuit) or ***standby*** (corresponding to an APS protect-circuit).

For example, setting so-0/0/0 as the primary and so-0/0/1 as the standby SONET interfaces for container interface ci0:

```
[edit]
user@host#edit interfaces so-0/0/0 # Enter config mode for interface so-0/0/0
[edit interfaces so-0/0/0]
user@host# set container-options container-list ci0 primary # Set so-0/0/0 as
  APS primary interface
[edit interfaces so-0/0/0]
user@host# top
[edit]
user@host#edit interfaces so-0/0/1 # Enter config mode for interface so-0/0/1
[edit interfaces so-0/0/1]
user@host# set container-options container-list ci0 standby # Set so-0/0/1 as
  APS standby interface
```

Optionally, you can set the **allow-configuration-override** statement to allow the physical configuration of a member link to override the container configuration:

```
[edit interfaces so-0/0/1]
user@host# set container-options container-list ci0 standby
  allow-configuration-override
```

Example Container Interface Configuration

The following is a sample container interface configuration:

```
[edit chassis]
container-devices {
  device-count 1;
```

```
}
[edit interfaces]
so-1/0/2 {
    container-options {
        container-list ci0;
        primary;
    }
}
so-1/0/3 {
    container-options {
        container-list ci0;
        standby;
    }
}
ci0 {
    encapsulation cisco-hdlc;
    container-options {
        container-type aps {
            member-interface-type sonet {
                member-interface-speed mixed;
            }
        }
    }
    unit 0 {
        family inet {
            address 192.168.11.1/24;
        }
    }
}
```

You can run the **show aps** command to display the APS container interface configuration, as follows:

```
user@host> show aps
Interface    Group                          Circuit    Intf state
ci0           CONTAINER_ci0                 Container  enabled, up
so-1/2/2      MEMBER_OF_ci0                 Working    enabled, up
so-1/2/3      MEMBER_OF_ci0                 Protect    disabled, up
```

Configuring APS Using a Container Interface with ATM Encapsulation

M Series and T Series routers with ATM2 PICs automatically copy the parent container interface (CI) configuration to the specified children interfaces. All ATM configurations configured in a single location on the parent container interface are automatically copied to the children interfaces. Container interfaces do not go down during APS switchover, shielding upper layers (Layer 3 and above) from noticing the Layer 1 failures. This feature allows the various ATM features to work over the container ATM for APS.

For more information on container interfaces, see Container Interfaces Overview.

Configuring APS Using a Container Interface with ATM Encapsulation

To specify ATM children within a container interface, include the **container-list ci*n*** statement and **(primary | standby)** option at the **[edit interface at-*fpc/pic/slot* container-options]** hierarchy level.

To configure a container interface, including its children, include the **ci*n*** statement and its options at the **[edit interfaces]** hierarchy level.

Container ATM APS does not support interchassis APS.

MLPPP over ATM CI is not supported.

The following example shows the configuration of a parent container interface (**ci0**) and the resulting automatic configuration of its children (**at-0/0/0** and **at-0/0/1**):

```
[edit interfaces]
  at-0/0/0 {
    container-options {
      container-list ci0;
      primary;
    }
  }
  at-0/0/1 {
    container-options {
      container-list ci0;
      standby;
    }
  }
  ci0 {
    encapsulation atm-pvc;
    atm-options {
      vpi 0 {
        oam-period 3;
      }
      ilmi;
    }
    container-options {
      container-type {
        aps;
      }
      member-interface-type {
        atm {
          member-interface-speed oc3;
        }
      }
    }
    unit 0 {
      vci 100;
      oam-period 3;
      family inet {
        address 1.0.0.1/30;
      }
    }
    unit 1 {
      vci 200;
      oam-period 3;
      family inet {
        address 2.0.0.1/30;
      }
    }
  }
```

Viewing the APS Container Interface Configuration

You can use the following **show** commands to view the APS container interface configuration:

- **show aps**
- **show aps extensive**
- **show interfaces ci*n* extensive**
- **show interfaces at-*fpc/pic/port* extensive**

See the *Junos OS Interfaces Command Reference*.

Configuring Switching Between the Working and Protect Circuits

When there are multiple reasons to switch between the working and protect circuits, a priority scheme is used to decide which circuit to use. The routers and the ADM might automatically switch traffic between the working and protect circuits because of circuit and router failures. You can also choose to switch traffic manually between the working and protect circuits.

When an ATM2 PIC is configured for APS, and the protect circuit comes online for the first time, there are no open VCs and the PIC discards the input traffic received on the protect circuit. The **show interface extensive** or **show monitor interface traffic** commands display the statistics as zero since the PIC drops the packets at the VC.

When the APS switches from the working circuit to the protect circuit, VCs are created on the protect circuit to accept traffic. However, the VCs on the working circuit remain open to support any future APS switches even though the interface is down or disabled. The input traffic received on the working circuit (current backup) is accepted by the PIC but discarded in the PFE. The **show interface extensive** or **show monitor interface traffic** commands displays live statistics for the traffic since it is accepted by the PIC.

When APS switches from the protect circuit to the working circuit again, the VCs on the protect circuit remain open to support a future APS switch even though the interface is down or disabled. The input traffic received on the current backup protect circuit is accepted by the PIC but discarded in the PFE. The **show interface extensive** or the **show monitor interface traffic** command displays live statistics for this traffic since it is accepted by the PIC.

There are three priority levels of manual configuration, listed here in order from lowest to highest priority:

- Request (also known as manual switch)—Overridden by signal failures, signal degradations, or any higher-priority reasons.
- Force (also known as forced switch)—Overrides manual switches, signal failures, and signal degradation.
- Lockout (also known as lockout of protection)—Do not switch between the working and protect circuits.

NOTE: Do not use the **disable** statement at the **[edit interfaces *interface-name* aps]** hierarchy level to switch between interface working and protect circuits; it can cause loss of traffic on the disabled interface. Use only the **request** statement or the **force** statement at the **[edit interfaces interface-name aps]** hierarchy level to modify interface status.

A router failure is considered to be equivalent to a signal failure on a circuit.

To perform a manual switch, include the **request** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level. This statement is honored only if there are no higher-priority reasons to switch.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
request (protect | working);
```

When the working circuit is operating in nonrevertive mode, use the **request working** statement to switch the circuit manually to being the working circuit or to override the revert timer.

To perform a forced switch, include the **force** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level. This statement is honored only if there are no higher-priority reasons to switch. This configuration can be overridden by a signal failure on the protect circuit, thus causing a switch to the working circuit.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
force (protect | working);
```

To configure a lockout of protection, forcing the use of the working circuit and locking out the protect circuit regardless of anything else, include the **lockout** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options aps]
lockout;
```

M120 routers and M320 routers with Enhanced III FPCs support Annex B lockout.

The lockout feature is supported as follows:

- The selector position will be at what it was before the lockout feature was configured (no switching of working and protect circuits).
- Transmitted K1/K2 will be frozen (same K1 and K2 bytes will be transmitted as before the lockout).
- The APS will ignore requests from the peer to switch working and protect circuits.
- For Annex B, **lockout** must be configured on both local and remote ends, as they are not signaled using K1/K2 bytes as in a non Annex B configuration.

To configure Annex B lockout, use the **lockout** statement at the **[edit interfaces so-*fpc/pic/port* sonet-options aps]** hierarchy level.

```
interfaces so-x/y/z {
  sonet-options {
```

```
        aps {
          annex-b;
          lockout;
        }
      }
    }
```

To display an Annex B lockout configuration, use the **show aps extensive** command.

Configuring Revertive Mode

By default, APS is nonrevertive, which means that if the protect circuit becomes active, traffic is not switched back to the working circuit unless the protect circuit fails or you manually configure a switch to the working circuit. In revertive mode, traffic is automatically switched back to the working circuit.

You should configure the ADM and routers consistently with regard to revertive or nonrevertive mode.

To configure revertive mode, include the **revert-time** statement, specifying the amount of time to wait after the working circuit has again become functional before making the working circuit active again:

```
[edit interfaces so-fpc/pic/port sonet-options aps]
revert-time seconds;
```

If you are using nonrevertive APS, you can use the **request working** statement to switch the circuit manually to being the working circuit or to override the revert timer (configured with the **revert-time** statement).

Configuring Unidirectional Switching Mode Support

You can configure interoperation with SONET/SDH Line Terminating Equipment (LTE) that is provisioned for unidirectional linear APS in 1+1 architecture on the following interfaces:

- Unchannelized OC3, OC12, and OC48 SONET/SDH interfaces on T Series routers
- SONET/SDH interfaces on the M40e router
- ATM over SONET interfaces

By default, APS supports only SONET/SDH LTE that is provisioned for bidirectional mode.

In bidirectional switching mode, the working interface switches to the protect interface for both receipt and transmission of data, regardless of whether the signal failure is in the transmit or receive direction.

In true unidirectional mode, the working interface switches to the protect interface only for the direction in which signal failure occurs; for example, if there is a signal failure in the transmit direction, the working interface switches over to the protect interface for transmission but not receipt of data. When the protect interface operates in unidirectional mode, the working and protect interfaces must cooperate to operate the transmit and receive interfaces in a bidirectional fashion.

The Junos OS does not support true unidirectional mode. Instead the software supports interoperation with SONET/SDH LTE provisioned for unidirectional switching. This means that the SONET/SDH LTE on the router receives and transmits on one interface, even when you configure unidirectional support. The Junos implementation of unidirectional mode support allows the router to do the following:

- Accept a unidirectional mode as valid
- Trigger the peer (ADM) selector to switch receive from working interface to protect interface or the reverse
- Not send reverse requests to the far end (ADM)

To configure unidirectional mode support, include the **switching-mode unidirectional** statement, at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level:

```
[edit interfaces interface-name sonet-options aps]
switching-mode unidirectional;
```

NOTE: On interfaces with unidirectional APS support configured, revertive mode and load sharing between circuits are not supported.

To restore the default behavior, include the **switching-mode bidirectional** statement, at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level:

```
[edit interfaces interface-name sonet-options aps]
switching-mode bidirectional;
```

Configuring APS Timers

The protect and working routers periodically send packets to their neighbors to advertise that they are operational. By default, these advertisement packets are sent every 1000 milliseconds. A router considers its neighbor to be operational for a period, called the hold time, that is, by default, three times the advertisement interval. If the protect router does not receive an advertisement packet from the working router within the hold time configured on the protect router, the protect router assumes that the working router has failed and becomes active.

APS is symmetric; either side of a circuit can time out the other side (for example, when detecting a crash of the other). Under normal circumstances, the failure of the protect router does not cause any changes because the traffic is already moving on the working router. However, if you had configured **request protect** and the protect router failed, the working router would enable its interface.

To modify the advertisement interval, include the **advertise-interval** at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level:

```
[edit interfaces so-fpc/pic/port sonet-options aps]
advertise-interval milliseconds;
```

To modify the hold time, include the **hold-time** at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level:

[edit interfaces so-*fpc/pic/port* sonet-options aps]
hold-time *milliseconds*;

The advertisement intervals and hold times on the protect and working routers can be different.

Configuring Link PIC Redundancy

Link state replication, also called interface preservation, is an addition to the SONET Automatic Protection Switching (APS) functionality that helps promote redundancy of link PICs used in LSQ configurations, providing MLPPP link redundancy at the port level.

Link state replication provides the ability to add two sets of links, one from the active SONET PIC and the other from the standby SONET PIC, to the same bundle. If the active SONET PIC fails, links from the standby PIC are used without link renegotiation. All the negotiated state is replicated from the active links to the standby links to prevent link renegotiation. For more information about LSQ configurations, see the *Junos OS Services Interfaces Configuration Guide*.

To configure link state replication, include the **preserve-interface** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level on the interfaces on both PICs:

preserve-interface;

APS functionality must be available on the SONET PICs and the interface configurations must be identical on both ends of the link. Any configuration mismatch causes the commit operation to fail.

This feature is supported with SONET APS and the following link PICs:

- Channelized OC3 IQ and IQE PICs
- Channelized OC12 IQ and IQE PICs
- Channelized STM1 IQ and IQE PICs

Link state replication supports MLPPP and PPP over Frame Relay (**frame-relay-ppp**) encapsulation, and fully supports GRES.

Example: Configuring Link PIC Redundancy

Configure link state replication configuration between the ports **coc3-1/0/0** and c**oc3-2/0/0**.

```
interfaces {
    coc3-1/0/0 {
        sonet-options {
            aps {
                preserve-interface;
                working-circuit aps-group-1;
            }
        }
    }
    coc3-2/0/0 {
        sonet-options {
```

```
        aps {
          preserve-interface;
          working-circuit aps-group-1;
        }
      }
    }
  }
```

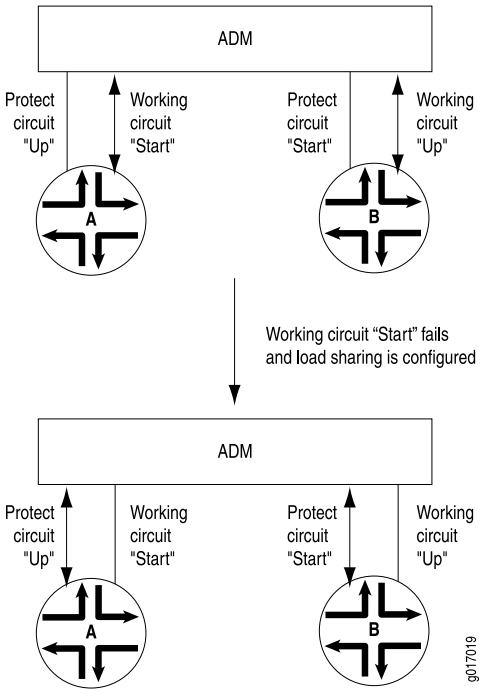
Configuring APS Load Sharing Between Circuit Pairs

When two routers are connected to a single add/drop multiplexer (ADM), you can have them back up each other on two different pairs of circuits. This arrangement provides load balancing between the routers if one of the working circuits fails.

Figure 2 on page 58 illustrates load sharing between circuits on two routers. Router A has a working circuit “Start” and a protect circuit “Up,” and Router B has a working circuit “Up” and a protect circuit “Start.” Under normal circumstances, Router A carries the “Start” circuit traffic and Router B carries the “Up” circuit traffic. If the working circuit “Start” were to fail, Router B would end up carrying all the traffic for both the “Start” and “Up” circuits.

To balance the load between the circuits, you pair the two circuits. In this case, you pair the “Start” and “Up” circuits. Then, if the working circuit “Start” fails, the two routers automatically switch the “Up” traffic from the working to the protect circuit so that each router is still carrying only one circuit’s worth of traffic. That is, the working circuit on Router A would be “Up” and the working circuit on Router B would be “Start.”

Figure 2: APS Load Sharing Between Circuit Pairs



To configure load sharing between two working–protect circuit pairs, include the **paired-group** statement when configuring one of the circuits on one of the routers. In this

statement, the ***group-name*** is the name of the group you assigned to one of the circuits with the **working-circuit** and **protect-circuit** statements. The Junos OS automatically configures the remainder of the load-sharing setup based on the group name.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
paired-group group-name;
```

Example: Configuring APS Load Sharing Between Circuit Pairs

Configure APS load sharing to match the configuration shown in Figure 2 on page 58:

On Router A

```
[edit interfaces so-7/0/0 sonet-options aps]
user@host# set working-circuit start
[edit interfaces so-7/0/0 sonet-options aps]
user@host# set authentication-key linsey
[edit interfaces so-7/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
...
[edit interfaces so-0/0/0 sonet-options aps]
user@host# set protect-circuit up
[edit interfaces so-0/0/0 sonet-options aps]
user@host# set authentication-key woolsey
[edit interfaces so-0/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
```

On Router B

```
[edit interfaces so-1/0/0 sonet-options aps]
user@host# set working-circuit up
[edit interfaces so-1/0/0 sonet-options aps]
user@host# set authentication-key woolsey
[edit interfaces so-1/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
...
[edit interfaces so-6/0/0 sonet-options aps]
user@host# set protect-circuit start
[edit interfaces so-6/0/0 sonet-options aps]
user@host# set authentication-key linsey
[edit interfaces so-6/0/0 sonet-options aps]
user@host# set paired-group "Router A-Router B"
```

Configuring SONET Options for 10-Gigabit Ethernet Interfaces

The 10-Gigabit Ethernet IQ2 and IQ2-E PIC is supported on the M120, M320, and T Series routers. The PIC provides one external interface running at 10 Gbps. The interface operates in either LAN PHY or WAN PHY mode. When the external interface is running in WAN PHY mode, it uses the WIS sublayer to transport 10-Gigabit Ethernet frames in an OC192c SONET payload, and can interoperate with SONET section or line level repeaters. This creates an advantage when the interface is used for long-distance, point-to-point 10-Gigabit Ethernet links.

When the external interface is running in WAN PHY mode, you can configure specific physical SONET options. To configure SONET options, include the **loopback**, **mpls**, **path-trace**, and **trigger** statements at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces]
xe-0/0/0 {
  sonet-options {
    loopback (local | remote);
    mpls {
      pop-all-labels {
        required-depth number;
      }
    }
    path-trace trace-string;
    trigger {
      defect ignore {
        defect hold-time up milliseconds down milliseconds;
      }
    }
  }
}
```

For information about using the **loopback** statement, see "Configuring SONET/SDH Loopback Capability" on page 38. For information about using the **mpls** statement, see "Removing MPLS Labels from Incoming Packets" on page 61. For information about using the **path-trace** statement, see "Configuring the SONET/SDH Path Trace Identifier" on page 40. For information about using the **trigger** statement, see "Configuring SONET/SDH Defect Triggers to Be Ignored" on page 41.

Configuring the Media MTU on SONET/SDH Interfaces

The default media MTU size used on a physical interface depends on the encapsulation being used on that interface. For a listing of MTU sizes for each encapsulation type, see Configuring the Media MTU. For information about configuring the encapsulation on an interface, see "Configuring Interface Encapsulation on SONET/SDH Interfaces" on page 65.

To modify the default media MTU size for a physical interface, include the **mtu** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
mtu bytes;
```

If you change the size of the media MTU, you must ensure that the size is equal to or greater than the sum of the protocol MTU and the encapsulation overhead. You configure the protocol MTU by including the **mtu** statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* family *family*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]**

For more information, see Setting the Protocol MTU.

Enabling Passive Monitoring on SONET/SDH Interfaces

The Monitoring Services I and Monitoring Services II PICs are designed to enable IP services. If you have a Monitoring Services PIC and a SONET/SDH PIC installed in an M Series, MX Series, or T Series router, you can monitor IPv4 and IPv6 traffic from another router.

On SONET/SDH interfaces, you enable packet flow monitoring by including the **passive-monitor-mode** statement:

```
passive-monitor-mode;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces so-*fpc/pic/port* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces so-*fpc/pic/port* unit *logical-unit-number*]**

If you include the **passive-monitor-mode** statement in the configuration, the SONET/SDH interface does not send keepalives or alarms, and does not participate actively on the network.

On monitoring services interfaces, you enable packet flow monitoring by including the **family** statement at the **[edit interfaces mo-*fpc/pic/port* unit *logical-unit-number*]** hierarchy level, specifying the **inet** option:

```
[edit interfaces mo-fpc/pic/port unit logical-unit-number]
family inet;
```

For conformity with cflowd record structure, you must include the **receive-options-packets** and **receive-ttl-exceeded** statements at the **[edit interfaces mo-*fpc/pic/port* unit *logical-unit-number* family inet]** hierarchy level:

```
[edit interfaces mo-fpc/pic/port unit logical-unit-number family inet]
receive-options-packets;
receive-ttl-exceeded;
```

For the monitoring services interface, you can configure multiservice physical interface properties. For more information, see Configuring Multiservice Physical Interface Properties and the *Junos OS Services Interfaces Configuration Guide*.

Removing MPLS Labels from Incoming Packets

The Junos OS can forward only IPv4 packets to a Monitoring Services PIC. IPv4 packets with MPLS labels cannot be forwarded to a Monitoring Services PIC. By default, if packets with MPLS labels are forwarded to the Monitoring Services PIC, they are discarded. To monitor packets with MPLS labels, you must remove the MPLS labels as the packets arrive on the interface.

You can remove up to two MPLS labels from an incoming packet by including the **pop-all-labels** statement at the **[edit interfaces *interface-name* sonet-options mpls]** hierarchy level:

```
[edit interfaces interface-name sonet-options mpls]
pop-all-labels {
  required-depth number;
}
```

By default, the **pop-all-labels** statement takes effect for incoming packets with one or two labels. You can specify the number of MPLS labels an incoming packet must have

for the **pop-all-labels** statement to take effect by including the **required-depth** statement at the **[edit interfaces *interface-name* atm-options mpls pop-all-labels]** hierarchy level:

```
[edit interfaces interface-name atm-options mpls pop-all-labels]
required-depth number;
```

The required depth can be **1**, **2**, or **[1 2]**. If you include the **required-depth 1** statement, the **pop-all-labels** statement takes effect for incoming packets with one label only. If you include the **required-depth 2** statement, the **pop-all-labels** statement takes effect for incoming packets with two labels only. If you include the **required-depth [1 2]** statement, the **pop-all-labels** statement takes effect for incoming packets with one or two labels. A required depth of **[1 2]** is equivalent to the default behavior of the **pop-all-labels** statement.

When you remove MPLS labels from incoming packets, note the following:

- The **pop-all-labels** statement has no effect on IP packets with three or more MPLS labels.
- When you enable MPLS label removal, you must configure all ports on a PIC with the same label popping mode and required depth.
- You use the **pop-all-labels** statement to enable passive monitoring applications, not active monitoring.
- You cannot apply MPLS filters or accounting to the MPLS labels because the labels are removed as soon as the packet arrives on the interface.

Configuring the Clock Source on SONET/SDH Interfaces

For interfaces such as SONET/SDH that can use different clock sources, you can configure the source of the transmit clock on each interface. The source can be internal or external. The default source is internal, which means that each interface uses the router's internal Stratum 3 clock.

For DS3 channels on a channelized OC12 interface, the **clocking** statement is supported only for channel 0; it is ignored if included in the configuration of channels 1 through 11. The clock source configured for channel 0 applies to all channels on the channelized OC12 interface. The individual DS3 channels use a gapped 45-MHz clock as the transmit clock. For more information, see Clock Sources on Channelized Interfaces.

NOTE: On channelized STM1 interfaces, you should configure the clock source at one side of the connection to be internal (the default Junos OS configuration) and configure the other side of the connection to be external.

To configure loop timing on an interface, include the **clocking external** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
clocking external;
```

To explicitly configure line timing on an interface, include the **clocking internal** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
clocking internal;
```

Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces

Congestion control is particularly difficult in high-speed networks with high volumes of traffic. When congestion occurs in such a network, it is usually too late to react. You can avoid congestion by regulating the flow of packets into your network. Smoother flows prevent bursts of packets from arriving at (or being transmitted from) the same interface and causing congestion.

For all interface types except ATM, Fast Ethernet, Gigabit Ethernet, and channelized IQ and IQE, you can configure leaky bucket properties, which allow you to limit the amount of traffic received on and transmitted by a particular interface. You effectively specify what percentage of the interface's total capacity can be used to receive or transmit packets. You might want to set leaky bucket properties to limit the traffic flow from a link that is known to transmit high volumes of traffic.

NOTE: Instead of configuring leaky bucket properties, you can limit traffic flow by configuring policers. Policers work on all interfaces. For more information, see the *Junos OS Routing Policy Configuration Guide*.

The leaky bucket is used at the host-network interface to allow packets into the network at a constant rate. Packets might be generated in a bursty manner, but after they pass through the leaky bucket, they enter the network evenly spaced. In some cases, you might want to allow short bursts of packets to enter the network without smoothing them out. By controlling the number of packets that can accumulate in the bucket, the **threshold** property controls burstiness. The maximum number of packets entering the network in **t** time units is **threshold + rate * t**.

By default, leaky buckets are disabled and the interface can receive and transmit packets at the maximum line rate.

For each DS3 channel on a channelized OC12 interface, you can configure unique receive and transmit buckets.

NOTE: HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling, because the Junos OS rejects configurations that have both features enabled. For more information, see "Configuring SONET/SDH HDLC Payload Scrambling" on page 40.

To configure leaky bucket properties, include one or both of the **receive-bucket** and **transmit-bucket** statements at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
receive-bucket {
  overflow (discard | tag);
  rate percentage;
  threshold bytes;
}
transmit-bucket {
  overflow discard;
  rate percentage;
  threshold bytes;
}
```

In the **rate** statement, specify the percentage of the interface line rate that is available to receive or transmit packets. The percentage can be a value from 0 (none of the interface line rate is available) to 100 (the maximum interface line rate is available). For example, when you set the line rate to 33, the interface receives or transmits at one third of the maximum line rate.

In the **threshold** statement, specify the bucket threshold, which controls the burstiness of the leaky bucket mechanism. The larger the value, the more bursty the traffic, which means that over a very short amount of time the interface can receive or transmit close to line rate, but the average over a longer time is at the configured bucket rate. The threshold can be a value from 0 through 65,535 bytes. For ease of entry, you can enter ***number*** either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1,000). For example, the entry **threshold 2k** corresponds to a threshold of 2,000 bytes.

In the **overflow** option, specify how to handle packets that exceed the threshold:

- **tag**—(**receive-bucket** only) Tag, count, and process received packets that exceed the threshold.
- **discard**—Discard received packets that exceed the threshold. No counting is done.

Damping Interface Transitions on SONET/SDH Interfaces

By default, when an interface changes from being up to being down, or from down to up, this transition is advertised immediately to the hardware and the Junos OS. In some situations—for example, when an interface is connected to an add-drop multiplexer (ADM) or wavelength-division multiplexer (WDM), or to protect against SONET/SDH framer holes—you might want to damp interface transitions. This means not advertising the interface's transition until a certain period of time has transpired.

When you have damped interface transitions and the interface goes from up to down, the interface is not advertised to the rest of the system as being down until it has remained down for the hold-time period. Similarly when an interface goes from down to up, it is not advertised as being up until it has remained up for the hold-time period.

To damp interface transitions, include the **hold-time** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
hold-time up milliseconds down milliseconds;
```

The time can be a value from 0 through 4,294,967,295 milliseconds. The default value is 0, which means that interface transitions are not damped. The Junos OS advertises the transition within 100 milliseconds of the time value you specify.

Configuring Interface Encapsulation on SONET/SDH Interfaces

Point-to-Point Protocol (PPP) encapsulation is the default encapsulation type for physical interfaces. You need not configure encapsulation for any physical interfaces that support PPP encapsulation. If you do not configure encapsulation, PPP is used by default. For physical interfaces that do not support PPP encapsulation, you must configure an encapsulation to use for packets transmitted on the interface. You can optionally configure an encapsulation on a logical interface, which is the encapsulation used within certain packet types.

Configuring the Encapsulation on a Physical SONET/SDH Interface

For SONET/SDH interfaces, the physical interface encapsulation can be one of the following:

- Point-to-Point Protocol (PPP)—PPP encapsulation is defined in RFC 1661, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*. PPP is the default encapsulation type for physical interfaces. Two related versions are supported:
  - Circuit cross-connect (CCC) version (**ppp-ccc**)—The logical interfaces do not require an encapsulation statement. When you use this encapsulation type, you can configure the **ccc** family only.
  - Translational cross-connect (TCC) version (**ppp-tcc**)—Similar to CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.
- Cisco HDLC—E1, E3, SONET/SDH, T1, and T3 interfaces can use Cisco HDLC encapsulation. Two related versions are supported:
  - CCC version (**cisco-hdlc-ccc**)—The logical interfaces do not require an encapsulation statement. When you use this encapsulation type, you can configure the **ccc** family only.
  - TCC version (**cisco-hdlc-tcc**)—Similar to CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.
- Frame Relay—Defined in RFC 1490, *Multiprotocol Interconnect over Frame Relay*. E1, E3, SONET/SDH, T1, and T3 interfaces can use Frame Relay encapsulation. Two related versions are supported:
  - CCC version (**frame-relay-ccc**)—The same as standard Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to CCC. This numbering restriction does not apply to IQ and IQE interfaces. The logical interface must also have **frame-relay-ccc** encapsulation.

  - TCC version (**frame-relay-tcc**)—Similar to Frame Relay CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

- Frame Relay Ether Type (**frame-relay-ether-type**)—Physical interfaces can use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. IETF Frame Relay encapsulation identifies the payload format using NLPID and SNAP formats. Cisco-compatible Frame Relay encapsulation uses the Ethernet type to identify the type of payload. Two related versions are supported:
  - TCC version (**frame-relay-ether-type-tcc**)—Cisco-compatible Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to TCC. This numbering restriction does not apply to IQ and IQE interfaces. This encapsulation is used for circuits with different media on either side of the connection.
  - Extended TCC version (**extended-frame-relay-ether-type-tcc**)—This encapsulation allows you to dedicate Cisco-compatible Frame Relay TCC for DLCIs 1 through 1022. This encapsulation is used for circuits with different media on either side of the connection. All ether type TCC encapsulation is supported on the same PICs as non-ether type Frame Relay TCC encapsulation.

NOTE: **When the encapsulation type is set to Cisco-compatible Frame Relay encapsulation, ensure that the LMI type is set to ANSI or Q933-A.**

To configure the encapsulation on a physical interface, include the **encapsulation** statement at the **[edit interfaces *interface-name*]** hierarchy level:

```
[edit interfaces interface-name]
encapsulation (cisco-hdlc | cisco-hdlc-ccc | cisco-hdlc-tcc | frame-relay | frame-relay-ccc |
  frame-relay-tcc | frame-relay-tcc | ppp | ppp-ccc | ppp-tcc);
```

When you configure a point-to-point encapsulation (such as PPP or Cisco HDLC) on a physical interface, the physical interface can have only one logical interface (that is, only one **unit** statement) associated with it. When you configure a multipoint encapsulation (such as Frame Relay), the physical interface can have multiple logical units, and the units can be either point to point or multipoint. Use PPP if you are running Cisco IOS Release 12.0 or later. If you need to run Cisco HDLC, the Junos OS automatically configures an ISO family MTU of 4469 in the router. This is due to an extra byte of padding used by Cisco.

For more information about physical interface encapsulation, see Configuring Interface Encapsulation on Physical Interfaces.

Example: Configuring the Encapsulation on a Physical SONET/SDH Interface

Configure PPP encapsulation on a SONET/SDH interface. The second two **family** statements allow IS-IS and MPLS to run on the interface.

```
[edit interfaces]
so-7/0/0 {
  encapsulation ppp;
```

```
    unit 0 {
      point-to-point;
      family inet {
        address 192.168.1.113/32 {
          destination 192.168.1.114;
        }
      }
      family iso;
      family mpls;
    }
  }
```

Configuring the Encapsulation on a Logical SONET/SDH Interface

Generally, you configure an interface's encapsulation at the **[edit interfaces** *interface-name***]** hierarchy level. However, for Frame Relay encapsulation, you can also configure the encapsulation type that is used inside the Frame Relay packet itself. To do this, include the **encapsulation** statement, specifying the **frame-relay-ccc frame-relay-tcc**, **frame-relay-ether-type**, or **frame-relay-ether-type-tcc** option:

```
encapsulation (frame-relay-ccc | frame-relay-tcc | frame-relay-ether-type |
  frame-relay-ether-type-tcc);
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces** *interface-name* **unit** *logical-unit-number***]**
- **[edit logical-systems** *logical-system-name* **interfaces** *interface-name* **unit** *logical-unit-number***]**

The ATM encapsulations are defined in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*.

With the **atm-nlpid**, **atm-cisco-nlpid**, and **atm-vc-mux** encapsulations, you can configure the **inet** family only. With the circuit cross-connect (CCC) encapsulations, you cannot configure a family on the logical interface. A logical interface cannot have **frame-relay-ccc** encapsulation unless the physical device also has **frame-relay-ccc** encapsulation. A logical interface cannot have **frame-relay-tcc** encapsulation unless the physical device also has **frame-relay-tcc** encapsulation. In addition, you must assign this logical interface a DLCI from 512 through 1022. This numbering restriction does not apply to IQ and IQE interfaces. You must configure the logical interface as point-to-point.

For more information about logical interface encapsulation, see Configuring Interface Encapsulation on Logical Interfaces.

Example: Configuring SONET/SDH Interfaces

SONET/SDH interfaces can use either PPP or Cisco HDLC encapsulation. Use PPP if you are running Cisco IOS Release 12.0 or later. If you need to run Cisco HDLC, the Junos OS automatically configures an ISO family MTU of 4469 in the router. This is due to an extra byte of padding used by Cisco. The following configuration, which uses PPP encapsulation, is sufficient to get a SONET/SDH OC3 or OC12 interface up and running:

```
[edit interfaces]
```

```
so-fpc/pic/port {
  encapsulation ppp;
  unit 0 {
    family inet {
      address local-address {
        destination remote-address;
      }
    }
  }
}
```

Configuring Aggregated SONET/SDH Interfaces

The Junos OS enables link aggregation of SONET/SDH interfaces; this is similar to Ethernet link aggregation, but is not defined in a public standard. The Junos OS balances traffic across the member links within an aggregated SONET/SDH bundle based on the Layer 3 information carried in the packet. This implementation uses the same load balancing algorithm used for per-packet load balancing. For information about per-packet load balancing, see the *Junos OS Routing Protocols Configuration Guide*.

You configure an aggregated SONET/SDH virtual link by specifying the link number as a physical device and then associating a set of physical interfaces that have the same speed. Channelized OC IQ, IQE, and SONET/SDH OC48/STM16 IQE PICs do not support SONET aggregation.

By default, no aggregated SONET/SDH interfaces are created. You must define the number of aggregated SONET/SDH interfaces by including the **device-count** statement at the **[edit chassis aggregated-devices sonet]** hierarchy level:

```
[edit chassis aggregated-devices sonet]
device-count number;
```

The maximum number of aggregated interfaces is 16. The aggregated SONET/SDH interfaces are numbered from **as0** through **as15**. For more information, see the *Junos OS Services Interfaces Configuration Guide*.

NOTE: SONET/SDH aggregation is proprietary to the Junos OS and might not work with other software.

To configure aggregated SONET/SDH interfaces, assign a number for the aggregated SONET/SDH interface **as***x* at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
asx {
  ...
}
```

The following example shows an aggregated SONET/SDH configuration:

```
[edit interfaces]
as0 {
  aggregated-sonet-options {
```

```
        minimum-links 1;
        link-speed oc3;
      }
      unit 0 {
        family inet {
          address 10.2.11.1/30;
        }
      }
    }
```

You also need to specify the constituent physical interfaces by including the **aggregate** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level; for more information, see "Configuring SONET/SDH Link Aggregation" on page 69. You can optionally specify other physical properties that apply specifically to the aggregated SONET/SDH interfaces; for details, see "Configuring SONET/SDH Physical Interface Properties" on page 28. For a sample configuration, see "Example: Configuring Aggregated SONET/SDH Interfaces" on page 72.

To remove the configuration statements related to **as*x*** and set the aggregated SONET/SDH interface to down state, delete the interface from the configuration:

```
[edit]
user@host# delete interfaces asx
```

However, the aggregated SONET/SDH interface is not deleted until you delete the **chassis aggregated-devices sonet device-count** configuration statement.

You can configure the following aggregated SONET/SDH properties:

Configuring SONET/SDH Link Aggregation

On SONET/SDH interfaces, you can associate a physical interface with an aggregated SONET/SDH interface. To associate the interface with an aggregated SONET/SDH link, include the **aggregate** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level:

```
[edit interfaces interface-name sonet-options]
aggregate asx;
```

x is the interface instance number and can be from 0 through 15, for a total of 16 aggregated interfaces. You should not mix SONET and SDH mode on the same aggregated interface. You must also include a statement configuring **as*x*** at the **[edit interfaces]** hierarchy level. For a sample configuration, see "Example: Configuring Aggregated SONET/SDH Interfaces" on page 72.

Configuring Aggregated SONET/SDH Link Speed

On aggregated SONET/SDH interfaces, you can set the required link speed for all interfaces included in the bundle, or specify that the bundle contains interfaces with mixed interface speeds.

NOTE: For nonconcatenated interfaces on aggregated SONET/SDH interfaces, you can configure the link speed of the aggregate to match the speed of the nonconcatenated interface. For example, an OC12 PIC can have nonconcatenated interfaces with a link speed of OC3.

To set the required link speed or specify mixed interface speeds, include the **link-speed** statement at the **[edit interfaces *interface-name* aggregated-sonet-options]** hierarchy level:

```
[edit interfaces interface-name aggregated-sonet-options]
link-speed (speed | mixed);
```

The link speed can be one of the following values:

- **oc3**—Links are OC3c or STM1c.
- **oc12**—Links are OC12c or STM4c.
- **oc48**—Links are OC48c or STM16c.
- **oc192**—Links are OC192c or STM64c.
- **oc768**—Links are OC768c or STM256c.

Configuring Aggregated SONET/SDH Minimum Links

On aggregated SONET/SDH interfaces, you can configure the minimum number of links that must be up for the bundle as a whole to be labeled **up**. By default, only one link must be up for the bundle to be labeled **up**.

To configure the minimum number of links, include the **minimum-links** statement at the **[edit interfaces *interface-name* aggregated-sonet-options]** hierarchy level:

```
[edit interfaces interface-name aggregated-sonet-options]
minimum-links number;
```

On a T Series, TX Matrix router with SONET interfaces, the valid range for **minimum-links *number*** is from 1 through 16. When the maximum value (16) is specified, all configured links of a bundle must be up for the bundle to be labeled **up**.

On all other router routers, the range of valid values for **minimum-links *number*** is 1 through 8 and the maximum number of links supported in an aggregate is eight. When the maximum value (8) is specified, all configured links of a bundle must be up for the bundle to be labeled **up**.

Configuring Filters or Sampling on Aggregated SONET/SDH Links

To set up firewall filters or sampling on aggregated SONET/SDH interfaces, you must configure the **as*x*** interface with these properties. The filters function in the same manner as on other interfaces.

To configure a filter, include the **filter** statement:

```
filter {
    input input-filter-name;
    output output-filter-name;
}
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces as *x* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces as*x* unit *logical-unit-number*]**

You must also configure separate statements that define the properties of the filter. For more information, see the *Junos OS Routing Policy Configuration Guide* and "Examples: Configuring Filters or Sampling on Aggregated SONET/SDH Links" on page 71.

Examples: Configuring Filters or Sampling on Aggregated SONET/SDH Links

Configure filtering on aggregated SONET/SDH interfaces:

```
[edit interfaces]
asx {
    unit 0 {
        family inet {
            address 10.2.11.1/30;
            filter {
                input input-filter-name;
                output output-filter-name;
            }
        }
    }
}
```

Defining the Filter

```
[edit firewall]
filter input-filter-name {
    term match-any-input {
        then {
            accept;
        }
    }
}
filter output-filter-name {
    term match-any-output {
        then {
            accept;
        }
    }
}
```

Configuring Sampling on an Aggregated SONET/SDH Interface

```
[edit interfaces]
asx {
  unit 0 {
    family inet {
      address 10.2.11.1/30;
      filter {
        input input-sampler-name;
      }
    }
  }
}
```

Defining the Sampling Filter and the Forwarding Action

```
[edit firewall]
filter input-sampler-name {
  term match-any-input {
    then {
      sample;
      accept;
    }
  }
}
[edit forwarding-options]
sampling {
  input {
    family inet {
      rate 10000;
      run-length 1;
    }
  }
}
```

Example: Configuring Aggregated SONET/SDH Interfaces

The following configuration is sufficient to get an aggregated SONET/SDH interface up and running:

```
[edit interfaces]
as0 {
  aggregated-sonet-options {
    minimum-links 1;
    link-speed oc3;
  }
  unit 0 {
    family inet {
      address 10.2.11.1/30;
    }
  }
}
[edit chassis]
aggregated-devices {
  sonet {
    device-count 15;
  }
}
[edit interfaces]
```

```
so-1/3/0 {
  sonet-options {
    aggregate as0;
  }
}
```

Configuring Multicast Statistics Collection on Aggregated SONET Interfaces

T Series and TX Matrix routers support multicast statistics collection on aggregated SONET interfaces in both ingress and egress directions. The multicast statistics functionality can be configured on a physical interface thus enabling multicast accounting for all the logical interfaces below the physical interface.

The multicast statistics information is displayed only when the interface is configured with the **multicast-statistics** statement, which is not enabled by default.

Multicast statistics collection requires at least one logical interface is configured with family inet and/or inet6; otherwise, the commit for **multicast-statistics** will fail.

The multicast in/out statistics can be obtained via interfaces statistics query through CLI and via MIB objects through SNMP query.

To configure multicast statistics:

1. Include the **multicast-statistics** statement at the **[edit interfaces interface-name]** hierarchy level.

An example of a multicast statistics configuration for an aggregated SONET interface follows:

```
[edit interfaces]
as0 {
  multicast-statistics;
}
```

To display multicast statistics, use the **show interfaces *interface-name* statistics detail** command.

Related Documentation

- multicast-statistics
- Configuring Multicast Statistics Collection on SONET Interfaces

PART 3

SONET/SDH Interface Configuration Statements

CHAPTER 3

Summary of SONET/SDH Interfaces Configuration Statements

The following descriptions explain each of the interface configuration statements. The statements are organized alphabetically.

advertise-interval

Syntax advertise-interval *milliseconds*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Modify the Automatic Protection Switching (APS) interval at which the protect and working routers send packets to their neighbors to advertise that they are operational. A router considers its neighbor to be operational for a period, called the hold time, that is, by default, three times the advertisement interval.

Options ***milliseconds***—Interval between advertisement packets.

Range: 1 through 65,534 milliseconds

Default: 1000 milliseconds

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

Related Documentation

- Configuring APS Timers on page 56

aggregate (SONET/SDH)

Syntax aggregate as*x*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify aggregated SONET/SDH logical interface number.

Options as*x*—Aggregated SONET/SDH logical interface number.
Range: 0 through 15

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

Related Documentation
- Configuring Aggregated SONET/SDH Interfaces on page 68

aggregated-sonet-options

Syntax
```
aggregated-sonet-options {
  link-speed speed;
  minimum-links number;
}
```

Hierarchy Level [edit interfaces as*x*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure aggregated SONET/SDH-specific interface properties.

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
- Configuring Aggregated SONET/SDH Interfaces on page 68

annex

Syntax annex (annex-a | annex-b);

Hierarchy Level [edit interfaces *interface-name* shdsl-options],
[edit interfaces *interface-name* sonet-options aps],
[edit logical-systems *logical-system-name* interfaces *interface-name* shdsl-options]

Release Information Statement introduced in Junos OS Release 7.4.

Description For J Series Services Routers only, configure the type of SHDSL annex.

For M320 and M120 routers only, for Multiplex Section Protection (MSP) switching on SDH interfaces, set **annex-b**. You must also configure the **working protection circuit** under the **[edit interfaces so-*fpc/pic/port* sonet-options aps]** hierarchy level.

Default **annex-b**

Options **annex-a**—Use for North American SHDSL network implementations.

annex-b—Use for European SHDSL network implementations.

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

Related Documentation
- ATM-over-SHDSL Overview

aps

Syntax

```
aps {
  advertise-interval milliseconds;
  annex-b
  authentication-key key;
  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;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure Automatic Protection Switching (APS) on the router.

For DS3 channels on a channelized OC12 interface, configure APS on channel 0 only. If you configure APS on channels 1 through 11, it is ignored.

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

- Configuring APS and MSP on page 45

atm-options

Syntax

```
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 {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst
        length);
      queue-length number;
    }
  }
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure ATM-specific physical interface properties.

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
- Interface Encapsulations Overview
- multipoint-destination
- shaping
- vci

authentication-key

Syntax
authentication-key *key*;

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure the Automatic Protection Switching (APS) authentication key (password).

Options
key—Authentication password. It can be 1 through 8 characters long. Configure the same key for both the working and protect routers.

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

Related Documentation
- Configuring Basic APS Support on page 47
- For information about the **authentication-key** statement at the **[edit interfaces *interface-name* unit *unit-number* family inet address *address* (vrrp-group | vrrp-inet6-group) *group-number*]** or **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-number*]** hierarchy level, see the *Junos OS High Availability Configuration Guide*.

bytes

Syntax

```
bytes {
  c2 value;
  e1-quiet value;
  f1 value;
  f2 value;
  s1 value;
  z3 value;
  z4 value;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Set values in some SONET/SDH header bytes.

Options

c2 *value*—Path signal label SONET/SDH overhead byte. SONET/SDH frames use the C2 byte to indicate the contents of the payload inside the frame. SONET/SDH interfaces use the C2 byte to indicate whether the payload is scrambled.

Range: 0 through 255

Default: 0xCF

e1-quiet *value*—Default idle byte sent on the orderwire SONET/SDH overhead bytes. The router does not support the orderwire channel, and hence sends this byte continuously.

Range: 0 through 255

Default: 0x7F

f1 *value*, **f2 *value***, **z3 *value***, **z4 *value***—SONET/SDH overhead bytes.

Range: 0 through 255

Default: 0x00

s1 *value*—Synchronization message SONET overhead byte. This byte is normally controlled as a side effect of the system reference clock configuration and the state of the external clock coming from an interface if the system reference clocks have been configured to use an external reference.

Range: 0 through 255

Default: 0xCC

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

Related Documentation

- Configuring SONET/SDH Header Byte Values on page 35
- no-concatenate

clocking

Syntax clocking (external [interface *interface-name*] | internal);

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.
interface option added in Junos OS Release 8.2.

Description For interfaces that can use various clock sources, configure the source of the transmit clock on each interface.

Options **external**—The clock source is provided by the data communication equipment (DCE).

interface *interface-name*—For interfaces operating on T1/E1 PIMs for J Series Services Routers only, configure clocking for the drop-and insert feature. When configuring this feature, both ports must use the same clock source: either the router's internal clock or an external clock on one of the interfaces. If an external clock source is required, one interface must specify clocking external and the other must specify the same clock.

internal—Use the internal stratum 3 clock as the reference clock.

Default: **internal**

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

Related Documentation

- Configuring the Clock Source
- Configuring the Clock Source on SONET/SDH Interfaces on page 62
- Clock Sources on Channelized Interfaces
- Configuring a Channelized T1/E1 Interface to Drop and Insert Time Slots
- loop-timing on page 103

container-devices

Syntax

```
container-devices {
  device-count number;
}
```

Hierarchy Level [edit chassis]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the container devices configuration. The **number** option specifies the number of sequentially numbered container interfaces, from **ci0** to **ci127** maximum.

Options **number**—Number of container devices.

Range: 1 through 128

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

Related Documentation

- Configuring Container Interfaces on page 48

container-list

Syntax container-list [*container-interface-names*];

Hierarchy Level [edit interfaces container-options]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify a list of container interfaces; for example: **ci*0***, **ci*1***, and up to **ci*127***.

Options ***container-interface-names***—Name of each container interface.

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

Related Documentation

- Configuring Container Interfaces on page 48
- container-options on page 86

container-options

Syntax

```
container-options {
  container-list [ container-interface-names ];
  container-type aps;
  member-interface-type sonet {
    member-interface-speed [ speed ];
  }
}
```

Hierarchy Level [edit interfaces]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the container interface options.

Options **interface-name**—Name of the SONET or the container interface.

aps—Specify the member link interface type of the container as APS.

sonet—Protocol type of the container interface.

speed—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.

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

Related Documentation

- Configuring Container Interfaces on page 48

container-type

Syntax container-type *aps*;

Hierarchy Level [edit interfaces container-options]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify the container-options interface type.

Options **aps**—Configure the interface type to be Automatic Protection Switching (APS).

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

Related Documentation

- Configuring Container Interfaces on page 48

encapsulation

See the following sections:

- encapsulation (Container Interface) on page 87
- encapsulation (Logical Interface) on page 88

encapsulation (Container Interface)

Syntax encapsulation (cisco-hdlc | ppp);

Hierarchy Level [edit interfaces c*in*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Container link-layer encapsulation type.

Options **cisco-hdlc**—Use Cisco-compatible High-Level Data Link Control (HDLC) framing.

ppp—Use serial PPP encapsulation.

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

Related Documentation

- Configuring Container Interfaces on page 48

encapsulation (Logical Interface)

Syntax encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-snap | atm-tcc-snap | atm-tcc-vc-mux | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc | ether-vpls-over-fr | ether-vpls-over-ppp | ethernet | frame-relay-ccc | frame-relay-ether-type | frame-relay-ether-type-tcc | frame-relay-ppp | frame-relay-tcc | multilink-frame-relay-end-to-end | multilink-ppp | ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc | vlan-vci-ccc | vlan-tcc | vlan-vpls);

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]
[edit interfaces rlsq*number* unit *logical-unit-number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Logical link-layer encapsulation type.

Options

atm-ccc-cell-relay—Use ATM cell-relay encapsulation.

atm-ccc-vc-mux—Use ATM virtual circuit (VC) multiplex encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

atm-cisco-nlpid—Use Cisco ATM network layer protocol ID (NLPID) encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

atm-mlppp-llc—For ATM2 IQ interfaces only, use Multilink PPP (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a Link Services or Voice Services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.

atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

atm-ppp-llc—For ATM2 IQ interfaces only, use PPP over AAL5 LLC encapsulation.

atm-ppp-vc-mux—For ATM2 IQ interfaces only, use PPP over ATM AAL5 multiplex encapsulation.

atm-snap—Use ATM subnetwork attachment point (SNAP) encapsulation.

atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.

atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

atm-vc-mux—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

ether-over-atm-llc—For interfaces that carry IPv4 traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.

ether-vpls-over-atm-llc—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

ether-vpls-over-fr—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Frame Relay encapsulation to support Bridged Ethernet over Frame Relay encapsulated TDM interfaces for VPLS applications, as per *RFC 2427 (1490)*.

NOTE: **The SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, and the DS3/E3 MIC do not support Ethernet over Frame Relay encapsulation.**

ether-vpls-over-ppp—For E1, T1, E3, T3 and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over point-to-point-protocol (PPP) encapsulation to support Bridged Ethernet over PPP encapsulated TDM interfaces for VPLS applications.

ethernet—Use Ethernet II encapsulation (as described in RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*).

ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.

NOTE: **The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.**

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

frame-relay-ppp—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the **ppp** family only. J Series Routers do not support frame-relay-ppp encapsulation.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the **tcc** family only.

frame-relay-ether-type—Use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. The physical interface must be configured with flexible-frame-relay encapsulation.

frame-relay-ether-type-tcc—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect unlike media. The physical interface must be configured with flexible-frame-relay encapsulation.

multilink-frame-relay-end-to-end—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services, voice services interfaces and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

multilink-ppp—Use MLPPP encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

ppp-over-ether—For underlying Ethernet interfaces on J Series Services Routers, use PPP over Ethernet encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface. You also use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface on M120 and M320 Series routers with Intelligent Queuing 2 (IQ2) PICs, and on MX Series routers with Trio MPC/MIC interfaces.

ppp-over-ether-over-atm-llc—For underlying ATM interfaces on J Series Services Routers only, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface.

vlan-bridge—Use Ethernet VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q tagging, flexible-ethernet-services, and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

vlan-ccc—Use Ethernet virtual LAN (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-vci-ccc—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-tcc—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

vlan-vpls—Use Ethernet VLAN encapsulation on VPLS circuits.

Required Privilege Level

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

Related Documentation

- Configuring Interface Encapsulation on Logical Interfaces
- Circuit and Translational Cross-Connects Overview
- Identifying the Access Concentrator
- Configuring ATM Interface Encapsulation
- Configuring VLAN Encapsulation
- Configuring Extended VLAN Encapsulation
- Configuring ISDN Logical Interface Properties
- Configuring ATM-to-Ethernet Interworking
- *Junos OS Services Interfaces Configuration Guide*

family

Syntax

```
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | input output);
        }
    }
    access-concentrator name;
    address address {
        ... the address subhierarchy appears after the main [edit interfaces interface-name unit
            logical-unit-number family family-name] hierarchy ...
    }
    bridge-domain-type (bvlan | svlan);
    bundle interface-name;
    core-facing;
    demux-destination {
        destination-prefix;
    }
    demux-source {
        source-prefix;
    }
    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 ];
    }
    interface-mode (access | trunk);
    ipsec-sa sa-name;
    isid-list all-service-groups;
    keep-address-and-control;
    mac-validate (loose | strict);
    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;
    protocols [inet iso mpls];
    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 {
  input;
  output;
}
service {
  input {
    post-service-filter filter-name;
    service-set service-set-name <service-filter filter-name>;
  }
  output {
    service-set service-set-name <service-filter filter-name>;
  }
}
service-name-table table-name
short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
  maximum-seconds>;
(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;
vlan-id number;
vlan-id-list [number number-number];
address address {
  arp ip-address (mac | multicast-mac) mac-address <publish>;
  broadcast address;
  destination address;
  destination-profile name;
  eui-64;
  master-only;
  multipoint-destination address dlci dlci-identifier;
  multipoint-destination address {
    epd-threshold cells;
    inverse-arp;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
        sustained rate);
      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;
            track {
              interface interface-name {
                bandwidth-threshold bits-per-second priority-cost number;
              }
              priority-hold-time seconds;
              route ip-address/prefix-length routing-instance instance-name priority-cost cost;
            }
            virtual-address [ addresses ];
            virtual-link-local-address ipv6–address;
            vrrp-inherit-from {
              active-interface interface-name;
              active-group group-number;
            }
          }
        }
      }
```

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced before Junos OS Release 7.4.
Option **max-sessions-vsa-ignore** introduced in Junos OS Release 11.4.

Description Configure protocol family information for the logical interface.

NOTE: Not all subordinate stanzas are available to every protocol family. See the *Junos OS Configuration Statements and Commands* for details about each protocol family.

Options *family*—Protocol family:

- **any**—Protocol-independent family used for Layer 2 packet filtering
- **bridge**—(M Series and T Series routers only) Configure only when the physical interface is configured with **ethernet-bridge** type encapsulation or when the logical interface is configured with **vlan-bridge** type encapsulation
- **ccc**—Circuit cross-connect protocol suite
- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite
- **iso**—International Organization for Standardization Open Systems Interconnection (ISO OSI) protocol suite
- **mlfr-end-to-end**—Multilink Frame Relay FRF.15
- **mlfr-uni-nni**—Multilink Frame Relay FRF.16
- **multilink-ppp**—Multilink Point-to-Point Protocol
- **mpls**—Multiprotocol Label Switching (MPLS)
- **pppoe**—Point-to-Point Protocol over Ethernet
- **tcc**—Translational cross-connect protocol suite
- **tnp**—Trivial Network Protocol
- **vpls**—(M Series and T Series routers only) Virtual private LAN service

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

- Configuring the Protocol Family
- Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers
- *Junos OS Services Interfaces Configuration Guide*

fcs

Syntax fcs (16 | 32);

Hierarchy Level [edit interfaces e1-*fpc/pic/port*],
[edit interfaces t1-*fpc/pic/port*],
[edit interfaces *interface-name* ds0-options],
[edit interfaces *interface-name* e1-options],
[edit interfaces *interface-name* e3-options],
[edit interfaces *interface-name* sonet-options],
[edit interfaces *interface-name* t1-options],
[edit interfaces *interface-name* t3-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description For E1/E3, SONET/SDH, and T1/T3 interfaces, configure the frame checksum (FCS) on the interface. The checksum must be the same on both ends of the interface.

On a channelized OC12 interface, the SONET/SDH **fcs** statement is not supported. To configure FCS on each DS3 channel, you must include the **t3-options fcs** statement in the configuration for each channel. For SONET/SDH, the channelized OC12 interface supports DS3 to STS-1 to OC12. For SDH, the channelized OC12 interface supports *N*xDS3 to *N*xVC3 to AU3 to STM.

NOTE: When configuring E1 or T1 interfaces on 10-port Channelized E1/T1 IQE PICs, the **fcs** statement must be included at the **[edit interfaces e1-*fpc/pic/port*]** or **[edit interfaces t1-*fpc/pic/port*]** hierarchy level as appropriate.

Options **16**—Use a 16-bit frame checksum on the interface.

32—Use a 32-bit frame checksum on the interface. Using a 32-bit checksum provides more reliable packet verification, but some older equipment might not support 32-bit checksums.

Default: 16

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

Related Documentation

- Configuring the E1 Frame Checksum
- Configuring the E3 Frame Checksum
- Configuring the SONET/SDH Frame Checksum on page 37
- Configuring the T1 Frame Checksum
- Configuring the T3 Frame Checksum

filter

Syntax

```
filter {
  group filter-group-number;
  input filter-name;
  input-list [ filter-names ];
  output filter-name;
  output-list [ filter-names ];
}
```

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number* family *family*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Apply a filter to an interface. You can also use filters for encrypted traffic. When you configure filters, you can configure them under the **family ethernet-switching**, **inet**, **inet6**, **mpls**, or **vpls** only.

Options

group *filter-group-number*—Define an interface to be part of a filter group. The default filter group number is 0.

Range: 0 through 255

input *filter-name*—Name of one filter to evaluate when packets are received on the interface.

output *filter-name*—Name of one filter to evaluate when packets are transmitted on the interface.

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

- Applying a Filter to an Interface
- Configuring Firewall Filters (CLI Procedure)
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)
- Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches
- *Junos OS Services Interfaces Configuration Guide*
- *Junos OS Routing Policy Configuration Guide*
- *Junos OS System Basics Configuration Guide*

force

Syntax force (protect | working);

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Perform a forced switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch. It can be overridden by a signal failure on the protect circuit, thus causing a switch to the working circuit.

Options **protect**—Request the circuit to become the protect circuit.

working—Request the circuit to become the working circuit.

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

Related Documentation
- Configuring Switching Between the Working and Protect Circuits on page 53
- request on page 119

framing (SONET and SDH Interfaces)

Syntax framing (sdh | sonet);

Hierarchy Level [edit interfaces so-*fpc/pic/port*]

Release Information Statement introduced in Junos OS Release 8.1.

Description For the 4-port OC48 PIC with SFP installed and the 4-port OC192 PIC in T Series and M Series routers, configure SONET or SDH framing on a per-port basis. This functionality allows you to mix SONET and SDH modes on interfaces on the same PIC.

Options **sdh**—SDH framing.

sonet—SONET framing.

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

Related Documentation
- Configuring SONET/SDH Framing on page 30

hold-time

See the following sections:

NOTE: For information about the hold-time statement at the [edit interfaces *interface-name* unit *logical-unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-number* preempt] and [edit logical-systems *logical-system-name* interface *interface-name* unit *logical-unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-number* preempt], see the *Junos OS High Availability Configuration Guide*.

hold-time (APS)

Syntax hold-time *milliseconds*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Hold-time value to use to determine whether a neighbor APS router is operational.

Options *milliseconds*—Hold-time value.
Range: 1 through 65,534 milliseconds
Default: 3000 milliseconds (3 times the advertisement interval)

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

Related Documentation
- Configuring APS Timers on page 56
- advertise-interval on page 77

hold-time (SONET/SDH Defect Triggers)

Syntax hold-time up *milliseconds* down *milliseconds*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description For ATM over SONET/SDH and SONET/SDH interfaces only, apply up and down hold times to SONET/SDH defect triggers. When you apply a down hold time to a defect, the defect must remain present for at least the hold-time period before the interface is marked down. When you apply an up hold time to a defect, the defect must remain absent for at least the hold-time period before the interface is marked up, assuming no other defect is outstanding.

NOTE: On M Series and T Series platforms with Channelized SONET IQ PICs and Channelized SONET IQE PICs, the SONET defect alarm trigger hold-time statement is not supported.

Default If you do not include this statement, when a defect is detected the interface is marked down immediately, and when the defect becomes absent the interface is marked up immediately.

Options **down *milliseconds***—Hold time to wait before the interface is marked down.

Range: 1 through 65,534 milliseconds

Default: No hold time

up *milliseconds*—Hold time to wait before the interface is marked up.

Range: 1 through 65,534 milliseconds

Default: No hold time

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

Related Documentation

- Configuring SONET/SDH Defect Hold Times on page 43

ignore

Syntax ignore;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description For ATM over SONET/SDH and SONET/SDH interfaces only, ignore a specific SONET/SDH defect trigger.

Default If you do not include this statement, all defects are honored with no hold time.

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

Related Documentation

- Configuring SONET/SDH Defect Triggers to Be Ignored on page 41
- hold-time (Physical Interface)

link-speed (Aggregated SONET/SDH)

Syntax link-speed (*speed* | mixed);

Hierarchy Level [edit interfaces as*x* aggregated-sonet-options]

Release Information Statement introduced before Junos OS Release 7.4.
mixed option added in Release 8.0.

Description For aggregated SONET/SDH interfaces only, set the required link speed.

Options ***speed***—Aggregated SONET/SDH links can have one of the following speed values.

- **oc3**—Links are OC3c or STM1c.
- **oc12**—Links are OC12c or STM4c.
- **oc48**—Links are OC48c or STM16c.
- **oc192**—Links are OC192c or STM64c.
- **oc768**—Links are OC768c or STM256c.

mixed—For aggregated SONET/SDH links on T Series routers, you can mix interface speeds in SONET/SDH aggregation bundles. Interface speeds from OC3 through OC768 are supported.

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

Related Documentation

- Configuring Aggregated Ethernet Link Speed
- Configuring Aggregated SONET/SDH Link Speed on page 70

lockout

Syntax lockout;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a lockout of protection, forcing the use of the working circuit and locking out the protect circuit regardless of anything else.

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

Related Documentation

- Configuring Switching Between the Working and Protect Circuits on page 53

loop-timing

Syntax (loop-timing | no-loop-timing);

Hierarchy Level [edit interfaces ct3-*fpc/pic/port* t3-options],
[edit interfaces e1-*fpc/pic/port*:0 sonet-options],
[edit interfaces stm1-*fpc/pic/port* sonet-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description For channelized IQ interfaces and non-IQ channelized STM1 interfaces only, configure the SONET/SDH or DS3-level clocking source.

NOTE: On M Series, MX Series, and T Series routers, under E1 channels, loop timing can be configured only at channel 0. When you configure on channel 0, it is applicable on all channels as internal by default.

Options **loop-timing**—Configure loop timing (external) clocking.

no-loop-timing—Configure line timing (internal) clocking.

Default: no-loop-timing

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

Related Documentation

- Configuring Channelized IQ and IQE SONET/SDH Loop Timing on page 38
- Configuring the Channelized T3 Loop Timing
- clocking on page 84

loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3)

Syntax loopback (local | payload | remote);

Hierarchy Level
[edit interfaces ce1-*fpc/pic/port*],
[edit interfaces ct1-*fpc/pic/port*],
[edit interfaces t1-*fpc/pic/port*],
[edit interfaces *interface-name* ds0-options],
[edit interfaces *interface-name* dsl-options],
[edit interfaces *interface-name* e1-options],
[edit interfaces *interface-name* e3-options],
[edit interfaces *interface-name* shdsl-options},
[edit interfaces *interface-name* sonet-options],
[edit interfaces *interface-name* t1-options],
[edit interfaces *interface-name* t3-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a loopback connection. To turn off the loopback capability, remove the **loopback** statement from the configuration.

NOTE: When configuring CE1 or CT1 interfaces on 10-port Channelized E1/T1 IQE PICs, the **loopback** statement must be included with the **local** or **remote** option at the **[edit interfaces ce1-*fpc/pic/port*]** or **[edit interfaces ct1-*fpc/pic/port*]** hierarchy level as appropriate.

When configuring T1 interfaces on 10-port Channelized E1/T1 IQE PICs, the **loopback** statement must be included with the **payload** option at the **[edit interfaces t1-*fpc/pic/port*]** hierarchy level.

To configure loopback on channelized IQ and IQE PICs, SONET/SDH level, use the **sonet-options loopback** statement **local** and **remote** options at the controller interface (coc48, cstm16, coc12, cstm4, coc3, cstm1). It is ignored for path-level interfaces **so-*fpc/pic/port*** or **so-*fpc/pic/port*:*channel***.

Options
local—Loop packets, including both data and timing information, back on the local router's PIC. *N*xDS0 IQ interfaces do not support local loopback.

payload—For channelized T3, T1, and *N*xDS0 IQ interfaces only, loop back data only (without clocking information) on the remote router's PIC. With payload loopback, overhead is recalculated. Neither ATM-over-asymmetrical digital subscriber line (ADSL) interfaces nor ATM-over-SHDSL interfaces support payload loopback.

remote—Loop packets, including both data and timing information, back on the remote router's interface card. *N*xDS0 IQ interfaces do not support remote loopback.

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

Related Documentation

- Configuring E3 and T3 Parameters on ATM Interfaces
- Configuring E1 Loopback Capability
- Configuring E3 Loopback Capability
- Configuring Channelized IQ and IQE SONET/SDH Loop Timing on page 38
- Configuring SHDSL Operating Mode on an ATM Physical Interface
- Configuring T1 Loopback Capability
- Configuring T3 Loopback Capability
- feac-loop-respond

member-interface-speed

Syntax member-interface-speed *speed*;

Hierarchy Level [edit interfaces container-options member-interface-type]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify container-interface member-interface speed options.

Options ***speed***—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.

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

Related Documentation

- Configuring Container Interfaces on page 48
- container-options on page 86

member-interface-type

Syntax

```
member-interface-type sonet {
  member-interface-speed [ speed ];
}
```

Hierarchy Level [edit interfaces container-options]

Release Information Statement introduced in Junos OS Release 9.2.

Description Specify container-interface member-interface type as sonet and speed options.

Options **sonet**—Protocol type of the container interface, specify sonet.

speed—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.

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

Related Documentation

- Configuring Container Interfaces on page 48
- container-options on page 86

minimum-links

Syntax minimum-links *number*;

Hierarchy Level
[edit interfaces ae*x* aggregated-ether-options],
[edit interfaces ae*x* aggregated-sonet-options],
[edit interfaces *interface-name* mlfr-uni-nni-bundle-options],
[edit interfaces *interface-name* unit *logical-unit-number*],
[edit interfaces interface-range *range* aggregated-ether-options],
[edit interfaces interface-range *range* aggregated-sonet-options],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description For aggregated Ethernet, SONET/SDH, multilink, link services, and voice services interfaces only, set the minimum number of links that must be up for the bundle to be labeled up.

Options *number*—Number of links.

Range: 1 through 8 (1 through 16 for Ethernet and SONET interfaces on the MX Series, M320, M120, T Series, or TX Matrix routers, and 1 through 12 for EX8200 switches)

Default: 1

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

Related Documentation

- Configuring Aggregated Ethernet Minimum Links
- Configuring Aggregated SONET/SDH Minimum Links on page 70
- Configuring Aggregated Ethernet Interfaces (CLI Procedure)
- Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch
- *Junos OS Services Interfaces Configuration Guide*

mpls

Syntax

```
mpls {
  pop-all-labels {
    required-depth number;
  }
}
```

Hierarchy Level

[edit interfaces *interface-name* atm-options],
[edit interfaces *interface-name* sonet-options],
[edit interfaces *interface-name* fastether-options],
[edit interfaces *interface-name* gigether-options]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For passive monitoring on ATM and SONET/SDH interfaces and 10-Gigabit Ethernet interfaces in WAN PHY mode, process incoming IP packets that have MPLS labels.

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

- Removing MPLS Labels from Incoming Packets
- Removing MPLS Labels from Incoming Packets on page 61
- *Junos OS Services Interfaces Configuration Guide*

mtu

Syntax mtu *bytes*;

Hierarchy Level [edit interfaces *interface-name*],
[edit interfaces *interface-name* unit *logical-unit-number* family *family*],
[edit interfaces interface-range *name*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Specify the maximum transmission unit (MTU) size for the media or protocol. The default MTU size depends on the device type. Changing the media MTU or protocol MTU causes an interface to be deleted and added again.

To route jumbo data packets on the RVI on EX Series switches, you must configure the jumbo MTU size on the member physical interfaces and also on the RVI itself (the VLAN interface).

CAUTION: For EX Series switches, setting or deleting the jumbo MTU size on the RVI (the vlan interface) while the switch is transmitting packets might result in dropped packets.

NOTE: Not all devices allow you to set an MTU value, and some devices have restrictions on the range of allowable MTU values. You cannot configure an MTU for management Ethernet interfaces (fxp0, em0, or me0) or for loopback, multilink, and multicast tunnel devices.

For more information on configuring MTU for specific interfaces and router or switch combinations, see Configuring the Media MTU.

Options ***bytes***—MTU size.

Range: 256 through 9192 bytes

Default: 1500 bytes (INET, INET6, and ISO families), 1448 bytes (MPLS), 1514 bytes (EX Series interfaces)

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

Related Documentation

- Configuring the Media MTU
- Configuring Gigabit Ethernet Interfaces (CLI Procedure)

- Configuring Routed VLAN Interfaces (CLI Procedure)
- Setting the Protocol MTU

neighbor

Syntax neighbor *address*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description If you are configuring one router to be the working router and a second to be the protect router, configure the address of the remote interface. You configure this on one or both of the interfaces.

The address you specify for the neighbor must never be routed through the interface on which APS is configured, or instability will result. We strongly recommend that you directly connect the working and protect routers and that you configure the interface address of this shared network as the neighbor address.

Options ***address***—Neighbor's address.

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

Related Documentation
- Configuring Basic APS Support on page 47

overflow

See the following sections:

- overflow (Receive Bucket) on page 111
- overflow (Transmit Bucket) on page 111

overflow (Receive Bucket)

Syntax overflow (discard | tag);

Hierarchy Level [edit interfaces *interface-name* receive-bucket]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify how to handle packets that exceed the threshold for the receive leaky bucket.

Options **tag**—Tag, count, and process received packets that exceed the threshold.

discard—Discard received packets that exceed the threshold. No counting is done.

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

Related Documentation
- Configuring Receive and Transmit Leaky Bucket Properties
- Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 63

overflow (Transmit Bucket)

Syntax overflow discard;

Hierarchy Level [edit interfaces *interface-name* transmit-bucket]

Release Information Statement introduced before Junos OS Release 7.4.

Description Discard packets that exceed the threshold for the transmit leaky bucket.

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

Related Documentation
- Configuring Receive and Transmit Leaky Bucket Properties
- Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 63

paired-group

Syntax paired-group *group-name*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure load sharing between two working protect circuit pairs.

Options *group-name*—Circuit's group name, as configured with the **protect-circuit** or **working-circuit** statement.

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

Related Documentation
- Configuring APS Load Sharing Between Circuit Pairs on page 58
- working-circuit on page 130

passive-monitor-mode

Syntax passive-monitor-mode;

Hierarchy Level [edit interfaces *interface-name*],
[edit interfaces *interface-name* unit *logical-unit-number*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description For ATM, Ethernet, and SONET/SDH interfaces only, monitor packet flows from another router. If you include this statement in the configuration, the interface does not send keepalives or alarms, and does not participate actively on the network.

For ATM and Ethernet interfaces, you can include this statement on the physical interface only.

For SONET/SDH interfaces, you can include this statement on the logical interface only.

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

Related Documentation
- Enabling Passive Monitoring on ATM Interfaces
- Passive Monitoring on Ethernet Interfaces Overview
- Enabling Passive Monitoring on SONET/SDH Interfaces on page 60
- multiservice-options
- *Junos OS Services Interfaces Configuration Guide*

path-trace

Syntax path-trace *trace-string*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description For SONET/SDH interfaces and 10-Gigabit Ethernet interfaces in WAN PHY mode, configure a path trace identifier, which is a text string that identifies the circuit.

On SONET/SDH OC48 interfaces that are configured for channelized (multiplexed) mode (by including the **no-concatenate** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level), the **bytes e1-quiet** and **bytes f1** options have no effect. The **bytes f2**, **bytes z3**, **bytes z4**, and **path-trace** options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.

For DS3 channels on a channelized OC12 interface, you can configure a unique path trace for each of the 12 channels. Each path trace can be up to 16 bytes. For channels on a channelized OC12 IQ interface, each path trace can be up to 64 bytes.

Options ***trace-string***—Text string that identifies the circuit. If the string contains spaces, enclose it in quotation marks. A common convention is to use the circuit identifier as the path trace identifier. If you do not configure an identifier, the Junos OS uses the system and interface names to construct the default ***trace-string***. For all nonchannelized SONET/SDH interfaces, the default ***trace-string*** is ***system-name interface-name***. For channelized SONET/SDH interfaces and 10–Gigabit Ethernet WAN-PHY interfaces, the default ***trace-string*** is ***interface-name***.

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

Related Documentation

- Configuring the SONET/SDH Path Trace Identifier on page 40
- sonet-options on page 122

payload-scrambler

Syntax (payload-scrambler | no-payload-scrambler);

Hierarchy Level [edit interfaces *interface-name* e3-options],
[edit interfaces *interface-name* sonet-options],
[edit interfaces *interface-name* t3-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Enable or disable HDLC scrambling on an E3, a SONET/SDH, or a T3 interface. This type of scrambling provides better link stability. Both sides of a connection must either use or not use scrambling.

If you commit a T3 interface configuration that has HDLC payload scrambling enabled, the interface must also be configured to be compatible with the channel service unit (CSU) at the remote end of the line.

Disable payload scrambling on an E3 interface if Digital Link compatibility mode is used.

On a channelized OC12 interface, the **sonet payload-scrambler** statement is ignored. To configure scrambling on the DS3 channels on the interface, you can include the **t3-options payload-scrambler** statement in the configuration for each DS3 channel.

NOTE: The **payload-scrambler** statement at the **[edit interfaces *interface-name* e3-options]** hierarchy level is not valid for IQE PICs.

Default Payload scrambling is disabled on all E3 and T3 interfaces; it is enabled by default on E3/T3 over ATM interfaces and on SONET/SDH interfaces.

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

Related Documentation

- Configuring E3 and T3 Parameters on ATM Interfaces
- Configuring E3 HDLC Payload Scrambling
- Configuring SONET/SDH HDLC Payload Scrambling on page 40
- Configuring T3 HDLC Payload Scrambling
- Examples: Configuring T3 Interfaces
- compatibility-mode

pop-all-labels

Syntax

```
pop-all-labels {
  required-depth number;
}
```

Hierarchy Level

[edit interfaces *interface-name* atm-options mpls],
[edit interfaces *interface-name* sonet-options mpls],
[edit interfaces *interface-name* fastether-options mpls],
[edit interfaces *interface-name* gigether-options mpls]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For passive monitoring on ATM and SONET/SDH interfaces only, removes up to two MPLS labels from incoming IP packets.

This statement has no effect on IP packets with more than two MPLS labels. Packets with MPLS labels cannot be processed by the Monitoring Services PIC; if packets with MPLS labels are forwarded to the Monitoring Services PIC, they are discarded.

The remaining statement is explained separately.

Default

If you omit this statement, the MPLS labels are not removed, and the packet is not processed by the Monitoring Services PIC.

Required Privilege Level

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

Related Documentation

- Removing MPLS Labels from Incoming Packets
- Removing MPLS Labels from Incoming Packets on page 61
- *Junos OS Services Interfaces Configuration Guide*

preserve-interface

Syntax preserve-interface;

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

Release Information Statement introduced in Junos OS Release 7.6.

Description Provide link PIC replication, providing MLPPP link redundancy at the port level. This feature is supported with SONET APS and the following link PICs:

- Channelized OC3 IQ PIC
- Channelized OC12 IQ PIC
- Channelized STM1 IQ PIC

Link PIC replication provides the ability to add two sets of links, one from the active SONET PIC and the other from the standby SONET PIC, to the same bundle. If the active SONET PIC fails, links from the standby PIC are used without triggering link renegotiation. All the negotiated state is replicated from the active links to the standby links to prevent link renegotiation.

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

Related Documentation

- Configuring Link PIC Redundancy on page 57
- *Junos OS Services Interfaces Configuration Guide*

protect-circuit

Syntax protect-circuit *group-name*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the protect router in an APS circuit pair. When the working interface fails, APS brings up the protection circuit and the traffic is moved to the protection circuit.

Options ***group-name***—Circuit's group name.

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

Related Documentation

- Configuring Basic APS Support on page 47
- **working-circuit on page 130**

rate

Syntax rate *percentage*;

Hierarchy Level [edit interfaces *interface-name* receive-bucket],
[edit interfaces *interface-name* transmit-bucket]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify percentage of the interface line rate that is available to receive or transmit packets.

Options ***percentage***—Percentage of the interface line rate that is available to receive or transmit packets.

Range: 0 through 100

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

Related Documentation

- Configuring Receive and Transmit Leaky Bucket Properties
- Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 63

receive-bucket

Syntax

```
receive-bucket {
  overflow (discard | tag);
  rate percentage;
  threshold bytes;
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set parameters for the receive leaky bucket, which specifies what percentage of the interface's total capacity can be used to receive packets.

For each DS3 channel on a channelized OC12 interface, you can configure a unique receive bucket.

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

- Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 63
- transmit-bucket on page 128

receive-options-packets

Syntax receive-options-packets;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet]

Release Information Statement introduced before Junos OS Release 7.4.

Description For a Monitoring Services PIC and an ATM or SONET/SDH PIC installed in an M160, M40e, or T Series router, guarantee conformity with cflowd records structure. This statement is required when you enable passive monitoring.

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

Related Documentation
- Enabling Passive Monitoring on ATM Interfaces
- Enabling Passive Monitoring on SONET/SDH Interfaces on page 60

receive-ttl-exceeded

Syntax receive-ttl-exceeded;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family inet],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet]

Release Information Statement introduced before Junos OS Release 7.4.

Description For Monitoring Services PIC and an ATM or SONET/SDH PIC installed in an M160, M40e, or T Series router, guarantee conformity with cflowd records structure. This statement is required when you enable passive monitoring.

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

Related Documentation
- Enabling Passive Monitoring on ATM Interfaces
- Enabling Passive Monitoring on SONET/SDH Interfaces on page 60

request

Syntax request (protect | working);

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Perform a manual switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch.

Options **protect**—Request that the circuit become the protect circuit.

working—Request that the circuit become the working circuit.

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

Related Documentation

- Configuring Switching Between the Working and Protect Circuits on page 53
- force on page 98

required-depth

Syntax required-depth *number*;

Hierarchy Level [edit interfaces *interface-name* atm-options mpls pop-all-labels],
[edit interfaces *interface-name* sonet-options mpls pop-all-labels],
[edit interfaces *interface-name* fastether-options mpls pop-all-labels],
[edit interfaces *interface-name* gigether-options mpls pop-all-labels]

Release Information Statement introduced before Junos OS Release 7.4.

Description For passive monitoring on ATM and SONET/SDH interfaces only, specify the number of MPLS labels an incoming packet must have for the **pop-all-labels** statement to take effect.

If you include the **required-depth 1** statement, the **pop-all-labels** statement takes effect for incoming packets with one label only. If you include the **required-depth 2** statement, the **pop-all-labels** statement takes effect for incoming packets with two labels only.

Options *number*—Number of MPLS labels on incoming IP packets.

Range: 1 or 2 labels

Default: If you omit this statement, the **pop-all-labels** statement takes effect for incoming packets with one or two labels. The default is equivalent to including the **required-depth [1 2]** statement.

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

Related Documentation

- Removing MPLS Labels from Incoming Packets
- Removing MPLS Labels from Incoming Packets on page 61
- *Junos OS Services Interfaces Configuration Guide*

revert-time

Syntax revert-time *seconds*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure APS revertive mode.

Default APS operates in nonrevertive mode.

Options ***seconds***—Amount of time to wait after the working circuit has again become functional before making the working circuit active again.

Range: 1 through 65,535 seconds

Default: None (APS operates in nonrevertive mode)

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

Related Documentation
- Configuring Revertive Mode on page 55

rfc-2615

Syntax rfc-2615;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Include this statement to enable features described in RFC 2615, *PPP over SONET/SDH*.

Default Settings required by RFC 1619, *PPP over SONET/SDH*.

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

Related Documentation
- Configuring SONET/SDH RFC 2615 Support on page 41

sonet-options

Syntax

```
sonet-options {
  aps {
    advertise-interval milliseconds;
    annex-b
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    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;
    defect hold-time up milliseconds down milliseconds;
  }
}
vtmapping (itu-t | klm);
(z0-increment | no-z0-increment);
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure SONET/SDH-specific interface properties.

On SONET/SDH OC48 interfaces that you configure for channelized (multiplexed) mode (by including the **no-concatenate** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level), the **bytes e1-quiet** and **bytes f1** options have no effect. The

bytes f2, **bytes z3**, **bytes z4**, and **path-trace** options work correctly on channel 0 and work in the transmit direction only on channels 1, 2, and 3.

On a channelized OC12 interface, the **bytes e1-quiet, bytes f1, bytes f2, bytes z3,** and **bytes z4** options are not supported. The **fcs** and **payload-scrambler** statements are also not supported; you must configure these for each DS3 channel using the **t3-options fcs** and **t3-options payload-scrambler** statements. The **aps** and **loopback** statements are supported only on channel 0 and are ignored if included in the configurations for channels 1 through 11. You can configure loopbacks for each DS3 channel with the **t3-options loopback** statement. The **path-trace** statement can be included in the configuration for each DS3 channel, thereby configuring a unique path trace for each channel.

To configure loopback on channelized IQ and IQE PICs, SONET/SDH level, use the **loopback** statement **local** and **remote** options at the controller interface (coc48, cstm16, coc12, cstm4, coc3, and cstm1). It is ignored for path-level interfaces **so-*fpc/pic/port*** or **so-*fpc/pic/port*:*channel***.

If you are running Intermediate System-to-Intermediate System (IS-IS) over SONET/SDH interfaces, use PPP if you are running Cisco IOS Release 12.0 or later. If you need to run HDLC, configure an ISO family MTU of 4469 on the router.

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

- Configuring SONET/SDH Parameters on ATM Interfaces
- Channelized OC12/STM4 IQ and IQE Interfaces Overview
- Channelized STM1 Interfaces Overview
- Configuring SONET/SDH Physical Interface Properties on page 28
- no-concatenate

speed (SONET/SDH)

Syntax speed (oc3 | oc12 | oc48);

Hierarchy Level [edit interfaces so-*fpc/pic/port*],
[edit interfaces so-*fpc/pic/port*:*channel*]

Release Information Statement introduced in Junos OS Release 8.3.

Description Configure the interface speed. This statement applies to SONET/SDH interfaces on next-generation SONET/SDH Type 1 and Type 2 PICs with SFP. Available speeds depend on whether the PIC is in concatenated mode or nonconcatenated mode. Include the channel in the interface name when configuring nonconcatenated interfaces.

Options **oc3 | oc12 | oc48**—Speed when the PIC is in concatenated mode. For example, you can configure each port of a 4-port OC12 PIC to have a speed of **oc3**.

You can configure port 0 of a 4-port OC12 PIC to have a speed of **oc12**.

oc3 | oc12—Speed when the PIC is in nonconcatenated mode.

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

Related Documentation

- Configuring SONET/SDH Interface Speed on page 31

switching-mode

Syntax switching-mode (bidirectional | unidirectional);

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

Release Information Statement introduced before Junos OS Release 7.4.

Description For unchannelized OC3, OC12, and OC48 SONET/SDH interfaces on T Series routers only, configure the interface to interoperate with SONET/SDH line-terminating equipment (LTE) that is provisioned for unidirectional linear APS in 1+1 architecture.

Default If the **switching-mode** statement is not configured, the mode is bidirectional, and the interface does not interoperate with a unidirectional SONET/SDH LTE.

Options **bidirectional**—Support bidirectional mode only.

unidirectional—Interoperate with a SONET/SDH LTE provisioned for unidirectional mode.

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

Related Documentation

- Configuring Unidirectional Switching Mode Support on page 55

t3-options

Syntax

```
t3-options {
  atm-encapsulation (direct | plcp);
  bert-algorithm algorithm;
  bert-error-rate rate;
  bert-period seconds;
  (cbit-parity | no-cbit-parity);
  compatibility-mode (digital-link | kentrox | larscom) <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);
  start-end-flag value;
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure T3-specific physical interface properties, including the properties of DS3 channels on a channelized OC12 interface. The **long-buildout** statement is not supported for DS3 channels on a channelized OC12 interface.

On T3 interfaces, the default encapsulation is PPP.

For ATM1 interfaces, you can configure a subset of E3 options statements.

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

- T3 Interfaces Overview

threshold

Syntax threshold *bytes*;

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the bucket threshold, which controls the burstiness of the leaky bucket mechanism. The larger the value, the more bursty the traffic, which means that over a very short amount of time, the interface can receive or transmit close to line rate, but the average over a longer time is at the configured bucket rate.

Options ***bytes***—Maximum size, in bytes, for traffic bursts. For ease of entry, you can enter ***number*** either as a complete decimal number or as a decimal number followed by the abbreviation **k** (1000). For example, the entry **threshold 2k** corresponds to a threshold of 2000 bytes.

Range: 0 through 65,535 bytes

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

Related Documentation

- Configuring Receive and Transmit Leaky Bucket Properties
- Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 63

transmit-bucket

Syntax

```
transmit-bucket {
  overflow discard;
  rate percentage;
  threshold bytes;
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Set parameters for the transmit leaky bucket, which specifies what percentage of the interface's total capacity can be used to transmit packets.

For each DS3 channel in a channelized OC12 interface, you can configure a unique transmit bucket.

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

- Configuring Receive and Transmit Leaky Bucket Properties
- Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 63
- receive-bucket on page 117

trigger

Syntax

```
trigger {
  defect ignore;
  defect hold-time up milliseconds down milliseconds;
}
```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description For ATM over SONET/SDH, SONET/SDH interfaces, and 10-Gigabit Ethernet interfaces in WAN PHY mode, configure SONET/SDH defect triggers to be ignored.

Default If you do not include this statement, all SONET/SDH defect triggers are honored.

Options ***defect***—Defect to ignore or hold. It can be one of the following:

- **ais-l**—Line alarm indication signal
- **ais-p**—Path alarm indication signal
- **ber-sd**—Bit error rate signal degrade
- **ber-sf**—Bit error rate signal fault
- **locd** (ATM only)—Loss of cell delineation
- **lof**—Loss of frame
- **lol**—PHY loss of light
- **lop-p**—Path loss of pointer
- **los**—Loss of signal
- **pll**—PHY phase-locked loop out of lock
- **plm-p**—Path payload label mismatch
- **rfi-l**—Line remote failure indication
- **rfi-p**—Path remote failure indication
- **uneq-p**—Path unequipped

  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

- Configuring SONET/SDH Defect Triggers to Be Ignored on page 41

vtmapping

Syntax vtmapping (itu-t | klm);

Hierarchy Level [edit interfaces *interface-name* sonet-options];
[edit chassis fpc *number* pic *number*]

Release Information Statement introduced before Junos OS Release 7.4.

Description For the Channelized STM1 IQ PIC or Channelized STM1 PIC, configure virtual tributary mapping.

For the Channelized STM1 PIC, you configure virtual tributary mapping at the **[edit chassis fpc *number* pic *number*]** hierarchy level.

Options **itu-t**—International Telephony Union standard.

klm—KLM standard.
Default: klm

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

Related Documentation
- Configuring Virtual Tributary Mapping of Channelized STM1 Interfaces
- *Junos OS System Basics Configuration Guide*

working-circuit

Syntax working-circuit *group-name*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the working router in an APS circuit pair.

Options ***group-name***—Circuit's group name.

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

Related Documentation
- Configuring Basic APS Support on page 47
- protect-circuit on page 116

z0-increment

Syntax (z0-increment | no-z0-increment);

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an incremental STM ID rather than a static one.

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

Related Documentation

- Configuring an Incrementing STM ID on page 37
- sonet-options on page 122

PART 4

Troubleshooting

CHAPTER 4

Investigate SONET Interfaces

Investigate Interface Steps and Commands

This section includes the following information to assist you when troubleshooting ATM interfaces:

Investigate Interface Steps and Commands Overview

The "Monitor Interfaces" on page 135 section helps you determine the nature of the interface problem. The "Perform a Loopback Test on an Interface" on page 136 section provides information to help you isolate the source of the problem. The "Locate Interface Alarms" on page 138 section explains some of the alarms and errors for the media.

Monitor Interfaces

Problem The following steps are a general outline of how you monitor interfaces to determine the nature of interface problems. For more detailed information on a specific interface, see the corresponding monitor interfaces section.

Solution To monitor interfaces, follow these steps:

1. Display the status of an interface.
2. Display the status of a specific interface.

3. Display extensive status information for a specific interface.
4. Monitor statistics for an interface.

The "*Commands Used to Monitor Interfaces*" table lists and describes the operational mode commands you use to monitor interfaces.

Table 13: Commands Used to Monitor Interfaces

CLI Command	Description
show interfaces terse ***interface-name*** For example: **show interfaces terse t1***	Displays summary information about the named interfaces.
show interfaces ***interface-name*** For example: **show interfaces t1-***x/x/x*	Displays static status information about a specific interface.
show interfaces ***interface-name*****extensive** For example: **show interfaces t1-***x/x/x* **extensive**	Displays very detailed interface information about a specific interface.
monitor interface ***interface-name*** For example: **monitor interface t1-***x/x/x*	Displays real-time statistics about a physical interface, updated every second.

Perform a Loopback Test on an Interface

Problem The following steps are a general outline of how you use loopback testing to isolate the source of the interface problem. For more detailed information on a specific interface, see the corresponding loopback section.

Solution To use loopback testing for interfaces, follow these steps:

1. Diagnose a suspected hardware problem.
   a. Create a loopback.
   b. Set clocking to internal. (Not for Fast Ethernet/Gigabit Ethernet or Multichannel DS3 interfaces.)
   c. Verify that the status of the interface is up.
   d. Configure a static address resolution protocol table entry. (Fast Ethernet/Gigabit Ethernet interfaces only)
   e. Clear the interface statistics.
   f. Force the link layer to stay up.
   g. Verify the status of the logical interface.

h. Ping the interface.

i. Check for interface error statistics.

2. Diagnose a suspected connection problem.

   a. Create a loop from the router to the network.

   b. Create a loop to the router from various points in the network.

The "*Commands Used to Perform Loopback Testing on Interfaces*" table lists and describes the operational and configuration mode commands you use to perform loopback testing on interfaces (the commands are shown in the order in which you perform them).

Table 14: Commands Used to Perform Loopback Testing on Interfaces

CLI Statement or Command	Interface Type	Description
[edit interfaces *interface-name interface-* options] set loopback (local | remote)	All interfaces	The **loopback** statement at the hierarchy level configures a loopback on the interface. Packets can be looped on either the local router or the remote channel service unit (CSU). To turn off loopback, remove the **loopback** statement from the configuration.
show	All interfaces	Verify the configuration before you commit it.
commit	All interfaces	Save the set of changes to the database and cause the changes to take operational effect. Use after you have verified a configuration in all configuration steps.
[edit interfaces *interface-name*] set clocking internal	T1, T3, ATM, and SONET interfaces	The **clocking** statement at this hierarchy level configures the clock source of the interface to internal.
show interfaces *interface-name*	Used for all interfaces	Display static status information about a specific interface.
[edit interfaces *interface-name* unit *logical-unit-number* family inet *address* address] arp *ip-address* mac *mac-address*	Fast Ethernet and Gigabit Ethernet interfaces	The **arp** statement at this hierarchy level defines mappings between IP and Media Access Control (MAC) addresses.
show arp no-resolve	Fast Ethernet and Gigabit Ethernet interfaces	Display the entries in the ARP table without attempting to determine the hostname that corresponds to the IP address (the **no-resolve** option).
clear interfaces statistics *interface-name*	All interfaces	Reset the statistics for an interface to zero.
[edit interfaces *interface-name*] set encapsulation cisco-hdlc	T1, T3, SONET, and Multichannel DS3 interfaces	The **encapsulation** statement at this hierarchy level sets the encapsulation to the Cisco High-level Data-Link Control (HDLC) transport protocol on the physical interface.

Table 14: Commands Used to Perform Loopback Testing on Interfaces *(continued)*

CLI Statement or Command	Interface Type	Description
[edit interfaces *interface-name*] **set no-keepalives**	T1, T3, SONET, and Multichannel DS3 interfaces	The **no-keepalives** statement at this level disables the sending of keepalives on the physical interface.
show interfaces *interface-name* terse	T1, T3, and SONET interfaces	Display summary information about interfaces. (Use to display the status of the logical interfaces for these interfaces.)
ping interface t1- *x/x/x local-IP-address* bypass-routing count 1000 rapid	All interfaces	Check the reachability of network hosts by sending **ICMP ECHO_REQUEST** messages to elicit **ICMP ECHO_RESPONSE** messages from the specified host. Use the **bypass-routing** option to ping a local system through an interface that has no route through it. The **count** option sends 1000 ping requests through the system. Type **Ctrl+C** to interrupt a **ping** command.
show interfaces *interface-name* extensive	All interfaces	Display very detailed interface information about a specific interface.

Locate Interface Alarms

Problem Locating alarms and errors for the media can be a simple process.

Solution To locate interface alarms and errors, use the **show interfaces *interface-name* extensive** command and examine the output for active alarms and defects.

Monitor SONET Interfaces

This section includes the following information to assist you when troubleshooting SONET interfaces:

Checklist for Monitoring SONET Interfaces

Purpose To monitor SONET interfaces and begin the process of isolating SONET interface problems when they occur.

Action Table 15 on page 139 provides the links and commands for monitoring SONET interfaces.

Table 15: Checklist for Monitoring SONET Interfaces

Tasks	Command or Action
"Monitor SONET Interfaces" on page 139	
1. Display the Status of SONET Interfaces on page 139	**show interfaces terse so***
2. Display the Status of a Specific SONET Interface on page 140	**show interfaces so-*fpc/pic/port***
3. Display Extensive Status Information for a Specific SONET Interface on page 141	**show interfaces so-*fpc/pic/port* extensive**
4. Monitor Statistics for a SONET Interface on page 143	**monitor interface so-*fpc/pic/port***

Monitor SONET Interfaces

By monitoring SONET interfaces, you begin the process of isolating SONET interface problems when they occur.

To monitor your SONET interface, follow these steps:

1. Display the Status of SONET Interfaces on page 139
2. Display the Status of a Specific SONET Interface on page 140
3. Display Extensive Status Information for a Specific SONET Interface on page 141
4. Monitor Statistics for a SONET Interface on page 143

Display the Status of SONET Interfaces

Purpose To display the status of SONET interfaces, use the following Junos OS command-line interface (CLI) operational mode command:

Action

```
user@host> show interfaces terse so*
```

Meaning The sample output lists only the SONET interfaces. It shows the status of both the physical and logical interfaces.

For a description of what the output means, see Table 16 on page 139.

Table 16: Status of SONET Interfaces

Physical Interface	Logical Interface	Status Description
so-1/0/0 Admin Up Link Up	so-1/0/0.0 Admin Up Link Up	This interface has both the physical and logical links up and running.

Table 16: Status of SONET Interfaces *(continued)*

Physical Interface	Logical Interface	Status Description
so-1/1/1 Admin Down Link Up	so-1/1/1.0 Admin Up Link Down	This interface is administratively disabled. The physical link is healthy (**Link Up**), but the logical link is not established end to end (**Link Down**).
so-3/0/1 Admin Up Link Up	so-3/0/1.0 Admin Up Link Down	This interface is administratively enabled and the physical link is healthy (**Link Up**), but the logical interface is not established end to end (**Link Down**).
so-5/3/0 Admin Up Link Down	so-5/3/0.0 Admin Up Link Down	This interface has the physical link down and the logical interface is down also.

Display the Status of a Specific SONET Interface

Purpose To display the status of a specific SONET interface when you need to investigate its status further, use the following Junos OS CLI operational mode command:

Action user@host> **show interfaces so-*fpc/pic/port***

Sample Output The following sample output is for an interface with the physical link down:

```
user@router> show interfaces so-1/1/1
Physical interface: so-1/1/1, Enabled, Physical link is Down
  Interface index: 17, SNMP ifIndex: 16
  Description: router-02 pos 4/0
  Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET mode
  Speed: OC3, Loopback: None, CRC: 32, Payload scrambler: Enabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down Link-Layer-Down Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Keepalive Input: 621 (00:02:57 ago), Output: 889 (00:00:09 ago)
  Input rate     : 0 bps (0 pps), Output rate: 0 bps (0 pps)
  Active alarms  : LOL, LOS
  Active defects : LOL, LOF, LOS, SEF, AIS-L, AIS-P, PLM-P
  Logical interface so-1/1/1.0 (Index 18) (SNMP ifIndex 30)
    Description: router-02 pos 4/0
    Flags: Device-down Point-To-Point SNMP-Traps, Encapsulation: Cisco-HDLC
    Protocol inet, MTU: 4470
      Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
        Destination: 10.10.10.48/30, Local: 10.10.10.50
    Protocol iso, MTU: 4469
```

Meaning The first line of the sample output shows that the physical link is down. This means that the physical link is unhealthy and cannot pass packets. Further down the sample output, look for active alarms and defects. When you see this situation, to further diagnose the

problem, see "Display Extensive Status Information for a Specific SONET Interface" on page 141 to display more extensive information about the SONET interface and the physical interface that is down.

Sample Output The following output is for an interface with the physical layer up and the link layer down:

```
user@router> show interfaces so-3/0/1
Physical interface: so-3/0/1, Enabled, Physical link is Up
  Interface index: 28, SNMP ifIndex: 55
  Description:  Customer ABC
  Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET mode, Speed:
 OC3,
  Loopback: None, FCS: 16, Payload scrambler: Enabled
  Device flags   : Present Running
  Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 113 (00:00:02 ago), Output: 119 (00:00:02 ago)
  Input rate     : 80 bps (0 pps)
  Output rate    : 88 bps (0 pps)
  SONET alarms   : None
  SONET defects  : None
  Logical interface so-3/0/1.0 (Index 22) (SNMP ifIndex 56)
    Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: Cisco-HDLC
    Protocol inet, MTU: 4470, Flags: None
      Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
        Destination: 192.168.2.124/30, Local: 192.168.2.125
```

Meaning The sample output shows that the link layer is down. This means that the logical interface is not established end to end. When you see this situation, to further diagnose the problem, see "Monitor Statistics for a SONET Interface" on page 143 to monitor statistics for the SONET interface and the logical interface that is down.

Display Extensive Status Information for a Specific SONET Interface

Purpose To display extensive status information about a specific interface, use the following Junos OS CLI operational mode command:

Action user@host> **show interfaces so-*fpc/pic/port* extensive**

Sample Output

```
user@router> show interfaces so-1/1/1 extensive
Physical interface: so-1/1/1, Enabled, Physical link is Down
  Interface index: 17, SNMP ifIndex: 16
  Description: router-02 pos 4/0
  Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET mode
  Speed: OC3, Loopback: None, CRC: 32, Payload scrambler: Enabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down Link-Layer-Down Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Keepalive statistics:
    Input : 621 (last seen 00:05:35 ago)
    Output: 905 (last seen 00:00:07 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :            378736540                 0 bps
   Output bytes  :              6786356                 0 bps
   Input  packets:               225924                 0 pps
```

```
    Output packets:              104798                    0 pps
    Input errors:
     Errors: 8, Drops: 0, Framing errors: 4181286, Runts: 0, Giants: 8
     Policed discards: 9474, L3 incompletes: 0, L2 channel errors: 0
     L2 mismatch timeouts: 3, HS link CRC errors: 0, HS link FIFO overflows: 0
    Output errors:
     Carrier transitions: 2, Errors: 0, Drops: 0, Aged packets: 0
     HS link FIFO underflows: 0
    Active alarms   : LOL, LOS  <--  SONET active alarms and defects
    Active defects : LOL, LOF, LOS, SEF, AIS-L, AIS-P, PLM-P
   SONET PHY:            Seconds        Count  State  <-- SONET media-specific
errors
     PLL Lock                 0            0  OK
     PHY Light              328            1  Light Missing
   SONET section: <--  SONET section errors
     BIP-B1                   0            0
     SEF                    329            3  Defect Active
     LOS                    329            2  Defect Active
     LOF                    329            2  Defect Active
     ES-S                   329
     SES-S                  329
     SEFS-S                 329
    SONET line:
     BIP-B2                   0            0
     REI-L                    0            0
     RDI-L                    0            0  OK
     AIS-L                  328            1  Defect Active
     BERR-SF                  0            0  OK
     BERR-SD                  0            0  OK
     ES-L                   329
     SES-L                  329
     UAS-L                  318
     ES-LFE                   0
     SES-LFE                  0
     UAS-LFE                  0
    SONET path:
     BIP-B3                   0            0
     REI-P                    0            0
     LOP-P                    1            1  OK
     AIS-P                  328            1  Defect Active
     RDI-P                    0            0  OK
     UNEQ-P                   0            0  OK
     PLM-P                  328            1  Defect Active
     ES-P                   329
     SES-P                  329
     UAS-P                  318
     ES-PFE                   0
     SES-PFE                  0
     UAS-PFE                  0
[...Output truncated...]
```

Meaning The sample output details where the errors might be occurring. Error details include input and output errors, active alarms and defects, and media-specific errors. The SONET section, line, and path errors help narrow down the source of the problem.

If the physical link is down, look at the active alarms and defects for the SONET interface and troubleshoot the SONET media accordingly. See"List of Common SONET Alarms and Errors" on page 158 for an explanation of SONET alarms.

Monitor Statistics for a SONET Interface

Purpose To monitor statistics for a SONET interface, use the following Junos OS CLI operational mode command:

Action user@host> **monitor interface so-*fpc/pic/port***

CAUTION: We recommend that you use this command only for diagnostic purposes. Do not leave it on during normal router operations because real-time monitoring of traffic consumes additional CPU and memory resources.

Sample Output

```
user@router> monitor interface so-1/1/1
router                      Seconds: 168                Time: 15:48:50
Interface: so-1/1/1, Enabled, Link is Down
Encapsulation: Cisco-HDLC, Keepalives, Speed: OC3
Traffic statistics:                                        Current Delta
  Input bytes:                375527568 (0 bps)                    [0]
  Output bytes:                 6612857 (0 bps)                  [475]
  Input packets:                 224001 (0 pps)                    [0]
  Output packets:                102090 (0 pps)                   [20]
Encapsulation statistics:
  Input keepalives:                   0                           [0]
  Output keepalives:                176                          [17]
Error statistics:
  Input errors:                       0                           [0]
  Input drops:                        0                           [0]
  Input framing errors:             179                          [17]
  Policed discards:                  47                           [0]
  L3 incompletes:                     0                           [0]
  L2 channel errors:                  0                           [0]
  L2 mismatch timeouts:               0                           [0]
  Carrier transitions:                1                           [0]
  Output errors:                      0                           [0]
  Output drops:                       0                           [0]
  F2      : 0x00  Z3        : 0x00  Z4        : 0x00
Interface warnings:
  o Received keepalive count is zero
  o Framing errors are increasing, check FCS configuration and link
Next='n', Quit='q' or ESC, Freeze='f', Thaw='t', Clear='c', Interface='i'
```

Meaning This output checks for and displays common interface failures, whether or not loopback is detected, and any increases in framing errors. Information from this command can help you narrow down possible causes of an interface problem.

NOTE: If you are accessing the router from the console connection, make sure you set the CLI terminal type using the **set cli terminal** command.

The statistics in the second column are the cumulative statistics since the last time they were cleared using the **clear interfaces statistics *interface-name*** command. The statistics

in the third column are the statistics since the **monitor interface *interface-name*** command was executed.

If the framing errors are increasing, verify that the frame check sequence (FCS) and scrambling configuration match on both ends of the connection. If the configuration is correct, check the cabling to the router and have the carrier verify the integrity of the line.

If the input errors are increasing, check the cabling to the router and have the carrier verify the integrity of the line.

If you are sending output keepalives but are not receiving any input keepalives, verify that the encapsulation and keepalive configurations match on both ends of the connection.

Table 17 on page 144 lists and describes the SONET error statistics in the output for the **monitor interface** command. The output fields are listed in the order in which they appear in the output.

Table 17: SONET Error Statistics

Output Field	Output Field Description
Input errors	Sum of the incoming frame aborts and FCS errors.
Input drops	Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's random early detection (RED) mechanism.
Input framing errors	The number of packets that have FCS errors.
Policed discards	Frames that the incoming packet match code discarded because they were not recognized or of interest. Usually, this field reports protocols that the Junos OS does not handle.
L3 incompletes	Increments when the incoming packet fails Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header would be discarded and this counter would increment.
L2 channel errors	Increments when the software cannot find a valid logical interface for an incoming frame.
L2 mismatch timeouts	Count of malformed or short packets that cause the incoming packet handler to discard the frame as unreadable.
Carrier transitions	Number of times the interface has gone from down to up. This number should not increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or a similar problem occurs. If it increments quickly (perhaps once every 10 seconds), then the cable, the far-end system, or the PIC is broken.
Output errors	Sum of the outgoing frame aborts and FCS errors. Because output errors are rare, hardware problems, configuration, or software bugs might contribute to the cause of them. Use the output of the **show interfaces *type-fpc/pic/port* extensive** command for more details about which output errors are incrementing. Also, analyze the system or interface load to determine if those areas are contributing to the cause of the problem. If the problem persists, open a case with the Juniper Networks Technical Assistance Center (JTAC) at **support@juniper.net** or at 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

Table 17: SONET Error Statistics *(continued)*

Output Field	Output Field Description
Output drops	Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism.

Verify the Status of the Logical Interface

Purpose To verify the status of the logical interface, use the following two Junos OS CLI operational mode commands:

Action

```
user@host> show interfaces so-fpc/pic/port
user@host> show interfaces so-fpc/pic/port terse
```

Sample Output 1 The following sample output displays the information for a logical interface that is up:

```
user@host> show interfaces so-2/2/0
Physical interface: so-2/2/0, Enabled, Physical link is Up
Interface index: 21, SNMP ifIndex: 45
Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET mode, Speed:
OC3, Loopback: None
FCS: 16, Payload scrambler: Enabled
Device flags   : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link flags     : No-Keepalives
Input rate     : 0 bps (0 pps)
Output rate    : 0 bps (0 pps)
SONET alarms   : None
SONET defects  : None
Logical interface so-2/2/0.0 (Index 7) (SNMP ifIndex 33)
Flags: Point-To-Point SNMP-Traps Encapsulation: Cisco-HDLC
Protocol inet, MTU: 4470, Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 10.0.2/24, Local: 10.0.2.1

user@host> show interfaces so-2/2/0 terse
Interface       Admin Link Proto Local                 Remote
so-2/2/0        up    up
so-2/2/0.0      up    up   inet  10.0.2.1/24
```

Meaning The **show interfaces** command in sample output 1shows that the logical link is up because there are no flags indicating that the link layer is down. The output for the **show interfaces terse** command shows that logical interface **so-2/2/0.0** is up.

Sample Output 2 The following sample output displays the information for a logical interface that is down:

```
user@host> show interfaces so-2/2/0
Physical interface: so-2/2/0, Enabled, Physical link is Up
Interface index: 21, SNMP ifIndex: 45
Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET mode, Speed:
OC3, Loopback: None,
FCS: 16, Payload scrambler: Enabled
Device flags   : Present Running Loop-Detected
Interface flags: Link-Layer-Down  Point-To-Point SNMP-Traps
```

```
Link flags     : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 14 (00:00:05 ago), Output: 14 (00:00:05 ago)
Input rate     : 0 bps (0 pps)
Output rate    : 0 bps (0 pps)
SONET alarms   : None
SONET defects  : None
Logical interface so-2/2/0.0 (Index 7) (SNMP ifIndex 33)
Flags: Device-Down  Point-To-Point SNMP-Traps Encapsulation: Cisco-HDLC
Protocol inet, MTU: 4470, Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.0.2/24, Local: 10.0.2.1

user@host> show interfaces so-2/2/0 terse
Interface       Admin Link Proto Local                 Remote
so-2/2/0        up    down
so-2/2/0.0      up    down  inet  10.0.2.1/24
```

Meaning Both commands in sample output 2 show that the logical interface is down. The first command shows that the link layer, device, and destination route are all down. The second command shows that logical interface **so-2/2/0.0** is down.

Related Documentation

- Investigate Interface Steps and Commands Overview on page 135
- Monitor Interfaces on page 135
- Perform a Loopback Test on an Interface on page 136

Use Loopback Testing for SONET Interfaces

This section includes the following information to assist you when troubleshooting SONET interfaces:

- Checklist for Using Loopback Testing for SONET Interfaces on page 146
- Diagnose a Suspected Hardware Problem with a SONET Interface on page 148
- Create a Loopback on page 148
- Set Clocking to Internal on page 150
- Verify That the SONET Interface Is Up on page 150
- Clear SONET Interface Statistics on page 152
- Check That the Received and Transmitted Path Trace Are the Same on page 152
- Force the Link Layer to Stay Up on page 153
- Ping the SONET Interface on page 154
- Check for SONET Interface Error Statistics on page 155
- Diagnose a Suspected Circuit Problem on page 156

Checklist for Using Loopback Testing for SONET Interfaces

Purpose To use loopback testing to isolate SONET interface problems.

Action Table 18 on page 147 provides the links and commands for using loopback testing for SONET interfaces.

Table 18: Checklist for Using Loopback Testing for SONET Interfaces

Tasks	Command or Action
"Diagnose a Suspected Hardware Problem with a SONET Interface" on page 148	
1. Create a Loopback on page 148	
a. Create a Physical Loopback on page 148	Connect the transmit port to the receive port.
b. Configure a Local Loopback on page 149	[edit interfaces *interface-name* sonet-options] set loopback local show commit
2. Set Clocking to Internal on page 150	[edit interfaces *interface-name*] set clocking internal show commit
3. Verify That the SONET Interface Is Up on page 150	show interfaces so-*fpc/pic/port*
4. Clear SONET Interface Statistics on page 152	clear interfaces statistics so-*fpc/pic/port*
5. Check That the Received and Transmitted Path Trace Are the Same on page 152	show interfaces so-*fpc/pic/port* extensive
6. Force the Link Layer to Stay Up on page 153	
a. Configure Encapsulation to Cisco-HDLC on page 153	[edit interfaces *interface-name*] set encapsulation cisco-hdlc show commit
b. Configure No-Keepalives on page 154	[edit interfaces *interface-name*] set no-keepalives show commit
7. Verify the Status of the Logical Interface on page 145	show interfaces so-*fpc/pic/port* show interfaces so-*fpc/pic/port* terse
8. Ping the SONET Interface on page 154	ping interface so-*fpc/pic/port local-IP-address* bypass-routing count 1000 rapid
9. Check for SONET Interface Error Statistics on page 155	show interfaces so-*fpc/pic/port* extensive
"Diagnose a Suspected Circuit Problem" on page 156	
1. Create a Loop from the Router to the Network on page 156	[edit interfaces *interface-name* sonet-options] set loopback remote show commit

Table 18: Checklist for Using Loopback Testing for SONET Interfaces *(continued)*

Tasks	Command or Action
2. Create a Loop to the Router from Various Points in the Network on page 157	Perform Steps 2 through 8 from "Diagnose a Suspected Hardware Problem with a SONET Interface" on page 148.

Diagnose a Suspected Hardware Problem with a SONET Interface

Problem When you suspect a hardware problem, take the following steps to verify if there is a problem.

Solution To diagnose a suspected hardware problem with the SONET interface, follow these steps:

- Create a Loopback on page 148
- Set Clocking to Internal on page 150
- Verify That the SONET Interface Is Up on page 150
- Clear SONET Interface Statistics on page 152
- Check That the Received and Transmitted Path Trace Are the Same on page 152
- Force the Link Layer to Stay Up on page 153
- Verify the Status of the Logical Interface on page 145
- Ping the SONET Interface on page 154
- Check for SONET Interface Error Statistics on page 155

Create a Loopback

You can create a physical loopback or configure a local loopback to help diagnose a suspected hardware problem. Creating a physical loopback is recommended because it allows you to test and verify the transmit and receive ports. If a field engineer is not available to create the physical loopback, you can configure a local loopback for the interface. The local loopback creates a loopback internally in the Physical Interface Card (PIC).

1. Create a Physical Loopback on page 148
2. Configure a Local Loopback on page 149

Create a Physical Loopback

Action To create a physical loopback at the port, connect the transmit port to the receive port using a known good fiber cable.

NOTE: Make sure you use a single-mode fiber for a single-mode port and multimode fiber for a multimode port. (For OC192, you must use the appropriate attentuation.)

Meaning When you create and test a physical loopback, you are testing the transmit and receive ports of the PIC. This action is recommended if a field engineer is available to create the physical loop as it provides a more complete test of the PIC.

Configure a Local Loopback

Action To configure a local loopback without physically connecting the transmit port to the receive port, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit interfaces interface-name  sonet-options
   ```

2. Configure the local loopback:

   ```
   [edit interfaces interface-name  sonet-options]
   user@host# set loopback local
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit interfaces so-1/0/0 sonet-options]
   user@host# show
   loopback local;
   ```

4. Commit the change:

   ```
   user@host# commit
   ```

   For example:

   ```
   [edit interfaces so-1/0/0 sonet-options]
   user@host# commit
   commit complete
   ```

Meaning When you create a local loopback, you create an internal loop on the interface being tested. A local loopback loops the traffic internally on that PIC. A local loopback tests the interconnection of the PIC but does not test the transmit and receive ports.

NOTE: Remember to delete the loopback statement after completing the test.

Set Clocking to Internal

Purpose Clocking is set to internal because there is no external clock source in a loopback connection.

Action To configure clocking to internal, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit interfaces interface-name
   ```

2. Configure clocking to internal:

   ```
   [edit interfaces interface-name]
   user@host# set clocking internal
   user@host# commit
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit interfaces so-1/0/0]
   user@host# show
   clocking internal;
   ```

4. Commit the change:

   ```
   user@host# commit
   ```

   For example:

   ```
   [edit interfaces so-1/0/0]
   user@host# commit
   commit complete
   ```

Meaning The clock source for the interface is set to the internal Stratum 3 clock.

Verify That the SONET Interface Is Up

Purpose Displaying the status of the SONET interface provides the information you need to determine whether the physical link is up or down.

Action To verify that the SONET interface is up, use the following Junos OS command-line interface (CLI) operational mode command:

```
user@host> show interfaces so-fpc/pic/port
```

Sample Output 1 The following output is for a SONET interface with the physical link up:

```
user@host# show interfaces so-2/2/0
Physical interface: so-2/2/0, Enabled, Physical link is Up
Interface index: 21, SNMP ifIndex: 45
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
Loopback: None, FCS: 16,
Payload scrambler: Enabled
```

```
Device flags   : Present Running Loop-Detected
Interface flags: Point-To-Point SNMP-Traps
Link flags     : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 0 (never), Output: 0 (never)
LCP state: Conf-req-sent
NCP state: inet: Down, inet6: Not-configured, iso: Not-configured, mpls:
Not-configured
Input rate     : 48 bps (0 pps)
Output rate    : 56 bps (0 pps)
SONET alarms   :  None
SONET defects  :  None
Logical interface so-2/2/0.0 (Index 7) (SNMP ifIndex 33)
Flags: Hardware-Down Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 4470, Flags: Protocol-Down
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.0.2/24, Local: 10.0.2.1
```

Meaning Sample output 1 shows that the physical link is up, the loop is detected, and there are no SONET alarms or defects.

If the physical link is up, continue with "Check That the Received and Transmitted Path Trace Are the Same" on page 152.

Sample Output 2 When you see that the physical link is down, there might be a problem with the port. Sample output 2 shows that the physical link is down:

```
user@host# show interfaces so-2/2/0
Physical interface: so-2/2/0, Enabled, Physical link is Down
Interface index: 21, SNMP ifIndex: 45
Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
Loopback: None, FCS: 16,
Payload scrambler: Enabled
Device flags   : Present Running Down
Interface flags: Hardware-Down Point-To-Point SNMP-Traps
Link flags     : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive: Input: 0 (never), Output: 0 (never)
LCP state: Conf-req-sent
NCP state: inet: Down, inet6: Not-configured, iso: Not-configured, mpls:
Not-configured
Input rate     : 0 bps (0 pps)
Output rate    : 0 bps (0 pps)
SONET alarms   :  LOL, LOS
SONET defects  :  LOL, LOF, LOS, SEF, AIS-L, AIS-P
Logical interface so-2/2/0.0 (Index 7) (SNMP ifIndex 33)
Flags: Hardware-Down Device-Down Point-To-Point SNMP-Traps Encapsulation: PPP
Protocol inet, MTU: 4470, Flags: Protocol-Down
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.0.2/24, Local: 10.0.2.1
```

Meaning The sample output shows that the physical link is down, the device flags and interface flags are down, and there are SONET alarms and defects.

Table 19 on page 152 lists problem situations and actions for a physical link that is down.

Table 19: Problems and Solutions for a Physical Link That Is Down

Problem	Action
Cable mismatch	Verify that the fiber connection is correct.
Damaged and/or dirty cable	Verify that the fiber can successfully loop a known good port of the same type.
Too much or too little optical attenuation	Verify that the attenuation is correct per the PIC optical specifications.
The transmit port is not transmitting within the dBm optical range per the specifications	Verify that the Tx power of the optics is within range of the PIC optical specification.

Clear SONET Interface Statistics

Purpose You must reset SONET interface statistics before you initiate the ping test. Resetting the statistics provides a clean start so that previous input/output errors and packet statistics do not interfere with the current diagnostics.

Action To clear all statistics for the interface, use the following Junos OS CLI operational mode command:

```
user@host> clear interfaces statistics so-fpc/pic/port
```

Sample Output

```
user@host> clear interfaces statistics so-4/0/2
user@host>
```

Meaning This command clears the interface statistics counters for interface **so-4/0/2** only.

Check That the Received and Transmitted Path Trace Are the Same

Purpose The received and transmitted path trace shows whether the transmitted path trace is looped back.

Action To check that the received path trace matches the transmitted path trace, use the following Junos OS CLI operational mode command:

```
user@host> show interfaces so-fpc/pic/port  extensive
```

Sample Output

```
user@host#  show interfaces so-2/2/0 extensive
Physical interface: so-2/2/0, Enabled, Physical link is Up
Interface index: 21, SNMP ifIndex: 45, Generation: 20
[...Output truncated...]
Received path trace: host so-2/2/0
70 6c 75 74 6f 6e 69 63 20 73 6f 2d 32 2f 32 2f   host so-2/2/
30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   0 ...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 0d 0a      ..............
Transmitted path trace: host so-2/2/0
70 6c 75 74 6f 6e 69 63 20 73 6f 2d 32 2f 32 2f   host so-2/2/
```

```
30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   0 ...............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
[...Output truncated...]
```

Meaning This transmitted and received path trace information is near the end of the output. The sample output shows that the transmitted and received path trace are the same. When there is a loopback, the transmitted and received path trace should be the same. If they are, continue with "Force the Link Layer to Stay Up" on page 153.

If the transmitted and received path trace are not the same, the physical loopback cable is probably on the wrong port, or is incorrectly connected. In this case, verify the connection again.

Force the Link Layer to Stay Up

To complete the loopback test, the link layer must remain up. However, Junos OS is designed to recognize that loop connections are not valid connections and to bring the link layer down. You need to force the link layer to stay up by making some configuration changes to the encapsulation and keepalives.

To force the link layer to stay up, follow these steps:

1. Configure Encapsulation to Cisco-HDLC on page 153
2. Configure No-Keepalives on page 154

Configure Encapsulation to Cisco-HDLC

Action To configure encapsulation on a SONET physical interface, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host#  edit interfaces interface-name
   ```

2. Configure Cisco-HDLC:

   ```
   [edit interfaces interface-name]
   user@host#  set encapsulation cisco-hdlc
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit interfaces so-1/0/0]
   user@host# show
   encapsulation hdlc;
   ```

4. Commit the change:

   ```
   user@host# commit
   ```

   For example:

   ```
   [edit interfaces so-1/0/0]
   user@host# commit
   ```

commit complete

Meaning This command sets the interface encapsulation to the Cisco High-level Data-Link Control (HDLC) transport protocol.

Configure No-Keepalives

Action To disable the sending of link-layer keepalives on a SONET physical interface, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   [edit]
   user@host# **edit interfaces *interface-name***

2. Configure no-keepalives:

   [edit interfaces *interface-name*]
   user@host# **set no-keepalives**

3. Verify the configuration:

   user@host# **show**

   For example:

   [edit interfaces so-1/0/0]
   user@host# **show**
   no-keepalives;

4. Commit the change:

   user@host# **commit**

   For example:

   [edit interfaces so-1/0/0]
   user@host# **commit**
   commit complete

Meaning By setting no-keepalives, the link layer is forced to stay up. If the setting remains at keepalive, the router will recognize that the same link-layer keepalives are being looped back and will bring the link layer down.

Ping the SONET Interface

Purpose To ping the local interface and verify the loopback connection, use the following Junos OS CLI operational mode command:

Action user@host> **ping interface so-*fpc/pic/port local-IP-address* bypass-routing count 1000 rapid**

Sample Output

```
user@host# ping interface so-2/2/0 10.0.2.1 bypass-routing count 1000 rapid
PING 10.0.2.1 (10.0.2.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 10.0.2.1 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.374/0.446/9.744/0.754 ms
```

Meaning This command sends 1000 ping packets out of the interface to the local IP address. The ping should complete successfully with no packet loss. If there is any persistent packet loss, open a case with the Juniper Networks Technical Assistance Center (JTAC) at **support@juniper.net** or at 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

Check for SONET Interface Error Statistics

Purpose Persistent interface error statistics indicate that you need to open a case with JTAC.

Action To check the local interface for error statistics, use the following Junos OS CLI operational mode command:

user@host> **show interfaces so-*fpc/pic/port* extensive**

Sample Output

```
user@host# show interfaces so-2/2/0 extensive
Physical interface: so-2/2/0, Enabled, Physical link is Up
[...Output truncated...]
Statistics last cleared: 2002-04-24 10:39:40 EDT (00:13:26 ago)
Traffic statistics:
Input  bytes  :              169686                   0 bps
Output bytes  :              179802                   0 bps
Input  packets:                2101                   0 pps
Output packets:                2102                   0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Bucket drops: 0,
Policed discards: 0, L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts:
 0, HS link CRC errors: 0,HS link FIFO overflows: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, HS link FIFO
underflows: 0
SONET alarms   : None
SONET defects  : None
SONET PHY:            Seconds        Count  State
PLL Lock                    0            0  OK
PHY Light                   0            0  OK
SONET section:
BIP-B1                      0            0
SEF                         0            0  OK
LOS                         0            0  OK
LOF                         0            0  OK
ES-S                        0
SES-S                       0
SEFS-S                      0
SONET line:
BIP-B2                      0            0
REI-L                       0            0
RDI-L                       0            0  OK
```

```
AIS-L                       0              0  OK
BERR-SF                     0              0  OK
BERR-SD                     0              0  OK
ES-L                        0
SES-L                       0
UAS-L                       0
ES-LFE                      0
SES-LFE                     0
UAS-LFE                     0
SONET path:
BIP-B3                      0              0
REI-P                       0              0
LOP-P                       0              0  OK
AIS-P                       0              0  OK
RDI-P                       0              0  OK
UNEQ-P                      0              0  OK
PLM-P                       0              0  OK
ES-P                        0
SES-P                       0
UAS-P                       0
ES-PFE                      0
SES-PFE                     0
UAS-PFE                     0
[...Output truncated...]
```

Meaning Check for any error statistics that may appear in the section, line, and path areas of the output. There should not be any input or output errors. If there are any persistent input or output errors, open a case with JTAC at **support@juniper.net** or at 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

Diagnose a Suspected Circuit Problem

When you suspect a circuit problem, it is important to work with the transport-layer engineer to resolve the problem. The transport-layer engineer may ask you to create a loop from the router to the network, or the engineer may create a loop to the router from various points in the network.

To diagnose a suspected circuit problem, follow these steps:

1. Create a Loop from the Router to the Network on page 156
2. Create a Loop to the Router from Various Points in the Network on page 157

Create a Loop from the Router to the Network

Purpose Creating a loop from the router to the network allows the transport-layer engineer to test the router from various points in the network. This helps the engineer isolate where the problem might be located.

Action To create a loop from the router to the network, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit interfaces interface-name sonet-options
   ```

2. Configure the remote loopback:


```
[edit interfaces interface-name sonet-options]
user@host#  set loopback remote
```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit interfaces so-1/0/0 sonet-options]
   user@host# show
   loopback remote;
   ```

4. Commit the change:

   ```
   user@host# commit
   ```

   For example:

   ```
   [edit interfaces so-1/0/0 sonet-options]
   user@host# commit
   commit complete
   ```

Meaning This command loops any traffic from the network back into the network.

Create a Loop to the Router from Various Points in the Network

Purpose The transport-layer engineer creates a loop to the router from various points in the network. You can then perform tests to verify the connection from the router to that loopback in the network.

Action After the transport-layer engineer has created the loop to the router from the network, you must verify the connection from the router to the loopback in the network. Follow Steps 2 through 8 in "Diagnose a Suspected Hardware Problem with a SONET Interface" on page 148. Keep in mind that any problems encountered in the test indicate a problem with the connection from the router to the loopback in the network.

By performing tests to loopbacks at various points in the network, you can isolate the source of the problem.

Related Documentation

- Investigate Interface Steps and Commands on page 135
- Monitor SONET Interfaces on page 138
- Locate SONET Alarms and Errors on page 158
- Enable SONET Payload Scrambling on page 176
- Check the SONET Frame Checksum on page 180

Locate SONET Alarms and Errors

This section includes the following information to assist you when troubleshooting SONET interfaces:

List of Common SONET Alarms and Errors

Purpose To check for the most common SONET alarms and errors you can encounter when investigating line problems on a Juniper Networks router.

Action Table 20 on page 158 provides links and commands for checking SONET alarms and errors.

Table 20: List of Common SONET Alarms and Errors

Tasks	Command or Action
"Display SONET Alarms and Errors" on page 159	**show interfaces so-*fpc/pic/port* extensive**
"Locate Most Common SONET Alarms and Errors" on page 162	
1. Locate Loss of Signal Alarms on page 162	Check the connection between the router port and the first SONET network element.
2. Locate Alarm Indication Signal Alarms on page 163	Downstream from the router, check the path-terminating equipment, section-terminating equipment, and line-terminating equipment for a loss of signal or loss of frame.
3. Locate Remote Defect Indication Alarms on page 165	Upstream from the router, check the path-terminating equipment, section-terminating equipment, and line-terminating equipment for a loss of signal or loss of frame.
4. Locate Remote Error Indication Line Errors on page 167	Upstream from the router, check the line-terminating equipment and path-terminating equipment for an error in the B2 or B3 byte.

Table 20: List of Common SONET Alarms and Errors *(continued)*

Tasks	Command or Action
5. Locate Bit Error Rate Alarms on page 168	Check the following: • Optical fiber • Optical transmitter and receiver • Clocking • Attenuation in the optical signal
6. Locate Payload Label Mismatch Path Alarms on page 170	Check the received and transmitted C2 byte.
7. Locate Loss of Pointer Path Alarms on page 172	Check that both sides of the connection are configured for concatenate or nonconcatenate mode.
8. Locate Unequipped Payload Alarms on page 173	Check provisioning with the SONET provider, and if possible, check the configuration of the add/drop multiplexer (ADM).
9. Locate Phase Lock Loop Alarms on page 174	Investigate the timing source, and configure the clocking to external or internal depending on the situation.

Display SONET Alarms and Errors

Action To display SONET alarms and errors, use the following Junos OS command-line interface (CLI) operational mode command:

```
user@host> show interfaces so-fpc/pic/port extensive
```

Sample Output

```
user@host> show interfaces so-1/1/1 extensive
[...Output truncated...]
  Active alarms  : None
  Active defects : None
  SONET PHY:            Seconds        Count  State
    PLL Lock                  0            0  OK
    PHY Light                 0            0  OK
  SONET section:
    BIP-B1                    0            0
    SEF                       0            0  OK
    LOS                       0            0  OK
    LOF                       0            0  OK
    ES-S                      0
    SES-S                     0
    SEFS-S                    0
  SONET line:
    BIP-B2                    0            0
    REI-L                     0            0
    RDI-L                     0            0  OK
    AIS-L                     0            0  OK
    BERR-SF                   0            0  OK
    BERR-SD                   0            0  OK
    ES-L                      0
    SES-L                     0
    UAS-L                     0
    ES-LFE                    0
```

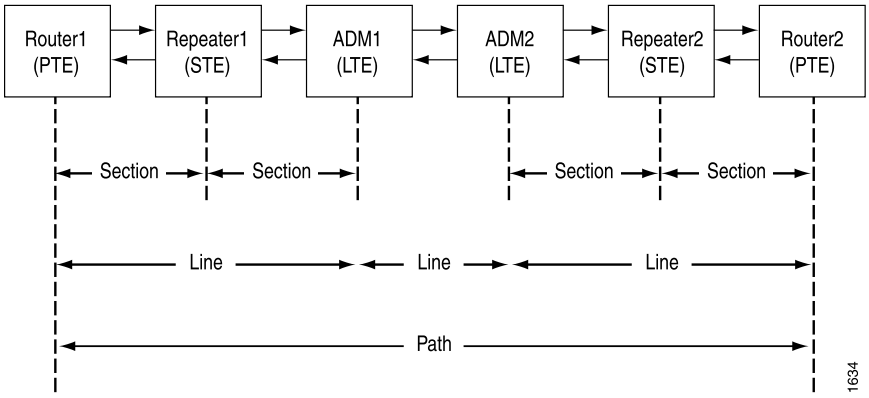
```
    SES-LFE                  0
    UAS-LFE                  0
  SONET path:
    BIP-B3                   0            0
    REI-P                    0            0
    LOP-P                    0            0  OK
    AIS-P                    0            0  OK
    RDI-P                    0            0  OK
    UNEQ-P                   0            0  OK
    PLM-P                    0            0  OK
    ES-P                     0
    SES-P                    0
    UAS-P                    0
    ES-PFE                   0
    SES-PFE                  0
    UAS-PFE                  0
[...Output truncated...]
```

Meaning The sample output shows where you find SONET alarms and errors. SONET alarms and errors fall into three different areas of the output: section, line, and path.

Section, line, and path errors occur over different spans of the SONET network and between different pieces of equipment. Figure 3 on page 160 shows an example of a SONET network with the section, line, and path areas delimited. Figure 3 on page 160 also shows the different pieces of equipment that comprise a SONET network:

- A router, usually a path-terminating equipment (PTE)
- An add/drop multiplexer (ADM), usually a line-terminating equipment (LTE)
- A repeater, usually a section-terminating equipment (STE)

Figure 3: Example of a SONET Network



SONET Section The SONET section is the connection between two STEs. The STE performs the simple regeneration of the SONET signal to the next SONET equipment span between itself, the PTE, and the ADM. For example, Repeater 1 (STE) regenerates the SONET signal between itself and ADM1, and the section between itself andRouter 1 (PTE). The STE checks to make sure that the incoming SONET frame, arriving from a directly connected neighbor, is good. An STE does not have any knowledge of the rest of the span.

An STE looks at the section overhead bytes of the SONET frame even though it can rewrite the other overhead bytes if an alarm is generated.

SONET Line

The SONET line is the span between two LTEs. The LTE pays particular attention to the line overhead bytes of the SONET frame, can add and remove payload, and has more knowledge of the SONET network than the STEs. The LTE does not do the final processing of the SONET payload as does the PTE. The ADM is an LTE.

SONET Path

The SONET path is the span between two PTEs. The PTE is the final destination where the SONET frame is terminated and the payload it carries is processed. A PTE pays particular attention to the path overhead bytes of the SONET frame.

SONET System Hierarchy

The SONET system hierarchy is comprised of PTEs, LTEs, and STEs. The characteristics of each are as follows:

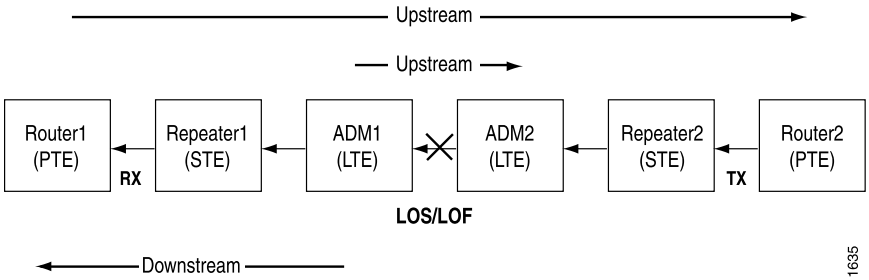
- The main role of a PTE is to read the path overhead bytes. However, it also reads the line overhead bytes and the section overhead bytes. Therefore the PTE also plays the role of an LTE and an STE.
- The main role of an LTE is to read the line overhead bytes. However, it also reads the section overhead bytes. Therefore the LTE also plays the role of an STE.
- An STE reads only the section overhead bytes of the SONET frame. (See Figure 4 on page 161.)

Upstream and Downstream

The terms *upstream* and *downstream* are used in defining SONET alarms and errors. The terms are meaningful when viewed from the point of view of the failure in the circuit.

For example, in Figure 4 on page 161 the failure occurs in the section between ADM 1 and ADM 2. The signal is transmitted from Router 2 in the direction of Router 1(from right to left). In this example, Router 1, Repeater 1, and ADM 1 are downstream from the failure. ADM 2, Repeater 2, and Router 2 are upstream from the failure.

Figure 4: Example of an Upstream or Downstream Failure

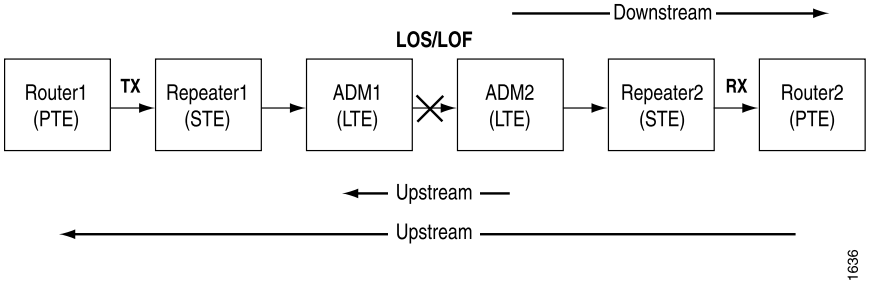


The failure sends an alarm from ADM 1 to Router 1 in the direction of the signal transmission (downstream). Alarms are also sent from ADM1 to ADM2 and from Router1 to Router2 in the opposite direction of the signal transmission (upstream).

In Figure 5 on page 162, the failure is also between ADM 1 and ADM 2. However, the signal is transmitted from Router 1 in the direction of Router 2 (from left to right). Router 2,

Repeater 2, and ADM 2 are downstream from the failure. ADM 1, Repeater 1, and Router 1 are upstream from the failure.

Figure 5: Another Example of an Upstream or Downstream Failure



This failure sends an alarm from ADM 2 to Router 2 in the direction of the signal transmission (downstream). Alarms are also sent from ADM 2 to ADM 1 and from Router 2 to Router 1 in the opposite direction of the signal transmission (upstream).

All diagnostics are from the perspective of the PTE (the Juniper Networks router). Although the exact source of the problem can be difficult to find without having access to the LTE or the STE, you can at least determine from the PTE output whether the problem is remote or local.

Locate Most Common SONET Alarms and Errors

Problem This information describes the most common SONET alarms and errors you can encounter when investigating line problems on a Juniper Networks router.

Solution The following alarms and errors are described in this section:

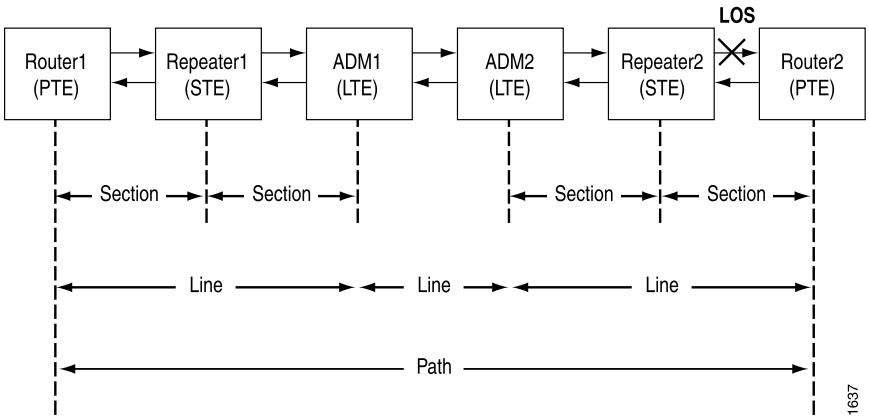
- Locate Loss of Signal Alarms on page 162
- Locate Alarm Indication Signal Alarms on page 163
- Locate Remote Defect Indication Alarms on page 165
- Locate Remote Error Indication Line Errors on page 167
- Locate Bit Error Rate Alarms on page 168
- Locate Payload Label Mismatch Path Alarms on page 170
- Locate Loss of Pointer Path Alarms on page 172
- Locate Unequipped Payload Alarms on page 173
- Locate Phase Lock Loop Alarms on page 174

Locate Loss of Signal Alarms

Problem A loss of signal (LOS) alarm indicates that there is a physical link problem with the connection to the router receive port from the neighboring SONET equipment transmit port.

Solution To locate the LOS alarm, check the connection between the router port and the first SONET network element. In the example network in Figure 6 on page 163, the X indicates that there is a connection problem between Repeater 2 and Router 2.

Figure 6: Location of an LOS Alarm in a SONET Network



To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

user@host> **show interfaces so-*fpc/pic/port* extensive**

Sample Output user@router2> **show interfaces so-1/1/1 extensive**

```
[... Output truncated...]
  Active alarms   : LOL, PLL, LOS
  Active defects  : LOL, PLL, LOF, LOS , SEF, AIS-L, AIS-P, PLM-P
  SONET PHY:             Seconds        Count  State
    PLL Lock                  51            0  PLL Lock Error
    PHY Light                 51            0  Light Missing
  SONET section:
    BIP-B1                     0            0
    SEF                       51            0  Defect Active
    LOS 51            0  Defect Active
    LOF                       51            0  Defect Active
[...Output truncated...]
```

Meaning The sample output shows at the time the command was run, Router 2 continued to be in a LOS alarm state for around 51 seconds.

Locate Alarm Indication Signal Alarms

An alarm indication signal (AIS) is sent downstream to signal an error condition. There are two types of AIS alarms:

- Alarm indication signal path (AIS-P) is sent by an LTE to a downstream PTE when an LOS or LOF is detected on a upstream SONET section.

- Alarm indication signal line (AIS-L) is sent by an STE to a downstream LTE when an LOS or LOF is detected on an incoming SONET section.

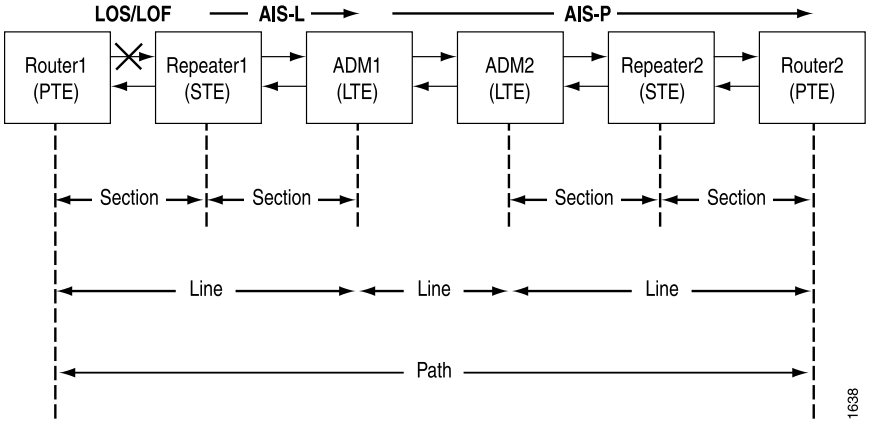
1. Example of a Router Receiving Only an AIS-P Alarm on page 164
2. Example of a Router Receiving Both an AIS-L and AIS-P Alarm on page 164

Example of a Router Receiving Only an AIS-P Alarm

Problem Figure 7 on page 164 shows a router receiving only an AIS-P alarm. The X indicates that the LOS or LOF occurs in the section between Router 1 and Repeater 1.

Solution All diagnostics are from the perspective of Router 2 (the Juniper Networks router).

Figure 7: Example of a Router Receiving Only an AIS-P Alarm



Meaning In Figure 7 on page 164, the progression of events occurring after the failure is as follows:

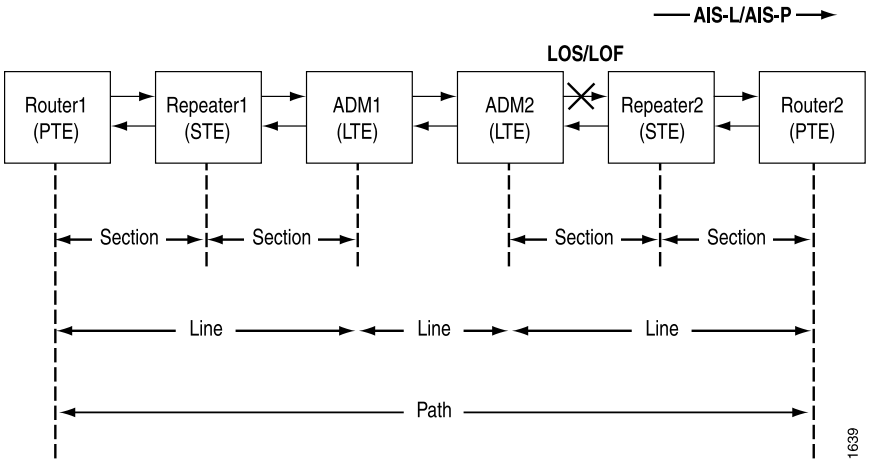
1. Repeater 1 detects an LOS or LOF on an incoming SONET section.
2. Repeater 1 sends an AIS-L downstream to ADM1 (LTE).
3. ADM 1 sends an AIS-P to Router 2 (PTE).
4. The only alarm that Router 2 receives is the AIS-P alarm from ADM 1.

Example of a Router Receiving Both an AIS-L and AIS-P Alarm

Problem Figure 8 on page 165shows a router receiving both an IS-L and AIS-P Alarm. The X indicates that the LOS or LOF occurs in the section between ADM 2 and Repeater 2.

Solution All diagnostics are from the perspective of Router 2 (the Juniper Networks router).

Figure 8: Example of a Router Receiving Both an AIS-L and an AIS-P Alarm



What It Means In Figure 8 on page 165, the progression of events occurring after the failure is as follows:

1. Repeater 2 detects an LOS or LOF on the incoming section.
2. Repeater 2 sends an AIS-L and AIS-P downstream to Router 2.
3. Router 2 receives both an AIS-L and an AIS-P from Repeater 2.

Locate Remote Defect Indication Alarms

A remote defect indication (RDI) is sent upstream to signal an error condition. There are two types of RDI alarms:

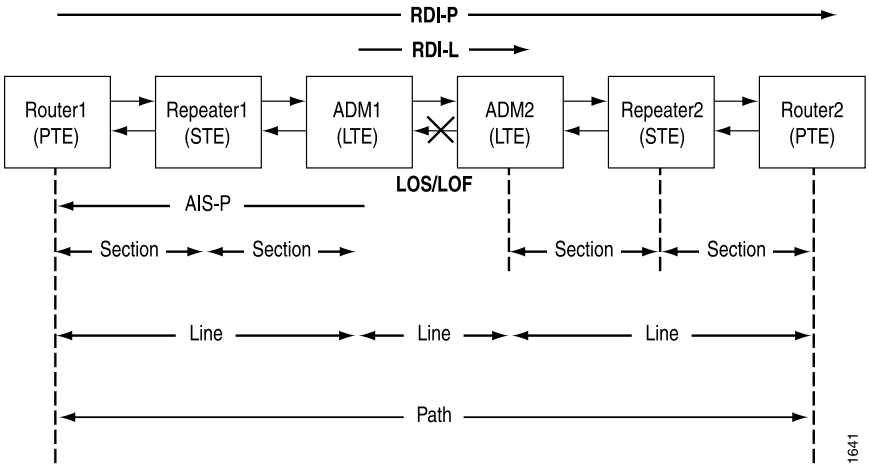
- Remote defect indication line (RDI-L) is sent upstream to a peer LTE when an alarm indication signal line (AIS-L) or low-level defects are detected.
- Remote defect indication path (RDI-P) is sent upstream to a peer PTE when a defect in the signal, typically an AIS-P, is detected.

Example of a Router Receiving Only an RDI-P Alarm

Problem Figure 9 on page 166 shows a router receiving only an RDI-P Alarm. The X indicates that the LOS or LOF occurs in the section between ADM 1 and ADM 2.

Solution All diagnostics are from the perspective of Router 2 (the Juniper Networks router).

Figure 9: Example of a Router Receiving Only an RDI-P Alarm



What It Means In Figure 9 on page 166, the progression of events occurring after the failure is as follows:

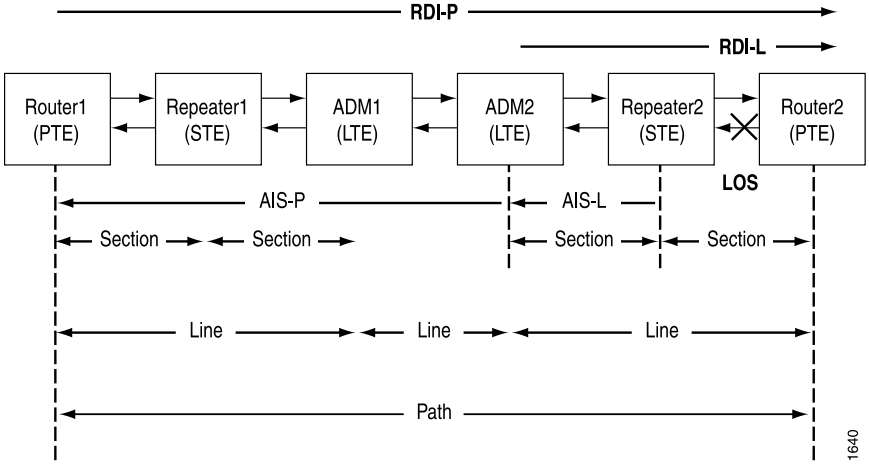
1. ADM 1 detects an LOS or LOF on an incoming SONET section.
2. ADM 1 sends an RDI-L to ADM 2.
3. ADM 1 sends an AIS-P downstream to Router 1.
4. Router 1 sends an RDI-P upstream to Router 2.
5. Router 2 only receives an RDI-P alarm.

Example of a Router Receiving Both an RDI-L and RDI-P Alarm

Problem Figure 10 on page 166 shows router receiving both an RDI-L and RDI-P Alarm. The X indicates that the LOS occurs in the section between Repeater 2 and Router 2.

Solution All diagnostics are from the perspective of Router 2 (the Juniper Networks router).

Figure 10: Example of a Router Receiving Both an RDI-L and RDI-P Alarm



Meaning In Figure 10 on page 166, the progression of events occurring after the failure is as follows:

1. Repeater 2 detects an LOS on an incoming section.
2. Repeater 2 sends an AIS-L downstream to ADM 2.
3. ADM 2 sends an RDI-L upstream to Router 2.
4. ADM 2 sends an AIS-P downstream to Router 1.
5. Router 1 sends an RDI-P upstream to Router 2.
6. Router 2 receives both RDI-P and RDI-L alarms.

Locate Remote Error Indication Line Errors

A remote error indication (REI) is sent upstream to signal an error condition. There are two types of REI alarms:

- Remote error indication line (REI-L) is sent to the upstream LTE when errors are detected in the B2 byte.
- Remote error indication path (REI-P) is sent to the upstream PTE when errors are detected in the B3 byte.

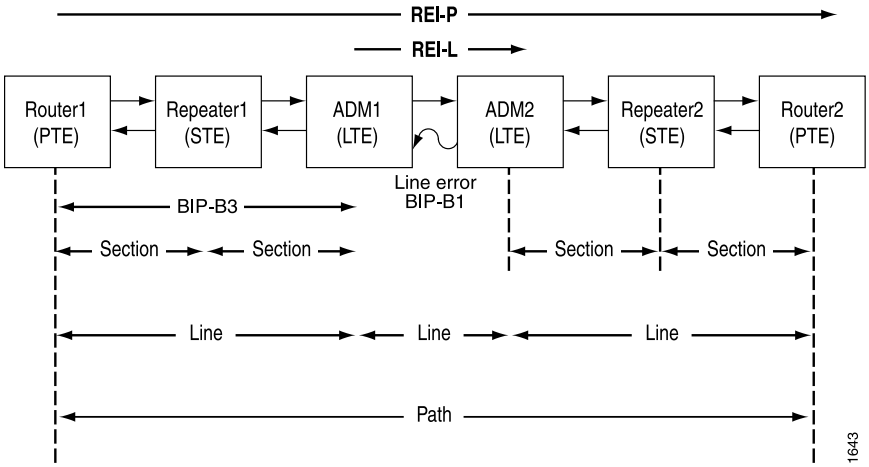
1. Example of Only an REI-P Counter Incrementing on page 167
2. Example of Both REI-L and REI-P Counters Incrementing on page 168

Example of Only an REI-P Counter Incrementing

Problem Figure 11 on page 167 shows an REI-P Counter Incrementing. The wavy line indicates that there is a line error in the section between ADM 1 and ADM 2.

Solution All diagnostics are from the perspective of Router 2 (the Juniper Networks router).

Figure 11: Example of a Router Receiving Only an REI-P Counter Incrementing



Meaning In Figure 11 on page 167, the progression of events occurring after the failure is as follows:

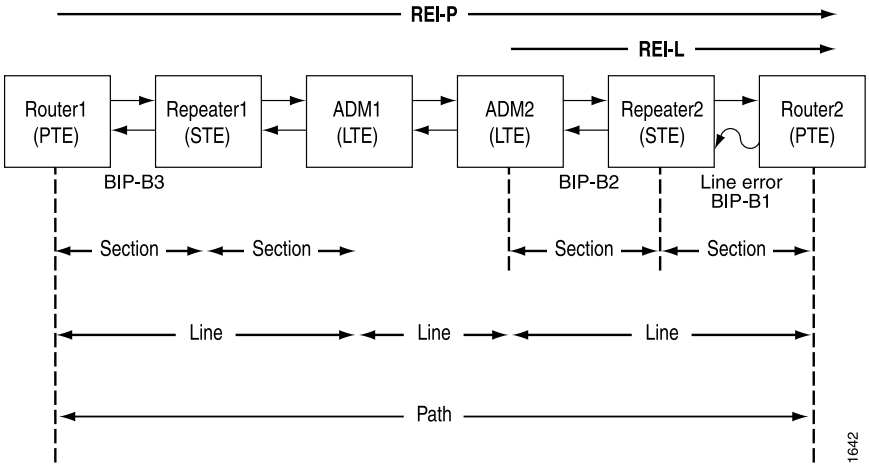
1. ADM 1 detects parity errors in the B1 byte.
2. ADM 1 sends an REI-L upstream to ADM 2.
3. Router 1 detects parity errors in the B3 byte.
4. Router 1 sends an REI-P upstream to Router 2.
5. Router 2 only sees an REI-P incrementing counter.

Example of Both REI-L and REI-P Counters Incrementing

Problem Figure 12 on page 168 shows both REI-L and REI-P Counters Incrementing. The wavy line indicates that there is a line error in the section between Repeater 2 and Router 2.

Solution All diagnostics are from the perspective of Router 2 (the Juniper Networks router).

Figure 12: Example of a Router Receiving Both An REI-L and REI-P Counter Incrementing



Meaning In Figure 12 on page 168, the progression of events occurring after the failure is as follows:

1. Repeater 2 detects some parity errors in the B1 byte from a corrupted SONET frame.
2. ADM 2 detects parity errors in the B2 byte.
3. ADM 2 sends an REI-L upstream to Router 2.
4. Router 1 detects parity errors in the B3 byte.
5. Router 1 sends back an REI-P upstream to Router 2.
6. Router 2 sees incrementing REI-L and REI-P errors.

Locate Bit Error Rate Alarms

Problem Bit error rate (BER) alarms are declared when the number of BIP-B2 errors hits a certain threshold. Depending on the threshold, there are two types of BER alarms. In both cases the interface is taken down.

- Bit error rate-signal degrade (BERR-SD) is declared when a bit error rate of 10^-6 is reached.
- Bit error rate-signal failure (BERR-SF) is declared when a bit error rate of 10^-3 is reached.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

user@host> **show interfaces so-*fpc/pic/port* extensive**

Sample Output

The following sample output displays a BERR-SD error:

```
user@router2> show interfaces so-1/1/1 extensive
[... Output truncated...]
  Active alarms  : BERR-SD
  Active defects : BERR-SD
  SONET PHY:            Seconds        Count  State
    PLL Lock                  0            0  OK
    PHY Light                 0            0  OK
  SONET section:
    BIP-B1                   22          101
    SEF                       0            0  OK
    LOS                       0            0  OK
    LOF                       0            0  OK
    ES-S                     22
    SES-S                     0
    SEFS-S                    0
  SONET line:
    BIP-B2                   22          103
    REI-L                     0            0
    RDI-L                     0            0  OK
    AIS-L                     0            0  OK
    BERR-SF                   0            0  OK
    BERR-SD                  11           53  Defect Active
    ES-L                     22
    SES-L                     4
    UAS-L                     2
    ES-LFE                    0
    SES-LFE                   0
    UAS-LFE                   0
  SONET path:
    BIP-B3                   22          166
    REI-P                     0            0
    LOP-P                     0            0  OK
    AIS-P                     0            0  OK
    RDI-P                     0            0  OK
    UNEQ-P                    0            0  OK
    PLM-P                     0            0  OK
    ES-P                     22
    SES-P                     3
    UAS-P                     1
    ES-PFE                    0
    SES-PFE                   0
    UAS-PFE                   0
```

Meaning Bit error rates can be caused by any of the following situations:

- Degrading optical fiber
- Optical transmitter or receiver problems
- Dirty fiber-optic connector
- Clocking issues
- Too much attenuation in the optical signal
- BIP-B1 and BIP-B3 are not used in the BER alarm calculations

Locate Payload Label Mismatch Path Alarms

Problem Payload mismatch path (PLM-P) alarms are reported by PTEs because the SONET byte used to determine the PLM-P alarm is located in the path overhead (the C2 byte). PLM-P alarms occur when the C2 byte received does not match the C2 byte transmitted by the PTE; for example, when the received C2 value is **Oxcf**, the transmitted C2 value must also be **Oxcf**.

NOTE: When the received C2 byte has a value of 0x01, the PTE accepts this value (regardless of the PTE setting) since 0x01 is considered a wildcard value.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

user@host> **show interfaces so-*fpc/pic/port* extensive**

Sample Output

```
user@router2> show interfaces so-1/1/1 extensive
[...Output truncated...]
SONET alarms   : PLM-P
SONET defects  : PLM-P
  [...Output truncated...]
SONET path:
    BIP-B3                    0           0
    REI-P                     0           0
    LOP-P                     0           0  OK
    AIS-P                     0           0  OK
    RDI-P                     2           1  OK
    UNEQ-P                    0           0  OK
    PLM-P        96     1 Defect Active
    ES-P                      0
    SES-P                     0
    UAS-P                     0
    ES-PFE                    2
    SES-PFE                   2
    UAS-PFE                   0
  Received SONET overhead:
    F1      : 0x00, J0      : 0x00, K1      : 0x00, K2      : 0x00
    S1      : 0x00, C2      :0x13 , C2(cmp) : 0xcf, F2      : 0x00
    Z3      : 0x00, Z4      : 0x00, S1(cmp) : 0x00, V5      : 0x00
    V5(cmp) : 0x00
```

```
Transmitted SONET overhead:
  F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
  S1      : 0x00, C2      : 0xcf , F2      : 0x00, Z3      : 0x00
  Z4      : 0x00, V5      : 0x00
```

Meaning In the **SONET path** section of the sample output, the PLM-P counter is incrementing and defective. In the **Received SONET overhead** and **Transmitted SONET overhead** sections, the received C2 value is **0x13** and the transmitted C2 value is **0xcf**. The C2 byte mismatch has caused a PLM-P alarm.

The C2 byte tells the PTE what kind of information is in the synchronous payload envelope (SPE). For example, when the SPE contains Asynchronous Transfer Mode (ATM) cells, the C2 byte has a value of **0x13**. If a Packet over SONET (POS) card is used on the Juniper Networks router, the link does not come up and a PLM-P alarm is raised (since the Juniper Networks router sends **0xcf** and receives **0x13**). However, if the C2 byte has a value of **0x01**, the PTE accepts this value (regardless of what the PTE is set to) since **0x01** is considered a wildcard value.

The SONET specifications have assigned a small handful of values (of the 256 possible binary values), but Juniper Networks routers only use a few of these (**0xcf** or **0x16** for POS, **0x13** for ATM, and so on). Table 21 on page 171 shows the synchronous transport signal (STS) path signal label assignments as described in Issue 3 (Sept. 2000) of the GR-253 CORE.

Table 21: STS Path Signal Label Assignments

Code (Hex)	Content of the STS SPE
00	Unequipped
01	Equipped - Nonspecific Payload
02	VT-Structured STS1 SPE a
03	Locked VT Mode a
04	Asynchronous Mapping for DS3
12	Asynchronous Mapping for DS4NA
13	Mapping for ATM
14	Mapping for DQDB
15	Asynchronous Mapping for FDDI
16	HDLC-over-SONET Mapping
FE	O.181 Test Signal (TSS1 to TSS3) Mapping b

On POS interfaces, Juniper Networks routers by default accept a C2 value of either **0xcf** or **0x16**. Any other values raise a PLM-P alarm. An important thing to remember is that the C2 byte value of **0x16** is a standardized value (per RFC 2615, G.707, and GR-253) used for POS interfaces. **0xcf** is used by default since much SONET equipment still uses this value. If you need to change this byte, use the **rfc-2615** option as follows:

user@host# **set interface so-*fpc/pic/port* sonet-options rfc-2615**

This option changes the following values:

```
C2 byte 22 (0x16)
FCS 32
payload-scrambling (this was already the default)
```

Locate Loss of Pointer Path Alarms

Problem A loss of pointer path (LOP-P) alarm indicates a possible provisioning problem and occurs when the Juniper Networks router cannot determine a valid payload pointer. The Juniper Networks router monitors the H1/H2 bytes, located in the line overhead area. This alarm is usually discovered upon initial provisioning of SONET circuits, and is not generally seen after the router has been deployed in the network for some time.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

user@host> **show interfaces so-*fpc/pic/port* extensive**

Sample Output

```
user@host> show interfaces so-1/1/1 extensive
[...Output truncated...]
SONET alarms  : LOP
  SONET defects : LOP
  SONET PHY:              Seconds        Count  State
    PLL Lock                    0            0  OK
    PHY Light                   0            0  OK
  SONET section:
    BIP-B1                      0            0
    SEF                         0            0  OK
    LOS                         0            0  OK
    LOF                         0            0  OK
    ES-S                        0
    SES-S                       0
    SEFS-S                      0
  SONET line:
    BIP-B2                      0            0
    REI-L                       0            0
    RDI-L                       0            0  OK
    AIS-L                       0            0  OK
    BERR-SF                     0            0  OK
    BERR-SD                     0            0  OK
    ES-L                        0
    SES-L                       0
    UAS-L                       0
    ES-LFE                      0
    SES-LFE                     0
    UAS-LFE                     0
  SONET path:
    BIP-B3                      0            0
    REI-P                       0            0
```

```
    LOP-P          174       0 Defect Active
    AIS-P                      0              0  OK
    RDI-P                      0              0  OK
    UNEQ-P                     0              0  OK
    PLM-P                      0              0  OK
     ES-P                    174
    SES-P                    174
    UAS-P                    174
    ES-PFE                     0
    SES-PFE                    0
    UAS-PFE                    0
[...Output truncated...]
```

Meaning The sample output shows that an LOP-P alarm occurred for 174 seconds. An LOP-P alarm can occur when the ADM on the other end is configured for nonconcatenate mode, while the Juniper Networks router is configured for concatenate mode (the default setting). In this instance, the pointer word in the required STS frame does not have the concatenation indicator set.

The condition of 8, 9, or 10 consecutive frames without valid pointer values can raise an LOP-P alarm.

NOTE: Although Juniper routers do not report pointer adjustments, an LOP-P alarm will not occur as long as the pointer adjustments stay within tolerance levels.

Locate Unequipped Payload Alarms

Problem An unequipped payload (UNEQ-P) alarm indicates a possible provisioning problem and occurs when the Juniper Networks router detects a value of **0x00** in the **C2** byte.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

user@host> **show interfaces so-*fpc/pic/port* extensive**

Sample Output

```
user@host> show interfaces so-1/1/1 extensive
[...Output truncated...]
SONET alarms  : UNEQ-P
  SONET defects : UNEQ-P
  SONET PHY:              Seconds        Count  State
    PLL Lock                    0            0  OK
    PHY Light                   0            0  OK
  SONET section:
    BIP-B1                      0            0
    SEF                         0            0  OK
    LOS                         0            0  OK
    LOF                         0            0  OK
    ES-S                        0
    SES-S                       0
    SEFS-S                      0
  SONET line:
    BIP-B2                      0            0
```

```
    REI-L                     0            0
    RDI-L                     0            0  OK
    AIS-L                     0            0  OK
    BERR-SF                   0            0  OK
    BERR-SD                   0            0  OK
    ES-L                      0
    SES-L                     0
    UAS-L                     0
    ES-LFE                    0
    SES-LFE                   0
    UAS-LFE                   0
  SONET path:
    BIP-B3                    0            0
    REI-P                     0            0
    LOP-P                     0            0  OK
    AIS-P                     0            0  OK
    RDI-P                     0            0  OK
    UNEQ-P                   10            2  Defect Active
    PLM-P                     0            0  OK
     ES-P                    10
    SES-P                    10
    UAS-P                     0
    ES-PFE                    0
    SES-PFE                   0
    UAS-PFE                   0
[...Output truncated...]
```

Meaning The sample output shows that an UNEQ-P alarm occurred within 10 seconds and was declared twice. An UNEQ-P alarm can occur when the ADM on the other end has not provisioned the SPE. An UNEQ-P alarm sets the STS SPE to all zeros when it is provisioned. If the alarm occurs, the problem is probably with the configuration of the ADM. Since the UNEQ-P is not a common alarm reported by Juniper Networks routers, it is a good idea to first check with the SONET provider.

Locate Phase Lock Loop Alarms

Problem The phase lock loop (PLL) alarm occurs when the PLL cannot lock on to a timing device, and indicates a possible hardware or network timing problem.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

```
user@host> show interfaces so-fpc/pic/port extensive
```

Sample Output

```
user@host> show interfaces so-1/1/1 extensive
[...Output truncated...]
Active alarms  : PLL
  Active defects : PLL
  SONET PHY:              Seconds        Count  State
   PLL Lock       26      0 PLL Lock Error
    PHY Light                 0            0  OK
  SONET section:
    BIP-B1                    0            0
    SEF                       0            0  OK
    LOS                       0            0  OK
    LOF                       0            0  OK
    ES-S                      0
    SES-S                     0
```

```
    SEFS-S                    0
  SONET line:
    BIP-B2                    0            0
    REI-L                     0            0
    RDI-L                     3            3  OK
    AIS-L                     0            0  OK
    BERR-SF                   0            0  OK
    BERR-SD                   0            0  OK
    ES-L                      0
    SES-L                     0
    UAS-L                     0
    ES-LFE                    0
    SES-LFE                   0
    UAS-LFE                   0
  SONET path:
    BIP-B3                    0            0
    REI-P                     0            0
    LOP-P                     0            0  OK
    AIS-P                     0            0  OK
    RDI-P                     0            0  OK
    UNEQ-P                    0            0  OK
    PLM-P                     0            0  OK
    ES-P                      0
    SES-P                     0
    UAS-P                     0
    ES-PFE                    0
    SES-PFE                   0
    UAS-PFE                   0
[...Output truncated...]
```

Meaning The sample output shows a PLL alarm lasting for 26 seconds. You must investigate the timing source to diagnose the problem. The timing source is derived from an incoming SONET circuit (when **clock external** is configured), or from the onboard Stratum 3 clock (when **clock internal** is configured). Internal clocking is the default for Juniper Networks routers.

The cause of the problem differs depending on the type of system board on the router. (See Table 22 on page 176.) For example:

- On the M20 and M40 Internet router OC48-SM-IR PIC and the M160 Internet router OC192 board, the problem might be caused by the following:
- An out-of-tolerance clock coming from the far end, if clocking external is configured.
- An out-of-tolerance clock coming from the far end or a problem with the board being unable to lock on to its internal clock to derive the transmit clock, if clocking internal is configured.
- On OC3 and OC12 PICs, the PIC not establishing a lock to the onboard clock to derive the outgoing clock.

To further diagnose the problem, try the following:

- Configure clocking to external. If the alarm disappears, the board might not have locked to the internal clock used to derive the outgoing clock.

- Configure clocking to internal and make sure that a loopback fiber is plugged in. If the PLL alarm persists, it is most likely a hardware problem. However, you may not be able to determine if the direction is on the inbound or outbound side of the board.

Table 22 on page 176 shows the location of the onboard clock on the various system boards of Juniper Networks routers.

Table 22: Location of the Onboard Clock

Router	System Board
M5, M10, M20, and M40 routers	System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), and Single Board Router (SBR)
OC48-SM-IR PIC used on the M20 and M40 routers	Flexible PIC Concentrator (FPC)
M40e and M160 routers	Miscellaneous Control Subsystem (MCS)
T-series routing platforms	SONET Clock Generator (SCG)

Related Documentation

- Investigate Interface Steps and Commands on page 135
- Monitor SONET Interfaces on page 138
- Use Loopback Testing for SONET Interfaces on page 146
- Enable SONET Payload Scrambling on page 176
- Check the SONET Frame Checksum on page 180

Enable SONET Payload Scrambling

This section includes the following information to assist you when troubleshooting SONET interfaces:

- Checklist for Enabling SONET Payload Scrambling on page 176
- Understand SONET Payload Scrambling on page 177

Checklist for Enabling SONET Payload Scrambling

Table 23 on page 176 provides links and commands for SONET payload scrambling and how to check and configure it.

Table 23: Checklist for Enabling SONET Payload Scrambling

Tasks	Command or Action
"Understand SONET Payload Scrambling" on page 177	
1. Check SONET HDLC Payload Scrambling on page 178	**show configuration interfaces | *interface-name*** **show interfaces *interface-name***

Table 23: Checklist for Enabling SONET Payload Scrambling *(continued)*

Tasks	Command or Action
2. Configure SONET HDLC Payload Scrambling on page 179	**[edit]** **edit interfaces *so-fpc/pic/port* sonet-options** **set payload-scrambler** **show** **commit**

Understand SONET Payload Scrambling

SONET payload scrambling preserves data integrity. Scrambling is designed to randomize the digital bits (pattern of 1s and 0s) carried in the Asynchronous Transfer Mode (ATM) cells (physical layer frame). Randomizing the digital bits can prevent continuous, long strings of all 1s or all 0s. Transitions between 1s and 0s are used by some physical layer protocols to maintain clocking. SONET interfaces support two levels of scrambling, as follows:

- SONET frame scrambling mode required by the International Telecommunications Union Telecommunication Standardization (ITU-T) GR-253 standard. This mode uses a 1 + x6 + x7 algorithm to scramble the section overhead of the SONET frame. It does not scramble the first row of the section overhead.
- Cell payload scrambling is optional and is defined in ITU-T I.432, section 4.5.3. This mode randomizes the bits in the payload portion of an ATM cell to make sure that the beginning of each new cell is recognized. It leaves the 5-byte header unscrambled.

Synchronous Transport System (STS) stream scrambling must be enabled on every SONET device and is the default for SONET interfaces.

Cell payload scrambling or SONET High-level Data Link Control (HDLC) scrambling can be enabled or disabled, and on Juniper routers is enabled by default to provide better link stability. Both sides of a connection must either use scrambling or not use it.

NOTE: HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling because the software rejects configurations that have both features enabled. For more information, see the *Junos Network Interfaces Configuration Guide*

On a Channelized OC12 interface, the SONET **payload-scrambler** statement is ignored. To configure scrambling on the DS3 channels on the interface, include the **t3-options payload-scrambler** statement in the configuration for each DS3 channel.

1. Check SONET HDLC Payload Scrambling on page 178
2. Configure SONET HDLC Payload Scrambling on page 179

Check SONET HDLC Payload Scrambling

Purpose If you find that payload scrambling is not enabled, you might want to enable or configure it because it provides better link stability when it is working.

Action In the Junos OS command-line interface (CLI) operational mode, you can use one of the following two commands to check for SONET HDLC control payload scrambling:

```
user@host> show configuration interfaces | interface-name
```

or

```
user@host> show interfaces interface-name
```

Sample Output 1

```
user@host> show configuration interfaces so-0/0/0
encapsulation cisco-hdlc;
sonet-options {
    payload-scrambler;
}
unit 0 {
    family inet {
        address 9.0.0.2/32 {
            destination 9.0.0.1;
        }
    }
    family mpls;
}
```

Sample Output 2

```
user@host> show configuration interfaces so-0/0/0
encapsulation cisco-hdlc;
sonet-options {
    no-payload-scrambler;
}
unit 0 {
    family inet {
        address 9.0.0.2/32 {
            destination 9.0.0.1;
        }
    }
    family mpls;
}
```

Sample Output 3

```
user@host> show interfaces so-0/0/1
Physical interface: so-0/0/1, Enabled, Physical link is Up
  Interface index: 48, SNMP ifIndex: 114
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
Loopback: None, FCS: 32,
  Payload scrambler: Disabled
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 70627 (00:00:07 ago), Output: 70791 (00:00:08 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Opened, mpls: Not-configured

  Input rate     : 78056456 bps (6504 pps)
  Output rate    : 78044840 bps (6503 pps)
  SONET alarms   : None
```

```
SONET defects  : None
Logical interface so-0/0/1.0 (Index 61) (SNMP ifIndex 118)
  Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
  Protocol inet, MTU: 4470, Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 192.168.50.0/30, Local: 192.168.50.1
  Protocol iso, MTU: 4470, Flags: None
```

Meaning Sample output 1 shows that the SONET interface payload scrambling has been enabled.

Sample output 2 shows that HDLC payload scrambling has been disabled. If you use the **show configuration** or **show configuration interfaces** command, you must scroll to the particular interface for payload scrambling status.

Sample output 3 shows that payload scrambling has been disabled. To explicitly configure payload scrambling, see "Configure SONET HDLC Payload Scrambling" on page 179.

Configure SONET HDLC Payload Scrambling

Purpose You might want to configure SONET HDLC payload scrambling (which is the configurable cell payload scrambling mentioned earlier) if it has been disabled. Configuring payload scrambling provides better link stability.

NOTE: Payload scrambling is the default for Juniper Networks routers. To return to the default, that is, to re-enable payload scrambling, delete the **no-payload-scrambler** statement from the configuration.

Action To explicitly configure HDLC payload scrambling, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit interfaces so-fpc/pic/port sonet-options
   ```

2. Configure payload scrambling:

   ```
   [edit interfaces so-fpc/pic/port sonet-options]
   user@host# set payload-scrambler
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit interfaces so-0/0/0 sonet-options]
   user@host# show
   payload-scrambler;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

Related Documentation

- Investigate Interface Steps and Commands on page 135
- Monitor SONET Interfaces on page 138
- Use Loopback Testing for SONET Interfaces on page 146
- Locate SONET Alarms and Errors on page 158
- Check the SONET Frame Checksum on page 180

Check the SONET Frame Checksum

This section includes the following information to assist you when troubleshooting SONET interfaces:

- Checklist for Checking the SONET Frame Checksum on page 180
- Check the SONET Frame Checksum on page 181
- Configure a SONET Frame Checksum on page 184

Checklist for Checking the SONET Frame Checksum

Purpose To check and configure SONET frame checksum.

Action Table 24 on page 180 provides the links and commands for SONET frame checksum.

Table 24: Checklist for Checking the SONET Frame Checksum

Tasks	Command or Action
Understand the SONET Frame Checksum	
"Check the SONET Frame Checksum" on page 181	
1. Examine Output for Framing Errors on page 181	**show interfaces *interface-name* extensive**
2. Check the FCS Configuration on page 183	**show configuration interfaces | *interface-name*** **show interfaces *interface-name***
"Configure a SONET Frame Checksum" on page 184	
1. Return to the Default 16-Bit Checksum on page 185	**[edit]** **edit interfaces *so-fpc/pic/port* sonet-options** **delete fcs 32** **show** **commit**
2. Configure a 16-Bit Checksum on page 185	**[edit]** **edit interfaces *so-fpc/pic/port* sonet-options** **set fcs 16** **show** **commit**

Table 24: Checklist for Checking the SONET Frame Checksum *(continued)*

Tasks	Command or Action
3. Configure a 32-Bit Checksum on page 186	[edit] edit interfaces *so-fpc/pic/port* sonet-options set (fcs 32 | rfc-2615) show commit

Check the SONET Frame Checksum

If you are having problems with a connection, check that the FCS matches on both sides of the connection.

To check the SONET frame checksum, follow these steps:

1. Examine Output for Framing Errors on page 181
2. Check the FCS Configuration on page 183

Examine Output for Framing Errors

Purpose By examining the output for an interface, you can determine if framing errors are incrementing in the absence of any SONET alarms or defects.

Action From the Junos OS command-line interface (CLI) operational mode, use the following command to check for framing errors:

user@host> **show interfaces** *interface-name* **extensive**

Sample Output

```
user@router1> show interfaces so-1/0/0 extensive
Physical interface: so-1/0/0, Enabled, Physical link is Up
  Interface index: 13, SNMP ifIndex: 18, Generation: 12
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
Loopback: None, FCS: 16 , Payload scrambler: Enabled
  Device flags   : Present Running
  Interface flags: Link-Layer-Down Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Hold-times     : Up 0 ms, Down 0 ms
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive statistics:
    Input : 6 (last seen 00:00:52 ago)
    Output: 11 (last sent 00:00:05 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Opened, mpls: Conf-req-sent

  CHAP state: Not-configured
  Last flapped   : 2002-11-01 22:28:30 UTC (1w5d 23:26 ago)
  Statistics last cleared: 2002-11-14 21:52:51 UTC (00:01:50 ago)
  Traffic statistics:
   Input  bytes  :                692                   0 bps
   Output bytes  :                716                  32 bps
   Input  packets:                 23                   0 pps
   Output packets:                 72                   0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 27 , Runs: 0, Giants: 0, Bucket drops: 0,
```

```
 Policed discards: 0, L3 incompletes: 0,
    L2 channel errors: 0, L2 mismatch timeouts: 0, HS link CRC errors: 0, HS link
 FIFO overflows: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, Aged packets: 0, HS link FIFO
underflows: 0
  SONET alarms  : None
  SONET defects : None
  SONET PHY:             Seconds        Count  State
    PLL Lock                   0            0  OK
    PHY Light                  0            0  OK
  SONET section:
    BIP-B1                     0            0
    SEF                        0            0  OK
    LOS                        0            0  OK
    LOF                        0            0  OK
    ES-S                       0
    SES-S                      0
    SEFS-S                     0
  SONET line:
    BIP-B2                     0            0
    REI-L                      0            0
    RDI-L                      0            0  OK
    AIS-L                      0            0  OK
    BERR-SF                    0            0  OK
    BERR-SD                    0            0  OK
    ES-L                       0
    SES-L                      0
    UAS-L                      0
    ES-LFE                     0
    SES-LFE                    0
    UAS-LFE                    0
  SONET path:
    BIP-B3                     0            0
    REI-P                      0            0
    LOP-P                      0            0  OK
    AIS-P                      0            0  OK
    RDI-P                      0            0  OK
    UNEQ-P                     0            0  OK
    PLM-P                      0            0  OK
    ES-P                       0
    SES-P                      0
    UAS-P                      0
    ES-PFE                     0
    SES-PFE                    0
    UAS-PFE                    0
  Received SONET overhead:
    F1      : 0x00, J0      : 0x00, K1      : 0x00, K2      : 0x00
    S1      : 0x00, C2      : 0xcf, C2(cmp) : 0xcf, F2      : 0x00
    Z3      : 0x00, Z4      : 0x00, S1(cmp) : 0x00, V5      : 0x00
    V5(cmp) : 0x00
  Transmitted SONET overhead:
    F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
    S1      : 0x00, C2      : 0xcf, F2      : 0x00, Z3      : 0x00
    Z4      : 0x00, V5      : 0x00
  Received path trace: router2 so-1/3/1
    73 6c 69 70 70 65 72 79 20 73 6f 2d 31 2f 33 2f   router2 so-1/3/1
    31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 0a   ................
  Transmitted path trace: router1 so-1/0/0
```

```
    68 61 69 72 79 20 73 6f 2d 31 2f 30 2f 30 00 00   router1 so-1/0/0
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
  HDLC configuration:
    Policing bucket: Disabled
    Shaping bucket : Disabled
    Giant threshold: 4484, Runt threshold: 3
  Packet Forwarding Engine configuration:
    Destination slot: 1, PLP byte: 1 (0x00)
    CoS transmit queue             Bandwidth           Buffer Priority   Limit
                              %          bps   %        bytes
    0 best-effort            95    147744000  95            0      low    none
    3 network-control         5      7776000   5            0      low    none
  Logical interface so-1/0/0.0 (Index 8) (SNMP ifIndex 108) (Generation 9)
    Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: PPP
    Protocol inet, MTU: 4470, Generation: 15, Route table: 1
      Flags: Is-Primary
      Addresses, Flags: Dest-route-down Is-Default Is-Preferred Is-Primary
       Destination: 1.1.6.1, Local: 1.1.6.2, Broadcast: Unspecified, Generation:
 15
    Protocol iso, MTU: 4470, Generation: 16, Route table: 1
      Flags: Is-Primary
    Protocol mpls, MTU: 4458, Generation: 17, Route table: 1
      Flags: Protocol-Down, Is-Primary
```

Meaning The sample output shows that Router 1 is configured for FCS 16, that framing errors have incremented to 27, and that there are no SONET alarms or defects. Incrementing framing errors, in the absence of any SONET alarms or defects, are a symptom of SONET frame checksum errors.

Check the FCS Configuration

Purpose If you are having problems with a connection, check your router's FCS configuration and, if possible, the FCS configuration on the router on the other side of the connection.

Action From the Junos OS CLI operational mode, use one of the following two commands to check the SONET frame checksum:

user@host> **show configuration interfaces** |*interface-name*

or

user@host> **show interfaces***interface-name*

NOTE: The option to display a specific configuration with the **show configuration** command hierarchy was introduced in Junos OS Release 5.3.

Sample Output 1

```
user@host> show configuration interfaces so-0/0/0
encapsulation cisco-hdlc;
sonet-options {
fcs 32;
    payload-scrambler;
}
```

```
unit 0 {
    family inet {
        address 9.0.0.2/32 {
            destination 9.0.0.1;
        }
    }
    family mpls;
}
```

Sample Output 2

```
user@host> show interfaces so-0/0/1
Physical interface: so-0/0/1, Enabled, Physical link is Up
  Interface index: 48, SNMP ifIndex: 114
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
Loopback: None, FCS: 32,
   Payload scrambler: Disabled
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 70627 (00:00:07 ago), Output: 70791 (00:00:08 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Opened, mpls: Not-configured

  Input rate     : 78056456 bps (6504 pps)
  Output rate    : 78044840 bps (6503 pps)
  SONET alarms   : None
  SONET defects  : None
  Logical interface so-0/0/1.0 (Index 61) (SNMP ifIndex 118)
    Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
    Protocol inet, MTU: 4470, Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 192.168.50.0/30, Local: 192.168.50.1
    Protocol iso, MTU: 4470, Flags: None
```

Meaning Sample output 1 shows that FCS 32 is configured. If you use the **show configuration** or **show configuration interfaces** command, you must scroll to the particular interface for the FCS configuration status.

Meaning Sample output 2 shows that FCS 32 is configured. To change the FCS configuration, see "Return to the Default 16-Bit Checksum" on page 185, "Configure a 16-Bit Checksum" on page 185, or "Configure a 32-Bit Checksum" on page 186.

Configure a SONET Frame Checksum

After you have checked the FCS and determined that a problem exists, you might need to do one of the following, depending on the situation:

NOTE: By default, SONET interfaces use a 16-bit frame checksum. You can configure a 32-bit checksum, which provides more reliable packet verification. However, some older equipment may not support 32-bit checksums.

Return to the Default 16-Bit Checksum

Action To return to the default 16-bit frame checksum, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host#  edit interfaces so-fpc/pic/port sonet-options
   ```

2. Delete the **fcs 32** statement from the configuration:

   ```
   [edit]
   user@host#  delete fcs 32
   ```

3. Verify the deletion:

   ```
   user@host# show
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

Configure a 16-Bit Checksum

Action To explicitly configure the 16-bit checksum, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit interfaces so-fpc/pic/port sonet-options
   ```

2. Configure the 16-bit checksum:

   ```
   [edit interfaces so-fpc/pic/port sonet-options]
   user@host# set fcs 16
   ```

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit interfaces so-0/0/0 sonet-options]
   user@host# show
   fcs 16;
   ```

4. Commit the configuration:

   ```
   user@host# commit
   ```

Configure a 32-Bit Checksum

Action To explicitly configure the 32-bit checksum, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit interfaces so-fpc/pic/port sonet-options
   ```

2. Configure the 32-bit checksum:

   ```
   [edit interfaces so-fpc/pic/port sonet-options]
   user@host# set (fcs 32 | rfc-2615)
   ```

   NOTE: The rfc-2615 statement automatically configures the interface to use FCS 32 and changes the C2 byte to 0x16, as per the RFC.

3. Verify the configuration:

   ```
   user@host# show
   ```

   For example:

   ```
   [edit interfaces so-0/0/0 sonet-options]
   user@host# show
   fcs 32;
   ```

   or

   ```
   [edit interfaces so-0/0/0 sonet-options]
   user@host# show
   rfc-2615;
   ```

1. Commit the configuration:

   ```
   user@host# commit
   ```

   NOTE: On a Channelized OC12 interface, the sonet-options fcs statement is not supported. To configure FCS on each DS3 channel, you must include the t3-options fcs statement in the configuration for each channel.

Related Documentation

- Investigate Interface Steps and Commands on page 135
- Monitor SONET Interfaces on page 138
- Use Loopback Testing for SONET Interfaces on page 146
- Locate SONET Alarms and Errors on page 158
- Enable SONET Payload Scrambling on page 176

PART 5

Index

Index

Symbols

A

B

C

D

E

F

H

I

K

L

R

S

T

U

V

W

Z

Index of Statements and Commands