

Junos[®] OS

SONET/SDH Interfaces User Guide for Routing Devices

Published
2020-03-23

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos[®] OS SONET/SDH Interfaces User Guide for Routing Devices
Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About the Documentation | xii

Documentation and Release Notes | xii

Using the Examples in This Manual | xii

 Merging a Full Example | xiii

 Merging a Snippet | xiv

Documentation Conventions | xiv

Documentation Feedback | xvii

Requesting Technical Support | xvii

 Self-Help Online Tools and Resources | xviii

 Creating a Service Request with JTAC | xviii

1

Overview

SONET/SDH Interfaces Overview | 2

SONET/SDH Interfaces Overview | 2

2

Configuring SONET/SDH Interfaces

Configuring SONET/SDH Physical Interface Properties | 5

Configuring SONET/SDH Physical Interface Properties | 6

 Configuring SONET/SDH Physical Interface Options | 6

 Configuring SONET/SDH Interface-Specific Options | 7

 Configuring MPLS Option for Passive Monitoring | 10

 Configuring Automatic Protection Switching Options | 10

Configuring the Media MTU | 14

Configuring the Media MTU on SONET/SDH Interfaces | 15

Framing Mode Overview | 17

Configuring SONET/SDH Framing Mode for Ports | 18

Configuring Virtual Tributary Mapping | 19

Incrementing STM ID Overview | 20

Configuring an Incrementing STM ID to Interoperate with Older Equipment in SDH Mode | 21

SONET/SDH Rate-Selectability Overview | 22

Configuring SONET/SDH Rate-Selectability | 24

SONET/SDH Interface Speed Overview	26
Configuring SONET/SDH Interface Speed	28
SONET/SDH Header Byte Values Overview	30
Configuring SONET/SDH Header Byte Values to Identify Error Conditions	32
Understand the SONET Frame Checksum	33
Configuring the SONET/SDH Frame Checksum	34
Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs	36
Configuring Junos OS to Enable SONET/SDH Framing for ATM MICs	40
Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External	42
Configuring SONET/SDH Loopback Capability	42
Displaying SONET/SDH Loopback Capability Configuration	43
Determining Whether the Problem Is Internal or External with Loopback Capability	44
SONET/SDH Path Trace Identifier Overview	45
Configuring the SONET/SDH Path Trace Identifier for a Circuit	46
SONET/SDH HDLC Payload Scrambling Overview	46
Configuring SONET/SDH HDLC Payload Scrambling for Link Stability	47
Configuring the Clock Source on SONET/SDH Interfaces	48
Configuring Channelized IQ and IQE SONET/SDH Loop Timing	50
Damping Shorter Physical Interface Transitions	52
Configuring SONET Options for 10-Gigabit Ethernet Interfaces	53
Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode	55
Receive and Transmit Leaky Bucket Properties Overview	56
Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion	57
Configuring Interface Encapsulation on SONET/SDH Interfaces 	59
Understanding Interface Encapsulation on SONET/SDH Interfaces	59
Understanding Encapsulation on a Physical SONET/SDH Interface	60
Point-to-Point Protocol (PPP)	60
Cisco HDLC	60
Frame Relay	60

Frame Relay Ether Type	61
Understanding Encapsulation on a Logical SONET/SDH Interface	61
Configuring Interface Encapsulation on SONET/SDH Interfaces	62
Configuring the Encapsulation on a Physical SONET/SDH Interface	62
Displaying the Encapsulation on a Physical SONET/SDH Interface	63
Configuring the Frame Relay Encapsulation on a Logical SONET/SDH Interface	64
Configuring the Point-to-Point Protocol Encapsulation on a Physical SONET/SDH Interface	65
PPP Support on SONET/SDH Interfaces	65
Configuring PPP Support on SONET/SDH Interfaces	66
Configuring How SONET/SDH Interface Defects Are Handled 	68
SONET/SDH Defect Triggers Overview	68
SONET/SDH Defect Hold Times for Damping Interface Transitions Overview	70
Configuring SONET/SDH Defect Triggers	72
Configuring SONET/SDH Defect Triggers to Be Ignored	72
Configuring SONET/SDH Defect Hold Times	72
Displaying the Configuration Where the SONET/SDH Defects to be Ignored are Listed	73
Configuring APS and MSP to Protect from Circuit Failures 	75
Automatic Protection Switching and Multiplex Section Protection Overview	76
Configuring Automatic Protect Switching	77
Basic Automatic Protect Switching Overview	81
Configuring Basic Automatic Protect Switching	82
Example: Configuring Basic APS Support on Routers	83
Configuring Lockout of Protection for SDH Interfaces	88
APS Timers Overview	89
Configuring APS Timers	90
Container Interfaces for APS on SONET Links Overview	91
Configuring Container Interfaces for APS on SONET Links	92
Configuring Container Interfaces on SONET Links	92
Displaying Container Interface Configuration	94
Displaying the APS Container Interface Configuration	96
APS Using a Container Interface with ATM Encapsulation Overview	97

Configuring APS Using a Container Interface with ATM Encapsulation	97
Displaying APS Using a Container Interface with ATM Encapsulation	98
Displaying APS Using a Container Interface with ATM Encapsulation	99
Displaying the APS Container Interface Configuration	100
APS Load Sharing Between Circuit Pairs Overview	101
Configuring APS Load Sharing	102
Example: Configuring APS Load Sharing Between Circuit Pairs	103
Link PIC Redundancy Overview	107
Configuring Link PIC Redundancy	108
Configuring Link State Replication	108
Displaying Link PIC Redundancy	108
Switching Between the Working and Protect Circuits Overview	110
Configuring Switching Between the Working and Protect Circuits	111
Revertive Mode Overview	113
Configuring Revertive Mode	113
Switching Mode Overview	115
Configuring Switching Mode	116
Configuring Aggregated SONET/SDH Interfaces for High Availability 	118
Understanding Aggregated SONET/SDH Interfaces	118
Understanding Aggregated SONET/SDH Properties	119
Creating Aggregated SONET/SDH Interfaces	119
SONET/SDH Link Aggregation Overview	119
Aggregated SONET/SDH Link Speed Overview	119
Configuring Aggregated SONET/SDH Minimum Links	120
Configuring Aggregated SONET/SDH Interfaces	121
Configuring Aggregated SONET/SDH Interfaces	121
Configuring Device Count	121
Configuring Constituent Physical Interface	121
Configuring an Aggregated SONET/SDH Interfaces	122
Displaying the Aggregated SONET/SDH Interface Configuration	123
Deleting an Aggregated SONET/SDH Interface	124
Deleting the Interface	124
Deleting Device Count	125

- Configuring Filtering on a Aggregated SONET/SDH Interface | 125
 - Configuring Filters or Sampling on Aggregated SONET/SDH Links | 126
 - Configuring Filter Options | 126
- Configuring Sampling on Aggregated SONET/SDH Interfaces | 127
 - Configuring Sampling on a Aggregated SONET/SDH Interface | 127
 - Configuring Sampling Filter Options | 127
 - Configuring Forwarding Options For a Sampling Filter | 128

Monitoring and Troubleshooting Information

Monitoring SONET/SDH Interfaces | 131

- Packet Flow Monitoring on SONET/SDH Interfaces Overview | 131
 - To Monitor Packets with MPLS Labels | 131
- Enabling Packet Flow Monitoring on SONET/SDH Interfaces | 132
 - Configuring Packet Flow Monitoring on a SONET/SDH Interface | 133
 - Configuring Packet Flow Monitoring on a Monitoring Services Interface | 133
 - Removing MPLS Labels from Incoming Packets | 134
- Configuring Multicast Statistics Collection on SONET Interfaces | 135
- Configuring Multicast Statistics Collection on Aggregated SONET Interfaces | 136

Troubleshooting SONET/SDH Interfaces | 138

- Configuring Interface Diagnostics Tools to Test the Physical Layer Connections | 138
 - Configuring Loopback Testing | 138
 - Configuring BERT Testing | 141
 - Starting and Stopping a BERT Test | 144
- Investigating Interface Steps and Commands | 146
 - Investigating Interface Steps and Commands Overview | 146
 - Monitoring Interfaces | 146
 - Performing a Loopback Test on an Interface | 147
 - Locating Interface Alarms | 150
- Monitoring SONET Interfaces | 151
 - Checklist for Monitoring SONET Interfaces | 151
 - Monitoring SONET Interfaces | 151
 - Displaying the Status of SONET Interfaces | 152
 - Displaying the Status of a Specific SONET Interface | 153

Displaying Extensive Status Information for a Specific SONET Interface	155
Monitoring Statistics for a SONET Interface	157
Verifying the Status of the Logical Interface	160
Using Loopback Testing for SONET Interfaces	162
Checklist for Using Loopback Testing for SONET Interfaces	162
Diagnosing a Suspected Hardware Problem with a SONET Interface	164
Creating a Loopback	164
Creating a Physical Loopback	165
Configuring a Local Loopback	165
Setting Clocking to Internal	166
Verifying That the SONET Interface Is Up	167
Clearing SONET Interface Statistics	170
Checking That the Received and Transmitted Path Trace Are the Same	170
Forcing the Link Layer to Stay Up	172
Configuring Encapsulation to Cisco-HDLC	172
Configuring No-Keepalives	173
Pinging the SONET Interface	174
Checking for SONET Interface Error Statistics	175
Diagnosing a Suspected Circuit Problem	177
Creating a Loop from the Router to the Network	177
Creating a Loop to the Router from Various Points in the Network	178
Locating SONET Alarms and Errors	179
List of Common SONET Alarms and Errors	179
Displaying SONET Alarms and Errors	181
Locating Most Common SONET Alarms and Errors	185
Locating Loss of Signal Alarms	186
Locating Alarm Indication Signal Alarms	188
Example of a Router Receiving Only an AIS-P Alarm	188
Example of a Router Receiving Both an AIS-L and AIS-P Alarm	189
Locating Remote Defect Indication Alarms	191
Example of a Router Receiving Only an RDI-P Alarm	191
Example of a Router Receiving Both an RDI-L and RDI-P Alarm	192

Locating Remote Error Indication Line Errors | 193

Example of Only an REI-P Counter Incrementing | 194

Example of Both REI-L and REI-P Counters Incrementing | 194

Locating Bit Error Rate Alarms | 196

Locating Payload Label Mismatch Path Alarms | 198

Locating Loss of Pointer Path Alarms | 201

Locating Unequipped Payload Alarms | 203

Locating Phase Lock Loop Alarms | 205

Enabling SONET Payload Scrambling | 209

Checklist for Enabling SONET Payload Scrambling | 209

Understanding SONET Payload Scrambling | 209

Checking SONET HDLC Payload Scrambling | 210

Configuring SONET HDLC Payload Scrambling | 213

Checking the SONET Frame Checksum | 214

Checklist for Checking the SONET Frame Checksum | 214

Understand the SONET Frame Checksum | 215

Checking the SONET Frame Checksum | 216

Examining Output for Framing Errors | 216

Checking the FCS Configuration | 219

Configuring a SONET Frame Checksum | 222

Returning to the Default 16-Bit Checksum | 222

Configuring a 16-Bit Checksum | 223

Configuring a 32-Bit Checksum | 224

Configuration Statements and Operational Commands

Configuration Statements | 227

advertise-interval | 229

aggregate (SONET/SDH) | 230

aggregate-ports | 231

aggregated-sonet-options | 232

annex | 233

aps | 234

atm-options | 236

authentication-key | 238

bytes | 239

clocking | 241

container-devices | 242

container-list | 243

container-options | 244

container-type | 245

encapsulation (Container Interface) | 246

encapsulation (Logical Interface) | 247

family | 252

fast-aps-switch | 258

fcs | 260

filter | 262

force | 264

framing | 265

framing (SONET and SDH Interfaces) | 266

hold-time (Physical Interface) | 268

hold-time (APS) | 270

hold-time (SONET/SDH Defect Triggers) | 271

ignore | 273

link-speed (Aggregated SONET/SDH) | 274

lockout | 275

loop-timing | 276

loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3) | 277

member-interface-speed | 279

member-interface-type | 280

minimum-links | 281

mpls (Interfaces) | 283

mtu | 284

neighbor (Automatic Protection Switching for SONET/SDH) | 288

overflow (Receive Bucket) | 289

overflow (Transmit Bucket) | 290

paired-group | 291

passive-monitor-mode | 292

path-trace | 293

payload-scrambler | 294

pop-all-labels | 296

preserve-interface | 297

protect-circuit | 298

rate | 299

receive-bucket | 300

receive-options-packets | 301

receive-ttl-exceeded | 302

request | 303

required-depth | 304

revert-time (Interfaces) | 305

rfc-2615 | 306

sonet-options | 307

speed (SONET/SDH) | 310

switching-mode | 311

t3-options | 312

threshold | 313

transmit-bucket | 314

trigger | 315

vtmapping | 317

working-circuit | 318

z0-increment | 319

Operational Commands | 320

show aps | 321

show interfaces (Aggregated SONET/SDH) | 326

show interfaces (SONET/SDH) | 336

show interfaces diagnostics optics (SONET) | 373

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xii
- Using the Examples in This Manual | xii
- Documentation Conventions | xiv
- Documentation Feedback | xvii
- Requesting Technical Support | xvii

Use this guide to configure and monitor SONET/SDH interfaces for high speed transmission of voice and data signals across fiber-optic networks.

[Junos OS Network Interfaces Library for Routing Devices](#)

Documentation and Release Notes

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

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

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

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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 [CLI Explorer](#).

Documentation Conventions

[Table 1 on page xv](#) 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xv 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
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

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

Convention	Description	Examples
<i>Italic text like this</i>	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 <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> 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)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

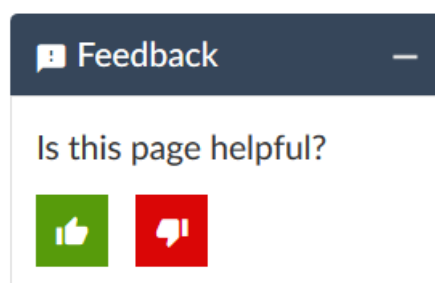
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

1

PART

Overview

SONET/SDH Interfaces Overview | 2

SONET/SDH Interfaces Overview

IN THIS CHAPTER

- [SONET/SDH Interfaces Overview | 2](#)

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 *Junos OS Administration Library*.



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 *request chassis pic*.

RELATED DOCUMENTATION

| [Configuring SONET/SDH Physical Interface Properties](#) | 6

2

PART

Configuring SONET/SDH Interfaces

Configuring SONET/SDH Physical Interface Properties | 5

Configuring Interface Encapsulation on SONET/SDH Interfaces | 59

Configuring How SONET/SDH Interface Defects Are Handled | 68

Configuring APS and MSP to Protect from Circuit Failures | 75

Configuring Aggregated SONET/SDH Interfaces for High Availability | 118

Configuring SONET/SDH Physical Interface Properties

IN THIS CHAPTER

- [Configuring SONET/SDH Physical Interface Properties | 6](#)
- [Configuring the Media MTU | 14](#)
- [Configuring the Media MTU on SONET/SDH Interfaces | 15](#)
- [Framing Mode Overview | 17](#)
- [Configuring SONET/SDH Framing Mode for Ports | 18](#)
- [Configuring Virtual Tributary Mapping | 19](#)
- [Incrementing STM ID Overview | 20](#)
- [Configuring an Incrementing STM ID to Interoperate with Older Equipment in SDH Mode | 21](#)
- [SONET/SDH Rate-Selectability Overview | 22](#)
- [Configuring SONET/SDH Rate-Selectability | 24](#)
- [SONET/SDH Interface Speed Overview | 26](#)
- [Configuring SONET/SDH Interface Speed | 28](#)
- [SONET/SDH Header Byte Values Overview | 30](#)
- [Configuring SONET/SDH Header Byte Values to Identify Error Conditions | 32](#)
- [Understand the SONET Frame Checksum | 33](#)
- [Configuring the SONET/SDH Frame Checksum | 34](#)
- [Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs | 36](#)
- [Configuring Junos OS to Enable SONET/SDH Framing for ATM MICs | 40](#)
- [Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External | 42](#)
- [SONET/SDH Path Trace Identifier Overview | 45](#)
- [Configuring the SONET/SDH Path Trace Identifier for a Circuit | 46](#)
- [SONET/SDH HDLC Payload Scrambling Overview | 46](#)
- [Configuring SONET/SDH HDLC Payload Scrambling for Link Stability | 47](#)
- [Configuring the Clock Source on SONET/SDH Interfaces | 48](#)
- [Configuring Channelized IQ and IQE SONET/SDH Loop Timing | 50](#)
- [Damping Shorter Physical Interface Transitions | 52](#)
- [Configuring SONET Options for 10-Gigabit Ethernet Interfaces | 53](#)
- [Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode | 55](#)

- [Receive and Transmit Leaky Bucket Properties Overview | 56](#)
- [Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion | 57](#)

Configuring SONET/SDH Physical Interface Properties

You can configure SONET/SDH physical interface options to accomplish various tasks.

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 Administration Library*.

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.

This topic includes the following tasks:

1. [Configuring SONET/SDH Physical Interface Options | 6](#)
2. [Configuring SONET/SDH Interface-Specific Options | 7](#)
3. [Configuring MPLS Option for Passive Monitoring | 10](#)
4. [Configuring Automatic Protection Switching Options | 10](#)

Configuring SONET/SDH Physical Interface Options

To configure the SONET/SDH physical interface options:

1. In configuration mode, go to the `[edit interfaces interface-name]` hierarchy level, where the *interface-name* is **so-fpc/pic/port**.

```
[edit]
user@host# edit interfaces so-fpc/pic/port
```


2. Configure the framing mode in SONET mode or SDH mode.

```
[edit interfaces so-fpc/pic/port]
user@host# set framing (sonet | sdh)
```

For more information, see [“Configuring SONET/SDH Framing Mode for Ports” on page 18](#).

3. Configure the virtual tributary mapping standard as either International Telephony Union standard (**itu-t**) or KLM standard (**klm**). Here, the KLM standard is set by default.

```
[edit interfaces so-fpc/pic/port]
user@host# set vt (itu-t | klm)
```

For more information, see [“Configuring Virtual Tributary Mapping” on page 19](#).

4. Configure an incrementing STM ID rather than a static one in the SDH overhead with the **z0-increment**. Note that you should include this option only for SDH mode. You can explicitly disable incrementing of the STM ID with the **no-z0-increment** option.

```
[edit interfaces so-fpc/pic/port]
user@host# set z0-increment | no-z0-increment
```

For more information, see [“Configuring an Incrementing STM ID to Interoperate with Older Equipment in SDH Mode” on page 21](#).

5. Configure the interface speed with the **oc3 | oc12 | oc48** option when the PIC is in concatenated mode and configure the speed with **oc3 | oc12** option when the PIC is in non-concatenated mode.

```
[edit interfaces so-fpc/pic/port]
user@host# set speed (oc3 | oc12 | oc48)
```

For more information, see [“Configuring SONET/SDH Interface Speed” on page 28](#).

Configuring SONET/SDH Interface-Specific Options

To configure the SONET/SDH interface-specific options:

1. Configure the **sonet-options** statement.

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

For more information, see [sonet-options](#).

2. Configure the aggregated SONET/SDH logical interface number from 0 through 15.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set aggregate asx
```

For more information, see [aggregate](#).

3. Configure the **bytes** option to set values in some SONET/SDH header bytes. You can configure this option with **c2 value**, **e1-quiet value**, **f1 value**, **f2 value**, **s1 value**, **z3 value**, and **z4 value**.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set bytes c2 value
user@host# set bytes e1-quiet value
user@host# set bytes f1 value
user@host# set bytes f2 value
user@host# set bytes s1 value
user@host# set bytes z3 value
user@host# set bytes z4 value
```

For more information, see “[Configuring SONET/SDH Header Byte Values to Identify Error Conditions](#)” on page 32.

4. Configure the frame checksum (FCS) on the interface as either 16-bit frame checksum or 32-bit frame checksum.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set fcs (16 | 32)
```

For more information, see “[Configuring the SONET/SDH Frame Checksum](#)” on page 34.

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

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set loopback (local | payload | remote)
```

For more information, see “[Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External](#)” on page 42.

6. Configure a path trace identifier, which is a text string that identifies the circuit. The text string that identifies the circuit.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set path-trace trace-string
```

For more information, see [“Configuring the SONET/SDH Path Trace Identifier for a Circuit” on page 46.](#)

7. Configure HDLC scrambling which provides better link stability. You can enable HDLC scrambling with **payload-scrambler** option and disable it with **no-payload-scrambler** option.

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

For more information, see [“Configuring SONET/SDH HDLC Payload Scrambling for Link Stability” on page 47.](#)

8. Configure the **rfc-2615** option to enable features described in RFC 2615, PPP over SONET/SDH.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set rfc-2615
```

For more information, see [“Configuring PPP Support on SONET/SDH Interfaces” on page 66.](#)

9. Configure SONET/SDH defect triggers as either ignore or hold time.

The defect triggers can be ignored. By default all SONET/SDH defect triggers are honored if you do not include the **trigger defect ignore** statement.

You can apply up and down hold times to SONET/SDH defect trigger. If you do not include the **trigger defect hold-time** statement, when a defect is detected the interface is marked down immediately and when the defect becomes absent the interface is marked up immediately.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set trigger defect ignore
user@host# set trigger defect hold-time up milliseconds down milliseconds
```

For more information, see [“Configuring SONET/SDH Defect Triggers” on page 72.](#)

Configuring MPLS Option for Passive Monitoring

To configure the MPLS options for passive monitoring:

1. Configure the **mpls** option to process incoming IP packets that have MPLS labels for passive monitoring on ATM and SONET/SDH interfaces and 10-Gigabit Ethernet interfaces in WAN PHY mode.

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

For more information, see [mpls](#).

2. Configure the **pop-all-labels** option to remove up to two MPLS labels from incoming IP packets in passive monitoring.

```
[edit interfaces so-fpc/pic/port sonet-options mpls]  
user@host# set pop-all-labels
```

For more information, see [pop-all-labels](#).

3. Configure the **required-depth** option as either **1** or **2** in the **pop-all-labels** statement to 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.

```
[edit interfaces so-fpc/pic/port sonet-options mpls pop-all-labels]  
user@host# set required-depth
```

For more information, see [required-depth](#).

Configuring Automatic Protection Switching Options

To configure Automatic Protection Switching (APS) options:

1. Configure the Automatic Protection Switching option.

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

For more information, see [“Configuring Basic Automatic Protect Switching” on page 82](#).

2. Configure the 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. You can set the APS interval from 1 through 65,534 millisecond. By default, 1000 milliseconds is set as advertise interval.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set advertise-interval milliseconds
```

For more information, see [“Configuring APS Timers” on page 90](#).

3. Configure the **annex-b** option for Multiplex Section Protection (MSP) switching on SDH interfaces for M320 and M120 routers only.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set annex-b
```

For more information, see [“Configuring Lockout of Protection for SDH Interfaces” on page 88](#).

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

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set authentication-key key
```

For more information, see [authentication-key](#).

5. Configure the **fast-aps-switch** option to reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits in M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set fast-aps-switch
```

For more information, see [fast-aps-switch](#).

6. Configure the **force** option to either protect mode or working mode to 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.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set force (protect | working)
```

For more information, see [force](#).

7. Configure the **hold-time** value in milliseconds to determine whether a neighbor APS router is operational where the hold-time value ranges from 1 through 65,354 milliseconds. By default, 3000 milliseconds (3 times the advertisement interval) is set as hold time.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set hold-time milliseconds
```

For more information, see [hold-time](#).

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

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set lockout
```

For more information, see [lockout](#).

9. Configure the address of the remote interface when you are configuring one router to be the working router and a second to be the protect router. You can configure this on one or both of the interfaces.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set neighbor address
```

For more information, see [neighbor](#).

10. Configure load sharing between two working protect circuit pairs where circuit's group name is as configured with the **protect-circuit** or **working-circuit** statement.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set paired-group group-name
```

For more information, see [“Configuring APS Load Sharing” on page 102](#).

11. Configure link state replication with **preserve-interface** option

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set preserve-interface
```

For more information, see [“Configuring Link PIC Redundancy” on page 108](#).

12. 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.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set protect-circuit group-name
```

For more information, see [protect-circuit](#).

13. Configure the **request** option as protect circuit or working circuit to perform a manual switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set request (protect | working)
```

For more information, see [“Configuring Switching Between the Working and Protect Circuits” on page 111](#).

14. Configure APS revertive mode in seconds ranging from 1 through 65,535 seconds which denotes the time to wait after the working circuit has again become functional before making the working circuit active again. By default, APS operates in nonrevertive mode.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set revert-time seconds
```

For more information, see [“Configuring Revertive Mode” on page 113](#).

15. Configure the interface in bidirectional mode or in unidirectional mode. By 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.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set switching-mode (bidirectional | unidirectional)
```

For more information, see [“Configuring Switching Mode” on page 116](#).

16. Configure the working router in an APS circuit pair.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set working-circuit group-name
```

For more information, see [working-circuit](#).

RELATED DOCUMENTATION

[Automatic Protection Switching and Multiplex Section Protection Overview | 76](#)

[Configuring SONET Options for 10-Gigabit Ethernet Interfaces | 53](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring the Media MTU

The media maximum transmission unit (MTU) is the largest data unit that can be forwarded without fragmentation. 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 *Media MTU Sizes by Interface Type*.

To configure the media-MTU size:

1. In configuration mode, go to the **[edit interfaces *interface-name*]** hierarchy level.

```
[edit ]
user@host# [edit interfaces interface-name]
```

2. Include the **mtu** statement.

```
[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*]

NOTE:

- Changing the media MTU or protocol MTU causes an interface to be deleted and added again.
- Because tunnel services interfaces are considered logical interfaces, you cannot configure the MTU setting for the physical interface. This means you cannot include the `mtu` statement at the [edit interfaces *interface-name*] hierarchy level for the following interface types: generic routing encapsulation (gr-), IP-IP (ip-), loopback (lo-), link services (ls-), multilink services (ml-), and multicast (pe-, pd-). You can, however, configure the protocol MTU on all tunnel interfaces except virtual tunnel (vt) interfaces. Starting in Junos OS Release 17.1R3, you cannot configure the maximum transmission unit (MTU) size for vt interfaces because the **mtu bytes** option is deprecated for vt interfaces. Junos OS sets the MTU size for vt interfaces by default to unlimited.
- If you configure an MTU value by including the `mtu` statement at the [edit interfaces *interface-name* unit *logical-unit-number* family *mpls*] hierarchy level, the configured value is used.

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” on page 14](#).

To configure the media-MTU size:

1. In configuration mode, go to the [edit interfaces *interface-name*] hierarchy level.

```
[edit ]
user@host# [edit interfaces interface-name]
```

2. Include the **mtu** statement.

```
[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*]

RELATED DOCUMENTATION

[Configuring Interface Encapsulation on SONET/SDH Interfaces](#) | 62

[mtu](#) | 284

Setting the Protocol MTU

Framing Mode Overview

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.

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. For per-port framing on SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP (MIC-3D-4OC3OC12-1OC48, MIC-3D-8OC3OC12-4OC48) in MX series routers, set the framing at the **[edit chassis fpc slot-number pic pic-number port port-number]** 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.

The following MICs and PICs support SONET or SDH framing mode on a per-port basis:

- The 4-port OC48 PIC with SFP installed, the next-generation SONET/SDH PICs with SFP, and the 4-port OC192 PIC on M Series, MX Series, and T Series routers.
- The SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, and the OC192/STM64 MICs with XFP on MX Series routers.

The 1-port OC192/STM64 MICs with XFP on MX Series routers support SONET or SDH framing on the single port. This functionality allows you to mix SONET and SDH modes on interfaces on a single PIC or MIC.

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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties](#) | 6

Configuring SONET/SDH Framing Mode for Ports

To configure framing on a per-port basis:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level.

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

2. Configure the SONET/SDH interface.

```
[edit interfaces]
user@host# edit so-fpc/pic/port
```

3. Configure the framing option in SDH mode or in SONET mode.

```
[edit interfaces so-fpc/pic/port]
user@host# set framing (sdh | sonet)
```

NOTE: For a channelized MIC, replace **so** with **coc3/coc12** when configuring the framing option as **sonet**. Similarly, replace **so** with **cstm1/cstm4** when configuring the framing option as **sdh**.

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

RELATED DOCUMENTATION

Configuring Virtual Tributary Mapping

You can configure virtual tributary mapping standard as either International Telephony Union standard (itu-t) or KLM standard (klm). Here, the KLM standard is set by default. For more information about virtual tributary mapping, see *Configuring Channelized STM1 Interfaces*.

To configure virtual tributary mapping on Channelized STM1 IQ and IQE PICs:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the interface name is **cau4-fpc/pic/port**.

```
[edit]
user@host# edit interfaces cau4-fpc/pic/port sonet-options
```

2. Configure virtual tributary mapping option in KLM standard. By default, virtual tributary mapping uses KLM standard.

```
[edit interfaces cau4-fpc/pic/port sonet-options]
user@host# set vtmapping klm
```

3. Configure virtual tributary mapping option in ITU-T standard alternatively.

```
[edit interfaces cau4-fpc/pic/port sonet-options]
user@host# set vtmapping itu-t
```

To configure virtual tributary mapping on STM1 PIC:

1. In configuration mode, go to the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level.

```
[edit]
user@host# edit chassis fpc slot-number pic pic-number
```

2. Configure virtual tributary mapping option in KLM mode. By default, virtual tributary mapping uses KLM mode.

```
[edit chassis fpc slot-number pic pic-number]
user@host# set vtmapping klm
```

3. Configure virtual tributary mapping option in ITU-T mode alternatively.

```
[edit chassis fpc slot-number pic pic-number]
user@host# set vtmapping itu-t
```

Channelized STM1-to-E1 Channel Mapping lists the KLM mappings used by the Channelized STM1-to-E1 PIC interfaces.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Interfaces Overview | 2](#)

Incrementing STM ID Overview

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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring an Incrementing STM ID to Interoperate with Older Equipment in SDH Mode | 21](#)

Configuring an Incrementing STM ID to Interoperate with Older Equipment in SDH Mode

To configure an incrementing STM ID explicitly.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the *interface-name* is **so-fpc/pic/port**.

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

2. Configure an incrementing STM ID rather than a static one in the SDH overhead with the **z0-increment**. Note that you should include this option only for SDH mode.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set z0-increment
```

To explicitly disable incrementing of the STM ID.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the *interface-name* is **so-fpc/pic/port**.

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

2. Configure the **no-z0-increment** option explicitly to disable incrementing of the STM ID.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set no-z0-increment
```

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Incrementing STM ID Overview | 20](#)

SONET/SDH Rate-Selectability Overview

You can configure rate selectability on the SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, and Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP by specifying the port speed as `oc12-stm4`, `oc3-stm1`, or `oc48-stm16`.

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

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 3 on page 22 shows the port speed restrictions on the SONET/SDH OC3/STM1 (Multi-Rate) MICs.

Table 3: 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	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 4 on page 22 and Table 5 on page 23 indicate the port configuration restrictions of the 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP.

Table 4: 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

Table 4: OC12/STM4 Port Configuration Restrictions on MIC-3D-8CHOC3-4CHOC12 (*continued*)

Ports Configured as OC3/STM1	Ports Available for OC12/STM4 Configuration
1 or 5	0, 2, and 3
2 or 6	0, 1, and 3
3 or 7	0, 1, and 2

Table 5: 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 6 on page 23](#) and [Table 7 on page 23](#) indicate the port configuration restrictions of the 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP.

Table 6: 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 7: OC3/STM1 Port Configuration Restrictions on MIC-3D-4CHOC3-2CHOC12

Ports Configured as OC12/STM4	Ports Available for OC3/STM1 Configuration
None	All ports (0 through 3)
0	All ports except 2

Table 7: OC3/STM1 Port Configuration Restrictions on MIC-3D-4CHOC3-2CHOC12 (continued)

Ports Configured as OC12/STM4	Ports Available for OC3/STM1 Configuration
1	All ports except 3

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring SONET/SDH Rate-Selectability | 24](#)

Configuring SONET/SDH Rate-Selectability

You can configure rate selectability on the SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, and Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP by specifying the port speed.

To configure the rate selectability:

1. In configuration mode, go to the `[edit chassis fpc slot-number pic pic-number port port-number]` hierarchy level.

```
[edit]
user@host# edit chassis fpc slot-number pic pic-number port port-number
```

2. Configure the **speed** option to enable rate selectability on SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP, and Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP.

```
[edit chassis fpc slot-number pic pic-number port port-number]
user@host# set speed (oc12-stm4 | oc3-stm1 | oc48-stm16)
```

NOTE:

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

To disable the rate selectability feature on the 8-port SONET/SDH OC3/STM1 (Multi-Rate) MIC:

1. In configuration mode, go to the **[edit chassis fpc slot-number pic pic-number port port-number]** hierarchy level.

```
[edit]
user@host# edit chassis fpc slot-number pic pic-number port port-number
```

2. Configure the **no-multi-rate** option to disable rate selectability.

```
[edit chassis fpc slot-number pic pic-number port port-number]
user@host# set no-multi-rate
```

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Rate-Selectability Overview | 22](#)

[SONET/SDH Interfaces Overview | 2](#)

SONET/SDH Interface Speed Overview

You can configure the interface speed. The speed you select is dependent upon whether the PIC is in concatenated or nonconcatenated mode. Available speeds depend on whether the PIC is in concatenated mode or nonconcatenated mode.

- Concatenated mode—Here, the bandwidth of the interface is in a single channel. You can select the **oc3** | **oc12** | **oc48** option when the PIC is in concatenated mode.
- Nonconcatenated mode—Here, the PIC operates in channelized (multiplexed) mode. You can select the **oc3** | **oc12** option when the PIC is in nonconcatenated mode.

You can configure the speed of SONET/SDH interfaces on next-generation SONET/SDH Type 1 and Type 2 PICs with SFP.

By default, SONET/SDH PICs operate in concatenated mode.

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, Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, and SONET/SDH OC3/STM1 (Multi-Rate) (MIC-3D-4OC3OC12-1OC48, MIC-3D-8OC3OC12-4OC48) MICs 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 Administration Library*.

Table 8 on page 26 shows the mode combinations for the next-generation SONET/SDH Type 1 PICs with SFP.

Table 8: Type 1 PIC Mode Combinations

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

Table 8: Type 1 PIC Mode Combinations (*continued*)

PIC	Mode	Speed Configuration	Default Mode
1-port OC12	1xOC12 concatenated	<i>fpc/pic/0</i> speed oc12	Concatenated
	1xOC12 nonconcatenated	<i>fpc/pic/0:0</i> speed oc3	Nonconcatenated
	1xOC3 concatenated	<i>fpc/pic/0</i> speed oc3	

Table 9 on page 27 shows the mode combinations for the next-generation SONET/SDH Type 2 PICs with SFP.

Table 9: Type 2 PIC Mode Combinations

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

Table 9: Type 2 PIC Mode Combinations (*continued*)

PIC	Mode	Speed Configuration	Default Mode
	4xOC3 concatenated	<i>fpc/pic/port</i> speed oc3	Concatenated

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)
[Configuring SONET/SDH Interface Speed | 28](#)

Configuring SONET/SDH Interface Speed

To configure the speed of SONET/SDH interfaces in concatenated mode:

1. In configuration mode, go to the **[edit interfaces *interface-name*]** hierarchy level, where the *interface-name* is ***so-fpc/pic/port***.

```
[edit]
user@host# edit interfaces so-fpc/pic/port
```

2. Configure interface speed in concatenated mode.

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.

```
[edit interfaces so-fpc/pic/port]
user@host# set speed (oc3 | oc12 | oc48)
```

To configure the speed of SONET/SDH interfaces in nonconcatenated mode:

1. In configuration mode, go to the **[edit interfaces *interface-name*]** hierarchy level, where the *interface-name* is ***so-fpc/pic/port***.

```
[edit]
user@host# edit interfaces so-fpc/pic/port
```

2. Configure interface speed in nonconcatenated mode.

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.

```
[edit interfaces so-fpc/pic/port]
user@host# set speed (oc3 | oc12)
```

To configure the PIC to operate in channelized (multiplexed) mode:

1. In configuration mode, go to the **[edit chassis fpc slot-number pic pic-number]** hierarchy level.

```
[edit]
user@host# [edit chassis fpc slot-number pic pic-number]
```

2. Configure the **no-concatenate** option.

```
[edit interfaces so-fpc/pic/port]
user@host# set no-concatenate
```

NOTE: On SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, and Channelized OC3/STM1 (Multi-Rate) Circuit Emulation 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 **no-concatenate** statement, see the *Junos OS Administration Library*.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Interface Speed Overview | 26](#)

[SONET/SDH Interfaces Overview | 2](#)

SONET/SDH Header Byte Values Overview

Header bytes are regenerated in every router in the network path. They help us to identify error conditions.

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 30 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
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

- The following header bytes are supported on the OC192/STM64 MIC with XFP.

F1—Section user channel bytes

K1, K2, S1— Line user channel bytes

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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring SONET/SDH Header Byte Values to Identify Error Conditions | 32](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring SONET/SDH Header Byte Values to Identify Error Conditions

To configure the values in SONET/SDH header bytes:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options
```

2. Configure the **bytes** option to set values in some SONET/SDH header bytes. You can configure this option with **c2 value**, **e1-quiet value**, **f1 value**, **f2 value**, **s1 value**, **z3 value**, and **z4 value**.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set bytes c2 value
user@host# set bytes e1-quiet value
user@host# set bytes f1 value
user@host# set bytes f2 value
user@host# set bytes s1 value
user@host# set bytes z3 value
user@host# set bytes 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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Header Byte Values Overview | 30](#)

Understand the SONET Frame Checksum

Problem

Description: The SONET frame checksum is a calculation that is added to a frame for error control purposes. SONET frame checksum is used in High-Level Data Link Control (HDLC), Frame Relay, and other data-link layer protocols. For example, Router A calculates the frame check sequence (FCS) and adds it to the outgoing message. Router B, on receiving the message recalculates the FCS and compares it to the FCS from Router A. If there is a difference, both sides of the connection might not match in relation to the FCS configuration.

Solution

If you are having problems with a connection, check whether the FCS matches on both sides of the connection. To check the SONET frame checksum, see [“Checking the SONET Frame Checksum” on page 216](#).

After you have checked the FCS and determined that a problem exists, you must configure a SONET frame checksum. For more information, see [“Configuring a SONET Frame Checksum” on page 222](#).

RELATED DOCUMENTATION

[Checklist for Checking the SONET Frame Checksum | 214](#)

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:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options
```

2. Configure the **fcs** option with 32-bit checksum.

```
[edit interfaces interface-name sonet-options]
user@host# set fcs 32
```

To return to default 16-bit frame checksum:

1. In configuration mode, go to the **[edit]** hierarchy level.

```
user@host# edit
```

2. Delete the **fcs** option.

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

To configure 16-bit frame checksum explicitly:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options
```

2. Configure the **fcs** option a 16-bit checksum explicitly.

```
[edit interfaces interface-name sonet-options]
```

```
user@host# set 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.

RELATED DOCUMENTATION

| [Configuring SONET/SDH Physical Interface Properties](#) | 6

Configuring the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs

In Junos OS Release 8.4 and later, the family of next-generation SONET Phase I PICs includes Type 1 and Type 2 PICs. Each PIC type has three varieties.

Type1 PICs include:

- 2-port OC3
- 4-port OC3
- 1-port OC12

Type 2 PICs include:

- 1-port OC48
- 4-port OC3
- 4-port OC12

The PICs are supported on Type 1 and Type 2 FPC interfaces. Hot-pluggable SFPs are used as optical transponders. The PICs provide unprecedented flexibility by allowing the user to configure a variety of modes on them through the configuration of concatenation/nonconcatenation and speed.

The 4-port OC48 PIC with SFP installed, the next-generation SONET/SDH PICs with SFP, and the 4-port OC192 PIC on M Series and T 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.

Port level framing is supported for only the PICs listed below in Table 1. This is expected behavior.

Table 11: PICs supporting port level framing

I2C-ID Name	Model Number	PIC Type
1xCOC12 Q2 PIC	1x CHOC12 IQE SONET	Type 1
4xCOC12 Q2 PIC	4x CHOC12 IQE SONET	Type 2
4xCOC12 Q2 TYPE3 PIC	4x CHOC12 (TYPE3) IQE SONET	Type 3
1x COC48 Q2 PIC	1x CHOC48 IQE SONET	Type 2
1x OC12 Q2 PIC	1x OC12 IQE SONET	Type 1
2xCOC3 Q2 PIC	2x CHOC-3 IQE SONET	Type 1
4xOC3 Q2 PIC	4x OC-3 IQE SONET	Type 1
8OC3OC12 4OC48 MIC	MIC-3D-8OC3OC12-4OC48	-
4OC3OC12 1OC48 MIC	MIC-3D-4OC3OC12-1OC48	-

Table 11: PICs supporting port level framing (*continued*)

I2C-ID Name	Model Number	PIC Type
8CHOC3 4CHOC12 MIC	MIC-3D-8CHOC3-4CHOC12	–
4CHOC3 2CHOC12 MIC	MIC-3D-4CHOC3-2CHOC12	–
1CHOC48 MIC	MIC-3D-1CHOC48 SFP	–
1OC192 HO VCAT MIC	MIC-3D-1OC192-XFP	–
IQECC 4XOC48 TYPE3 PIC	4x OC-48 IQE SONET	Type 3
CE 4xCOC3 SFP PIC	4x CHOC3 SONET CE SFP	–
2XOC12 8XOC3 ATM SFP MIC	2xOC12/8xOC3 CC-CE	–

For information about configuring port speed for concatenate mode on a next-generation PIC, see the *Junos OS Hardware Network Operations Guide*.

By default, SONET/SDH PICs use SONET framing. For a discussion of the differences between the two standards, see the *SONET/SDH Interfaces User Guide for Routing Devices*.

To configure a PIC to use SDH framing, include the **framing** statement at the **[edit chassis fpc slot-number pic pic-number]** hierarchy level, specifying the **sdh** option:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number framing sdh
[edit chassis]
user@host# show
fpc slot-number {
  pic pic-number {
    framing sdh;
  }
}
```

On a TX Matrix or TX Matrix Plus router, include the **framing** statement at the **[edit chassis lcc number fpc slot-number pic pic-number]** hierarchy level, specifying the **sdh** option:

```
[edit chassis lcc number]
user@host# set fpc slot-number pic pic-number framing sdh
[edit chassis lcc number]
user@host# show
```



```
fpc slot-number {
  pic pic-number {
    framing sdh;
  }
}
```

To explicitly configure a PIC to use SONET framing, include the **framing** statement at the **[edit chassis fpc slot-number pic pic-number]** hierarchy level, specifying the **sonet** option:

```
[edit chassis]
user@host# set fpc slot-number pic pic-number framing sonet
[edit chassis]
user@host# show
fpc slot-number {
  pic pic-number {
    framing sonet;
  }
}
```

On a TX Matrix or TX Matrix Plus router, include the **framing** statement at the **[edit chassis lcc number fpc slot-number pic pic-number]** hierarchy level, specifying the **sonet** option:

```
user@host# set fpc slot-number pic pic-number framing sonet
[edit chassis lcc number]
user@host# show
fpc slot-number {
  pic pic-number {
    framing sonet;
  }
}
```

RELATED DOCUMENTATION

[TX Matrix Router and T640 Router Configuration Overview](#)

[TX Matrix Plus Router Configuration Overview](#)

[Configuring the Junos OS to Enable a SONET PIC to Operate in Channelized \(Multiplexed\) Mode](#)

Configuring Junos OS to Enable SONET/SDH Framing for ATM MICs

In Junos OS Release 12.1 and later, the ATM MIC enables support for ATM pseudowire on MX Series routers. ATM MICs are rate-selectable at the following rates: 2-port OC12 or 8-port OC3. The MICs are supported on MPC interfaces. Hot-pluggable SFPs are used as optical transponders. The MICs allow the user to configure both the mode and the speed. The ATM MIC (2-port OC12 and the 8-port OC3) with SFP installed support SONET or SDH framing on a per-port or per-PIC basis. To enable the entire MIC to function in either SONET or SDH mode, you can configure framing at the MIC level. To enable the framing on a port-by-port basis, you can configure framing at the port level.

NOTE: This topic uses the term PIC for ATM MICs and the term FPC for MPC where the reference is to a CLI or Junos OS entity.

By default, ATM MICs use SONET framing. For a discussion of the differences between the two standards, see the *SONET/SDH Interfaces User Guide for Routing Devices*.

To configure the MIC to use SDH framing on a per-PIC basis:

1. At the **[edit chassis]** hierarchy level in configuration mode, specify the PIC and the framing mode to be configured.

```
[edit chassis]
user@host# set fpc fpc-slot pic pic-number framing sdh;
```

For example:

```
[edit chassis]
user@host# set fpc 2 pic 0 framing sdh;
```

2. Verify the configuration.

```
[edit chassis]
user@host# show
fpc 2 {
  pic 0 {
    framing sdh;
  }
}
```

To configure the MIC to use SDH framing on a per-port basis:

1. At the **[edit chassis]** hierarchy level in configuration mode, specify the PIC, port number, and the framing mode to be configured.

```
[edit chassis]
user@host# set fpc fpc-slot pic pic-number port port-number framing sdh;
```

For example:

```
[edit chassis]
user@host# set fpc 2 pic 0 port 0 framing sdh;
```

2. Verify the configuration.

```
[edit chassis]
user@host# show
fpc 2 {
  pic 0 {

    port 0 {
      framing sdh;
    }
  }
}
```

RELATED DOCUMENTATION

| [Configuring Port Speed on Multi-Rate MICs](#)

Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External

IN THIS SECTION

- Configuring SONET/SDH Loopback Capability | 42
- Displaying SONET/SDH Loopback Capability Configuration | 43
- Determining Whether the Problem Is Internal or External with Loopback Capability | 44

Configuring SONET/SDH Loopback Capability

To configure loopback capability on a SONET/SDH interface:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options
```

2. Configure the **loopback** option as local loopback, remote loopback, or payload.

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

```
[edit interfaces interface-name sonet-options]
user@host# set loopback (local | remote | payload)
```

For more information about configuring BERT, see *Configuring Interface Diagnostics Tools to Test the Physical Layer Connections*. For more information about using operational mode commands to test interfaces, see the [CLI Explorer](#).

To turn off the loopback capability:

1. In configuration mode, go to the **[edit]** hierarchy level.

```
user@host# edit
```

2. Remove the **loopback** option to turn off the loopback capability.

```
[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.

Displaying SONET/SDH Loopback Capability Configuration

Purpose

To display the loopback capability configuration in SONET/SDH.

Action

To display loopback capability, for example on the so-1/0/0 interface, perform the following steps:

1. In configuration mode, go to the **[edit interfaces interface-name]** hierarchy level, where the *interface-name* is so-1/0/0.

```
[edit]
user@host# edit interfaces so-1/0/0
```

2. Display the loopback capability by issuing the **show** operational mode command.

```
[edit interfaces so-1/0/0]
user@host# show
```

3. The following output is displayed.

```

no-keepalives;
encapsulation cisco-hdlc;
sonet-options {
    loopback local;
}
unit 0 {
    family inet {
        address 10.100.100.1/24;
    }
}

```

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.

Determining Whether the Problem Is Internal or External with Loopback Capability

Problem

Description: Problem is internal or external.

Solution

To determine whether a problem is internal or external, you have to loop packets on both the local and the remote router using the loopback capability.

To loop packets on both the local and the remote router, perform the following steps:

1. In configuration mode, go to the **[edit interfaces *interface-name*]** hierarchy level.

```

[edit]
user@host# edit interfaces interface-name sonet-options]

```

2. Configure the **no-keepalives** and **encapsulation cisco-hdlc** options.

```

[edit interfaces interface-name]
user@host# set no-keepalives
user@host# set encapsulation cisco-hdlc

```

3. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level.

```

[edit]
user@host# edit interfaces interface-name sonet-options]

```

4. Configure the **loopback local** option. This option causes the interface to loop within the PIC just before the data reaches the transceiver.

```
[edit interfaces interface-name sonet-options]  
user@host# set loopback local
```

You can also 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** operational mode command.

RELATED DOCUMENTATION

| [Configuring SONET/SDH Physical Interface Properties | 6](#)

SONET/SDH Path Trace Identifier Overview

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 than 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.

RELATED DOCUMENTATION

| [Configuring SONET/SDH Physical Interface Properties | 6](#)

| [Configuring the SONET/SDH Path Trace Identifier for a Circuit | 46](#)

Configuring the SONET/SDH Path Trace Identifier for a Circuit

To configure path trace identifier:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level.

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

2. Configure path trace identifier.

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

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set path-trace trace-string
```

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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Path Trace Identifier Overview | 45](#)

SONET/SDH HDLC Payload Scrambling Overview

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 to Reduce Network Congestion” on page 57](#).

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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring SONET/SDH HDLC Payload Scrambling for Link Stability | 47](#)

Configuring SONET/SDH HDLC Payload Scrambling for Link Stability

To explicitly enable payload scrambling, perform the following steps:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the *interface-name* is **so-fpc/pic/port**.

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

2. Configure the **payload-scrambler** option to enable HDLC payload scrambling.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set payload-scrambler
```

To disable HDLC payload scrambling:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the *interface-name* is **so-fpc/pic/port**.

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

2. Configure the **no-payload-scrambler** option to disable HDLC payload scrambling.

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

To re-enable payload scrambling and to return to the default setting.

1. In configuration mode, go to the **[edit]** hierarchy level.

```
user@host# edit
```

2. To return to the default setting, delete the **no-payload-scrambler** statement from the configuration.

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

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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)
[SONET/SDH HDLC Payload Scrambling Overview | 46](#)

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.

To configure the loop timing:

1. In configuration mode, go to the **[edit interfaces interface-name]** hierarchy level.

```
[edit ]
user@host# [edit interfaces interface-name]
```

2. Include the **clocking external** statement.

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

To explicitly configure line timing on an interface:

1. In configuration mode, go to the **[edit interfaces *interface-name*]** hierarchy level.

```
[edit ]  
user@host# [edit interfaces interface-name]
```

2. Include the **clocking internal** statement.

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

NOTE: On Channelized SONET/SDH PICs, if you set the parent (or the master) controller clock to **external**, then you must set the child controller clocks to the default value—that is, **internal**.

For example, on the Channelized STM1 PIC, if the clock on the Channelized STM1 interface (which is the master controller) is set to **external**, then you must not configure the CE1 interface (which is the child controller) clock to **external**. Instead you must configure the CE1 interface clock to **internal**.

RELATED DOCUMENTATION

Clock Sources on Channelized Interfaces

[clocking](#) | **241**

Configuring Channelized IQ and IQE SONET/SDH Loop Timing

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.

To configure SONET/SDH or DS3-level clocking:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level or to the **[edit interfaces *ct3-fpc/pic/port* t3-options]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options
```

```
[edit]
user@host# edit interfaces ct3-fpc/pic/port t3-options
```

2. Configure SONET/SDH or DS3-level clocking. By default, internal clocking (line timing) is used on channelized IQ and IQE interfaces.

```
[edit interfaces interface-name sonet-options]
user@host# set loop-timing
```

```
[edit interfaces ct3-fpc/pic/port t3-options]
user@host# set loop-timing
```

To configure the default line timing explicitly:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level or to the **[edit interfaces *ct3-fpc/pic/port* t3-options]**.

```
[edit]
user@host# edit interfaces interface-name sonet-options
```

```
[edit]
user@host# edit interfaces ct3-fpc/pic/port t3-options
```

2. Configure the default line timing explicitly.

```
[edit interfaces interface-name sonet-options]
user@host# set no-loop-timing
```

```
[edit interfaces ct3-fpc/pic/port t3-options]
user@host# set no-loop-timing
```

To configure clocking for all channelized IQ and IQE PICs which is supported on all channels.

1. In configuration mode, go to the **[edit interfaces *type-fpc/pic/port*]** hierarchy level.

```
[edit]
user@host# edit interfaces type-fpc/pic/port
```

2. Configure the **clocking** option. If you do not include the **clocking** statement, the individual interfaces use internal clocking by default.

```
[edit interfaces type-fpc/pic/port]
user@host# set clocking
```

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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)
[loop-timing | 276](#)

Damping Shorter Physical Interface Transitions

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 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 passed, called the *hold-time*. When you have damped interface transitions and the interface goes from up to down, the down hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still *down*, then the router begins to advertise the interface as being down. Similarly, when an interface goes from down to up, the up hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still *up*, then the router begins to advertise the interface as being up. For information about physical interface damping, see *Physical Interface Damping Overview*.

This task applies to damping shorter physical interface transitions in milliseconds. To damp longer physical interface transitions in seconds, see *Damping Longer Physical Interface Transitions*.

To configure damping of shorter physical interface transitions:

1. Select the interface to damp, where the interface name is ***interface-type-fpc/pic/port***:

```
[edit]
user@host# edit interfaces interface-name
```

2. Configure the hold-time for link up and link down.

```
[edit interfaces interface-name]
user@host# set hold-time up milliseconds down milliseconds
```

The hold 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. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

For most Ethernet interfaces, hold timers are implemented using a one-second polling algorithm. For 1-port, 2-port, and 4-port Gigabit Ethernet interfaces with small form-factor pluggable transceivers (SFPs), hold timers are interrupt-driven.

NOTE: The **hold-time** option is not available for controller interfaces.

RELATED DOCUMENTATION

[SONET/SDH Defect Hold Times for Damping Interface Transitions Overview | 70](#)

[Configuring SONET/SDH Defect Triggers | 72](#)

[hold-time | 268](#)

Configuring SONET Options for 10-Gigabit Ethernet Interfaces

The 10-Gigabit Ethernet IQ2 and IQ2-E PICs are supported on the M120, M320, and T Series routers. The 10-Gigabit Ethernet LAN/WAN PICs are supported on the T4000 routers. These PICs provides external interfaces 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. When WAN PHY mode is configured on an interface, the following SONET options are supported:

- Loopback (local and remote)
- Path trace
- Trigger options

To configure SONET options for 10-Gigabit Ethernet Interfaces:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the *interface-name* is ***so-fpc/pic/port***.

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

2. Configure a loopback connection.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set loopback (local | payload | remote)
```

3. Configure a path trace identifier, which is a text string that identifies the circuit.

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

```
user@host# set path-trace trace-string
```

4. Configure SONET/SDH defect triggers as either ignore or hold time.

The defect triggers can be ignored. By default all SONET/SDH defect triggers are honored if you do not include the **trigger defect ignore** statement.

You can apply up and down hold times to SONET/SDH defect trigger. When a defect is detected the interface is marked down immediately and when the defect becomes absent the interface is marked up immediately if you do not include the **trigger defect hold-time** statement.

```
[edit interfaces so-fpc/pic/port sonet-options]
user@host# set trigger defect ignore
user@host# set trigger defect hold-time up milliseconds down milliseconds
```

5. Configure the **mpls** option to process incoming IP packets that have MPLS labels for passive monitoring on ATM and SONET/SDH interfaces and 10-Gigabit Ethernet interfaces in WAN PHY mode.

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

6. Configure the **pop-all-labels** option to remove up to two MPLS labels from incoming IP packets in passive monitoring.

```
[edit interfaces so-fpc/pic/port sonet-options mpls]
user@host# set pop-all-labels
```

7. Configure the **required-depth** option as either **1** or **2** in the **pop-all-labels** statement. to 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.

```
[edit interfaces so-fpc/pic/port sonet-options mpls pop-all-labels]
user@host# set required-depth
```

For information about using the **mpls** statement, see [“Enabling Packet Flow Monitoring on SONET/SDH Interfaces” on page 132](#).

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)
[SONET/SDH Interfaces Overview | 2](#)

Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode

In the 4-port OC192 PIC with OC768-over-OC192 mode, four OC192 links are aggregated into one OC768 link with one logical interface. This single interface achieves data rates of approximately 40 Gbps. OC768 optics are expensive, and most long-distance networks currently use fiber optics and regenerators that cannot carry OC768 SONET. When you create an OC768 pipe as a large data pipe running over existing infrastructures, you transfer network traffic without link bonding or load sharing over parallel links. Load sharing is automatically accomplished in the Junos OS using a proprietary method, and does not need to be manually configured.

The following limitations apply to OC768-over-OC192 mode:

- The maximum difference in delay between all links in the bundle is 8 μ (microseconds), equivalent to approximately 1.5 km maximum difference in length between the longest and shortest fiber pairs.
- If a single link in the bundle fails, the whole bundle fails. If link redundancy is required, implement an aggregated SONET/SDH bundle instead.
- Only routers that contain 4-port OC192 PICs can operate in OC768-over-OC192 mode.

To configure the 4-port OC192 PIC to operate in OC768-over-OC192 mode:

1. In the configuration mode go to the **[edit chassis]** hierarchy level.

```
[edit]
user@host# edit chassis
```

2. Configure the aggregate-ports.

- On standalone T640, T1600, and T4000 routers, include the **aggregate-ports** statement at the **[edit chassis fpc slot-number pic pic-number]** hierarchy level.

```
[edit chassis]
user@host# edit fpc slot-number pic pic-number
user@host# set aggregate-ports
```

- On TX Matrix and TX Matrix Plus router, configure the **aggregate-ports** statement at the **[edit chassis lcc lcc-number fpc slot-number pic pic-number]** hierarchy level.

```
[edit chassis]
user@host# edit lcc lcc-number fpc slot-number pic pic-number
user@host# set aggregate-ports
```

3. To verify the configuration, execute the **show interfaces so-fpc/pic/port extensive** operational command. When this command is used for the 4-port OC192 PIC configured for OC768-over-OC192 mode, only port 0 (**so-fpc/pic/0**) is displayed. This port is displayed as **OC768**.

NOTE: When you configure the 4-port OC192 PIC for OC768-over-OC192 mode, only port 0 (the first port) needs be configured as the OC768 port.

RELATED DOCUMENTATION

[aggregate-ports](#) | 231

Receive and Transmit Leaky Bucket Properties Overview

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 *Routing Policies, Firewall Filters, and Traffic Policers User 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 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 for Link Stability” on page 47](#).

RELATED DOCUMENTATION

[Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion | 57](#)

[SONET/SDH Interfaces Overview | 2](#)

[receive-bucket | 300](#)

[transmit-bucket | 314](#)

Configuring Receive and Transmit Leaky Bucket Properties to Reduce Network Congestion

You can configure leaky bucket properties which allow you to limit the amount of traffic received on and transmitted by a particular interface. You can 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.

To configure leaky bucket properties:

1. In configuration mode, go to the **[edit interfaces *interface-name*]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name
```

2. Configure the **receive-bucket** statement.

```
[edit interfaces interface-name]  
user@host# set receive-bucket
```

3. Configure the **overflow** option, the **threshold** option, and the **rate** option for the receive leaky bucket, which specifies what percentage of the interface's total capacity can be used to receive packets.

```
[edit interfaces interface-name receive-bucket]  
user@host# set overflow (discard | tag)  
user@host# set threshold bytes  
user@host# set rate percentage
```

4. Configure the **transmit-bucket** statement.

```
[edit interfaces interface-name]  
user@host# set transmit-bucket
```

5. Configure the **overflow** option, the **threshold** option, and the **rate** option for the transmit leaky bucket, which specifies what percentage of the interface's total capacity can be used to transmit packets.

```
[edit interfaces interface-name transmit-bucket]  
user@host# set overflow (discard | tag)  
user@host# set threshold bytes  
user@host# set rate percentage
```

RELATED DOCUMENTATION

[Receive and Transmit Leaky Bucket Properties Overview | 56](#)

[SONET/SDH Interfaces Overview | 2](#)

[receive-bucket | 300](#)

[transmit-bucket | 314](#)

Configuring Interface Encapsulation on SONET/SDH Interfaces

IN THIS CHAPTER

- Understanding Interface Encapsulation on SONET/SDH Interfaces | 59
- Configuring Interface Encapsulation on SONET/SDH Interfaces | 62
- PPP Support on SONET/SDH Interfaces | 65
- Configuring PPP Support on SONET/SDH Interfaces | 66

Understanding 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. Note that 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.

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.

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.

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

Understanding Encapsulation on a Physical SONET/SDH Interface

IN THIS SECTION

- [Point-to-Point Protocol \(PPP\) | 60](#)
- [Cisco HDLC | 60](#)
- [Frame Relay | 60](#)
- [Frame Relay Ether Type | 61](#)

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

Physical interfaces can use Frame Relay ether type (**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.

Understanding 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 configure an encapsulation on a logical SONET/SDH interface, see [“Configuring Interface Encapsulation on SONET/SDH Interfaces” on page 62](#).

NOTE:

- 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.

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.

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

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

RELATED DOCUMENTATION

| [Configuring Interface Encapsulation on SONET/SDH Interfaces](#) | 62

Configuring Interface Encapsulation on SONET/SDH Interfaces

IN THIS SECTION

- [Configuring the Encapsulation on a Physical SONET/SDH Interface](#) | 62
- [Displaying the Encapsulation on a Physical SONET/SDH Interface](#) | 63
- [Configuring the Frame Relay Encapsulation on a Logical SONET/SDH Interface](#) | 64
- [Configuring the Point-to-Point Protocol Encapsulation on a Physical SONET/SDH Interface](#) | 65

You can configure encapsulation on a physical SONET/SDH interface and on a logical SONET/SDH interface. 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 tasks explain configuring encapsulation on a physical SONET/SDH interface, configuring frame relay encapsulation on a logical SONET/SDH interface, and configuring Point-to-Point Protocol encapsulation to get a SONET/SDH OC3 or OC12 interface up and running:

Configuring the Encapsulation on a Physical SONET/SDH Interface

To configure encapsulation on a physical SONET/SDH interface:

1. In configuration mode, go to the **[edit interfaces so-fpc/pic/port]** hierarchy level.

```
[edit]
user@host# edit interfaces so-fpc/pic/port
```

2. Configure the encapsulation as **cisco-hdlc**, **cisco-hdlc-ccc**, **cisco-hdlc-tcc**, **frame-relay**, **frame-relay-ccc**, **frame-relay-tcc**, **frame-relay-ether-type**, **frame-relay-ether-type-tcc**, **extended-frame-relay-ether-type-tcc**, **ppp**, **ppp-ccc**, or as **ppp-tcc**.

```
[edit interfaces mo-fpc/pic/port]
```



```
user@host# set encapsulation encapsulation-type
```

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.

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.

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

Displaying the Encapsulation on a Physical SONET/SDH Interface

Purpose

To display the configured encapsulation and its associated set options on a physical SONET/SDH interface when the following are set at the **[edit interfaces *interface-name*]** hierarchy level:

- interface-name—so-7/0/0
- Encapsulation—**ppp**
- Unit—0
- Family—**inet**
- Address—192.168.1.113/32
- Destination—192.168.1.114
- Family—**iso** and **mpls**

Action

Run the **show** command at the **[edit interfaces *interface-name*]** hierarchy level.

```
[edit interfaces so-7/0/0]
user@host# show
encapsulation ppp;
unit 0 {
  point-to-point;
```

```

family inet {
    address 192.168.1.113/32 {
        destination 192.168.1.114;
    }
}
family iso;
family mpls;
}

```

Meaning

The configured encapsulation and its associated set options are displayed as expected. Note that the second set of two **family** statements allow IS-IS and MPLS to run on the interface.

Configuring the Frame Relay 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 configure Frame Relay encapsulation on a logical SONET/SDH interface:

1. In configuration mode, go to the **[edit interfaces *so-fpc/pic/port unit logical-unit-number*]** hierarchy level.

```

[edit]
user@host# edit interfaces so-fpc/pic/port unit logical-unit-number

```

2. Configure the encapsulation as **frame-relay-ccc**, **frame-relay-tcc**, **frame-relay-ether-type**, or as **frame-relay-ether-type-tcc**.

```

[edit interfaces so-fpc/pic/port unit logical-unit-number]
user@host# set encapsulation encapsulation-type

```

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

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

Configuring the Point-to-Point Protocol Encapsulation on a Physical SONET/SDH Interface

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:

To configure PPP encapsulation on a physical SONET/SDH interface:

1. In configuration mode, go to the **[edit interfaces so-fpc/pic/port]** hierarchy level.

```
[edit]
user@host# edit interfaces so-fpc/pic/port
```

2. Configure the encapsulation as **ppp**.

```
[edit interfaces so-fpc/pic/port]
user@host# set encapsulation ppp
```

3. Configure local IP address and remote IP address with family inet.

```
[edit interfaces so-fpc/pic/port]
user@host# set unit 0 family inet address local-address destination remote-address
```

RELATED DOCUMENTATION

[Understanding Interface Encapsulation on SONET/SDH Interfaces](#) | 59

PPP Support on SONET/SDH Interfaces

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 12 on page 66](#) shows the older (RFC 1619) and newer (RFC 2615) values, together with the Juniper Networks default values.

Table 12: 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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring PPP Support on SONET/SDH Interfaces | 66](#)

[Understanding Interface Encapsulation on SONET/SDH Interfaces | 59](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring PPP Support on SONET/SDH Interfaces

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.

To enable support for the RFC 2615 features:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options
```

2. Configure the **rfc-2615** option.

```
[edit interfaces interface-name sonet-options]
user@host# set rfc-2615
```

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[PPP Support on SONET/SDH Interfaces | 65](#)

[Configuring Interface Encapsulation on SONET/SDH Interfaces | 62](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring How SONET/SDH Interface Defects Are Handled

IN THIS CHAPTER

- SONET/SDH Defect Triggers Overview | 68
- SONET/SDH Defect Hold Times for Damping Interface Transitions Overview | 70
- Configuring SONET/SDH Defect Triggers | 72

SONET/SDH Defect Triggers Overview

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 13 on page 68 lists the defects you can configure.

Table 13: SONET/SDH and ATM Active Alarms and Defects

Alarm	Description
Physical	
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

Table 13: SONET/SDH and ATM Active Alarms and Defects (*continued*)

Alarm	Description
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 (signal) label mismatch
rfi-p	Remote failure indication—path
uneq-p	Path unequipped

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.

You can prevent a loss of signal (LOS) from bringing down an interface. An LOS can lead to the following defects:

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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring SONET/SDH Defect Triggers | 72](#)

[SONET/SDH Interfaces Overview | 2](#)

SONET/SDH Defect Hold Times for Damping Interface Transitions

Overview

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 a hold-down timer is configured and the interface goes from up to down, the down hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still *down*, then the router begins to advertise the interface as being down. Similarly, when a hold-up timer is configured and an interface goes from down to up, the up hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still *up*, then the router begins to advertise the interface as being up.

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 Shorter Physical Interface Transitions” on page 52](#).
- 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

BEST PRACTICE:

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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring SONET/SDH Defect Triggers | 72](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring SONET/SDH Defect Triggers

IN THIS SECTION

- [Configuring SONET/SDH Defect Triggers to Be Ignored | 72](#)
- [Configuring SONET/SDH Defect Hold Times | 72](#)
- [Displaying the Configuration Where the SONET/SDH Defects to be Ignored are Listed | 73](#)

You can configure SONET/SDH defect triggers as either ignore or hold time. The following topics explain defect triggers in detail.

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.

To configure defects to be ignored:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options trigger]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options trigger
```

2. Configure the **defect ignore** option to turn off the loopback capability.

```
[edit interfaces interface-name sonet-options trigger]
user@host# set defect ignore
```

Configuring SONET/SDH Defect Hold Times

To configure hold timers:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options trigger]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options trigger
```

2. Configure the **hold-time** statement with **up** and **down** options in milliseconds ranging from 1 through 65,534 milliseconds.

```
[edit interfaces interface-name sonet-options trigger]
user@host# set defect hold-time up milliseconds down milliseconds
```

Displaying the Configuration Where the SONET/SDH Defects to be Ignored are Listed

Purpose

To display the configuration where the SONET/SDH defects to be ignored are listed.

Action

To display the defects in an interface, for example on so-1/0/0 interface, perform the following steps:

1. In configuration mode, go to the **[edit interfaces so-1/0/0 sonet-options trigger]** hierarchy level.

```
[edit]
user@host# edit interfaces so-1/0/0 sonet-options trigger
```

2. Issue the **show defect** operational mode command.

```
[edit interfaces so-1/0/0 sonet-options trigger]
user@host# show defect
```

The following output is displayed:

```
ais-l ignore;
lof ignore;
los ignore;
pll ignore;
rfi-l ignore;
rfi-p ignore;
```

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Defect Hold Times for Damping Interface Transitions Overview | 70](#)

[SONET/SDH Defect Triggers Overview | 68](#)

Configuring APS and MSP to Protect from Circuit Failures

IN THIS CHAPTER

- Automatic Protection Switching and Multiplex Section Protection Overview | 76
- Configuring Automatic Protect Switching | 77
- Basic Automatic Protect Switching Overview | 81
- Configuring Basic Automatic Protect Switching | 82
- Example: Configuring Basic APS Support on Routers | 83
- Configuring Lockout of Protection for SDH Interfaces | 88
- APS Timers Overview | 89
- Configuring APS Timers | 90
- Container Interfaces for APS on SONET Links Overview | 91
- Configuring Container Interfaces for APS on SONET Links | 92
- APS Using a Container Interface with ATM Encapsulation Overview | 97
- Configuring APS Using a Container Interface with ATM Encapsulation | 97
- Displaying APS Using a Container Interface with ATM Encapsulation | 98
- APS Load Sharing Between Circuit Pairs Overview | 101
- Configuring APS Load Sharing | 102
- Example: Configuring APS Load Sharing Between Circuit Pairs | 103
- Link PIC Redundancy Overview | 107
- Configuring Link PIC Redundancy | 108
- Switching Between the Working and Protect Circuits Overview | 110
- Configuring Switching Between the Working and Protect Circuits | 111
- Revertive Mode Overview | 113
- Configuring Revertive Mode | 113
- Switching Mode Overview | 115
- Configuring Switching Mode | 116

Automatic Protection Switching and Multiplex Section Protection Overview

Automatic Protection Switching (APS) is used by SONET add/drop multiplexers (ADM) 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.

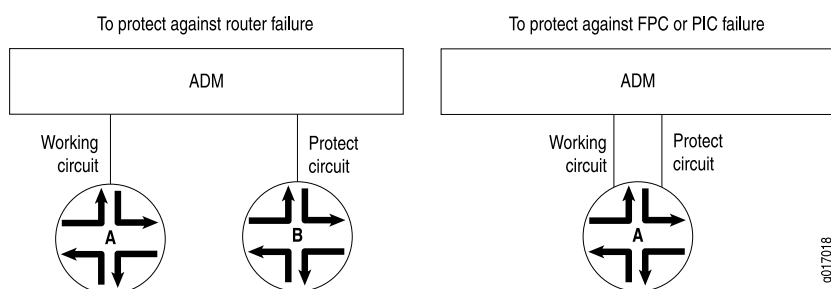
The Junos OS supports APS 1+1 switching, either revertive or nonrevertive mode, and bidirectional mode only (although you can configure interoperation with line-terminating equipment [LTE] provisioned for unidirectional mode). The Junos OS does not transmit identical data on the working and protect circuits, 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 76](#). 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



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 Library for Routing Devices*.

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
- **fast-aps-switch** *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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring Basic Automatic Protect Switching | 82](#)

[Basic Automatic Protect Switching Overview | 81](#)

[Example: Configuring Basic APS Support on Routers | 83](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring Automatic Protect Switching

To configure basic Automatic Protection Switching (APS) options:

1. In configuration mode, go to the [edit interfaces *so-fpc/pic/port* sonet-options aps] hierarchy level.

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

2. Configure the 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. You can set the APS interval from 1 through 65,534 milliseconds. By default, 1000 milliseconds is set.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set advertise-interval milliseconds
```

3. Configure the **annex-b** option for Multiplex Section Protection (MSP) switching on SDH interfaces for M320 and M120 routers only.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set annex-b
```

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

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set authentication-key key
```

5. Configure the **fast-aps-switch** option to reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits in M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set fast-aps-switch
```

6. Configure the **force** option to either protect mode or working mode to 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.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set force (protect | working)
```


7. Configure the **hold-time** value in milliseconds to determine whether a neighbor APS router is operational where the hold-time value ranges from 1 through 65,354 milliseconds. By default, 3000 milliseconds (3 times the advertisement interval) is set as hold time value.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set hold-time milliseconds
```

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

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set lockout
```

9. Configure the address of the remote interface when you are configuring one router to be the working router and a second to be the protect router. You can configure this on one or both of the interfaces.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set neighbor address
```

10. Configure load sharing between two working protect circuit pairs where circuit's group name is as configured with the **protect-circuit** or **working-circuit** statement.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set paired-group group-name
```

11. 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.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set protect-circuit group-name
```

12. Configure the **request** option as protect circuit or working circuit to perform a manual switch between the protect and working circuits. This statement is honored only if there are no higher-priority reasons to switch.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set request (protect | working)
```

13. Configure APS revertive mode in seconds ranging from 1 through 65,535 seconds which denotes the time to wait after the working circuit has again become functional before making the working circuit active again. By default, APS operates in nonrevertive mode.

```
[edit interfaces so-fpc/pic/port sonet-options aps]  
user@host# set revert-time seconds
```

14. Configure the interface in bidirectional mode or in unidirectional mode. By 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.

```
[edit interfaces so-fpc/pic/port sonet-options aps]  
user@host# set switching-mode (bidirectional | unidirectional)
```

15. Configure the working router in an APS circuit pair.

```
[edit interfaces so-fpc/pic/port sonet-options aps]  
user@host# set working-circuit group-name
```

RELATED DOCUMENTATION

[Automatic Protection Switching and Multiplex Section Protection Overview | 76](#)

[Basic Automatic Protect Switching Overview | 81](#)

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Example: Configuring Basic APS Support on Routers | 83](#)

Basic Automatic Protect Switching Overview

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.

RELATED DOCUMENTATION

[Automatic Protection Switching and Multiplex Section Protection Overview | 76](#)

[Configuring Basic Automatic Protect Switching | 82](#)

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Example: Configuring Basic APS Support on Routers | 83](#)

Configuring Basic Automatic Protect Switching

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.

To configure basic Automatic Protection Switching (APS) options on the working circuit:

1. In configuration mode, go to the **[edit interfaces so-fpc/pic/port sonet-options aps]** hierarchy level.

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

2. Configure the group name of the working circuit.

```
[edit]
user@host# set working-circuit group-name
```

3. Configure the authentication key.

```
[edit]
user@host# set authentication-key key
```

4. Configure the IP address in the **neighbor** statement. Note that this option is set only if the protect circuit is on a different router

```
[edit]
user@host# set neighbor address
```

To configure basic Automatic Protection Switching (APS) options on the protect circuit:

1. In configuration mode, go to the **[edit interfaces so-fpc/pic/port sonet-options aps]** hierarchy level.

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

2. Configure the group name of the protect circuit.

```
[edit]  
user@host# set protect-circuit group-name
```

3. Configure the authentication key.

```
[edit]  
user@host# set authentication-key key
```

4. Configure the IP address in the **neighbor** statement. Note that this option is set only if the working circuit is on a different router

```
[edit]  
user@host# set neighbor address
```

RELATED DOCUMENTATION

[Automatic Protection Switching and Multiplex Section Protection Overview | 76](#)

[Basic Automatic Protect Switching Overview | 81](#)

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Example: Configuring Basic APS Support on Routers | 83](#)

[SONET/SDH Interfaces Overview | 2](#)

Example: Configuring Basic APS Support on Routers

IN THIS SECTION

- [Requirements for a Basic APS Support | 84](#)
- [Basic APS Overview | 84](#)
- [Configuring Basic APS Support on Routers | 85](#)

Requirements for a Basic APS Support

This example uses the following hardware and software components:

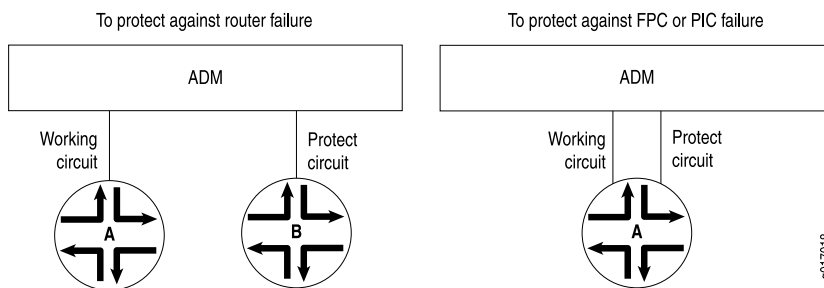
- Two MX Series, M Series, or T Series routers.
- Junos OS Release 7.4 or later

Basic APS Overview

Automatic Protection Switching (APS) is used by SONET add/drop multiplexers (ADM)s 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.

To configure APS or MSP, you configure a working and a protect circuit, as shown in [Figure 2 on page 84](#). 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 2: APS/MSP Configuration Topologies



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.

Configuring Basic APS Support on Routers

IN THIS SECTION

- On Router A (the Working Router) | 85
- On Router B (the Protect Circuit) | 85
- On a Single Platform, One Interface as the Working Circuit and Another Interface as the Protect Circuit | 86
- Results | 87

To configure Router A to be the working router and Router B to be the protect router as shown in [Figure 2 on page 84](#).

On Router A (the Working Router)

Step-by-Step Procedure

Configure basic APS support on Router A as the working router.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the interface is so-6/1/1.

```
[edit]
user@host# edit interfaces so-6/1/1 sonet-options
```

2. Configure the **working-circuit** option as **San-Jose**

```
[edit interfaces so-6/1/1 sonet-options]
user@host# set working-circuit San-Jose
```

3. Configure the **authentication-key** option as “**\$ABC123**”

```
[edit]
user@host# set authentication-key “ $ABC123”
```

On Router B (the Protect Circuit)

Step-by-Step Procedure

Configure basic APS support on Router B as the protect router.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the interface is so-0/0/0.

```
[edit]
user@host# edit interfaces so-0/0/0 sonet-options
```

2. Configure the **protect-circuit** option as **San-Jose**

```
[edit edit interfaces so-0/0/0 sonet-options]
user@host# set protect-circuit San-Jose
```

3. Configure the **authentication-key** option as “**\$9\$B2612345**”

```
[edit edit interfaces so-0/0/0 sonet-options]
user@host# set authentication-key “$9$B2612345”
```

4. Configure the **neighbor** option as **192.168.1.2** that is the address of Router A on the link between A and B.

```
[edit edit interfaces so-0/0/0 sonet-options]
user@host# set neighbor 192.168.1.2
```

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

Step-by-Step Procedure

Configure one interface as the working circuit.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the interface is so-2/1/1 .

```
[edit]
user@host# edit interfaces so-2/1/1 sonet-options
```

2. Configure the **working-circuit** option as **Bayward**

```
[edit edit interfaces so-2/1/1 sonet-options]
user@host# set protect-circuit Bayward
```


3. Configure the **authentication-key** option as **blarney**

```
[edit edit interfaces so-2/1/1 sonet-options]
user@host# set authentication-key blarney
```

Step-by-Step Procedure

Configure one interface as the protect circuit.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level, where the interface is so-3/0/2.

```
[edit]
user@host# edit interfaces o-3/0/2 sonet-options
```

2. Configure the **working-circuit** option as **Bayward**

```
[edit edit interfaces so-3/0/2 sonet-options]
user@host# set protect-circuit Bayward
```

3. Configure the **authentication-key** option as **blarney**

```
[edit edit interfaces so-3/0/2 sonet-options]
user@host# set authentication-key blarney
```

Results

Display the results of the configuration.

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;
}
```

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;
}
```

RELATED DOCUMENTATION

[Automatic Protection Switching and Multiplex Section Protection Overview | 76](#)

[Basic Automatic Protect Switching Overview | 81](#)

[Configuring Basic Automatic Protect Switching | 82](#)

[Configuring SONET/SDH Physical Interface Properties | 6](#)

Configuring Lockout of Protection for SDH Interfaces

To configure Annex B lockout, perform the following steps:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level, where the *interface-name* is ***so-fpc/pic/port***.

```
[edit]
```

```
user@host# edit interfaces so-fpc/pic/port sonet-options aps
```

2. Configure the **annex-b** option.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# edit annex-b
```

3. Configure the **lockout** option to provide a lockout of protection, forcing the use of the working circuit and locking out the protect circuit regardless of anything else.

```
[edit interfaces so-fpc/pic/port sonet-options aps annex-b]
user@host# set lockout
```

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Switching Between the Working and Protect Circuits Overview | 110](#)

[Configuring Switching Between the Working and Protect Circuits | 111](#)

[SONET/SDH Interfaces Overview | 2](#)

APS Timers Overview

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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring APS Timers | 90](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring APS Timers

To configure advertise interval and hold time:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options aps
```

2. Configure the **advertise-interval** option in milliseconds to modify the advertisement interval.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set advertise-interval milliseconds
```

3. Configure the **hold-time** option in milliseconds to modify hold time..

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set hold-time milliseconds
```

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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[APS Timers Overview | 89](#)

[SONET/SDH Interfaces Overview | 2](#)

Container Interfaces for APS on SONET Links Overview

The Junos OS supports container interfaces for APS on SONET links. 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 *Understanding Container Interfaces* 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.

To configure each container interface, you must assign two SONET interfaces (**so-fpc/pic/port**) using the **container-list cin** 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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring Container Interfaces for APS on SONET Links | 92](#)

Configuring Container Interfaces for APS on SONET Links

IN THIS SECTION

- [Configuring Container Interfaces on SONET Links | 92](#)
- [Displaying Container Interface Configuration | 94](#)
- [Displaying the APS Container Interface Configuration | 96](#)

Configuring Container Interfaces on SONET Links

To configure a container interface on SONET links, you should perform the following:

- 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.
- Configure each container interface, here, you must assign two SONET interfaces (**so-fpc/pic/port**) using the **container-list cin** 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 procedure explains configuring a container interface on SONET links in detail.

To configure a container interface on SONET links:

1. In configuration mode, go to the **edit chassis container-devices** hierarchy level.

```
[edit]
user@host# edit chassis container-devices
```

2. Specify the total number of container interfaces (up to 128) to create using the **device-count number** statement.

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

NOTE: 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 **cin**.

3. Configure the container interface parameters for a specified container **cin** as follows:

- a. Specify the container interface using the numbered identifier **cin**.

```
[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 cin]
user@host# set container-options container-type aps
```

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

```
[edit interfaces cin]
user@host# set 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 **cin**.

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

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

For example, set the so-0/0/0 interface as the primary circuit and the so-0/0/1 interface as the standby circuit for the container interface **cin** :

```
[edit]
user@host# edit interfaces so-0/0/0 # Enter configuration mode for interface so-0/0/0
[edit interfaces so-0/0/0]
user@host# set container-options container-list cin 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 configuration mode for interface so-0/0/1
[edit interfaces so-0/0/1]
user@host# set container-options container-list cin 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 cin standby allow-configuration-override
```

Displaying Container Interface Configuration

Purpose

To display a container interface.

Action

To display a container interface configuration in SONET/SDH where the **device-count** is **1** with the so-0/0/0 interface as primary and the so-0/0/1 interface as secondary, and the encapsulation is set to **cisco-hdlc**.

1. In configuration mode, go to the **[edit chassis]** hierarchy level.

```
[edit]
user@host# edit chassis
```

2. Issue the **show** command in configuration mode.


```
[edit chassis]
user@host# show
```

3. The following output is displayed.

```
container-devices {
    device-count 1;
}
```

4. In configuration mode, go to the **[edit interfaces]** hierarchy level.

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

5. Issue the **show** command in configuration mode.

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

6. The following output is displayed.

```
so-0/0/0 {
    container-options {
        container-list ci0;
        primary;
    }
}
so-0/0/1 {
    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;
    }
}
}

```

Displaying the APS Container Interface Configuration

Purpose

Display the APS container interface configuration parameters.

Action

You can run the **show aps** operational mode command to display the APS container interface configuration.

```
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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Container Interfaces for APS on SONET Links Overview | 91](#)

APS Using a Container Interface with ATM Encapsulation Overview

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 *Understanding Container Interfaces*.

Container ATM APS does not support interchassis APS.

MLPPP over ATM CI is not supported.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Displaying APS Using a Container Interface with ATM Encapsulation | 98](#)

[Configuring APS Using a Container Interface with ATM Encapsulation | 97](#)

Configuring APS Using a Container Interface with ATM Encapsulation

To configure APS using a container interface with ATM encapsulation by specifying the ATM children within a container interface:

1. In configuration mode, go to the **[edit interface at-*fpc/pic/slot* container-options]** hierarchy level.

```
[edit]
user@host# edit interfaces at-fpc/pic/slot container-options
```

2. Configure the **container-list cin** statement.

```
[edit interfaces at-fpc/pic/slot container-options]
user@host# set container-list cin
```

3. Configure primary or standby option as needed.

```
[edit interfaces at-fpc/pic/slot container-options]
```

```
user@host# set (primary | standby)
```

To configure a container interface by including its children:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level.

```
[edit]
user@host# edit interface at-fpc/pic/slot container-options
```

2. Configure the **cin** statement where **n** is the number of children.

```
[edit interface at-fpc/pic/slot container-options]
user@host# set container-list cin
```

Container ATM APS does not support interchassis APS.

MLPPP over ATM CI is not supported.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[APS Using a Container Interface with ATM Encapsulation Overview | 97](#)

[SONET/SDH Interfaces Overview | 2](#)

[Displaying APS Using a Container Interface with ATM Encapsulation | 98](#)

Displaying APS Using a Container Interface with ATM Encapsulation

IN THIS SECTION

- [Displaying APS Using a Container Interface with ATM Encapsulation | 99](#)
- [Displaying the APS Container Interface Configuration | 100](#)

Displaying APS Using a Container Interface with ATM Encapsulation

Purpose

Display APS using a container interface with ATM encapsulation.

Action

To display APS using a container interface with ATM encapsulation **atm-pvc** where 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**), perform the following steps:

1. In configuration mode, go to the **[edit interfaces]** hierarchy level.

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

2. Issue the **show** operational mode command.

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

3. The following output is displayed.

```
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 10.0.0.1/30;
    }
}
unit 1 {
    vci 200;
    oam-period 3;
    family inet {
        address 192.168.0.1/30;
    }
}
}

```

Displaying the APS Container Interface Configuration

Purpose

To display the APS container interface configuration

Action

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

- **show aps**
- **show aps extensive**
- **show interfaces cin extensive**
- **show interfaces at-*fpc/pic/port* extensive**

See the [CLI Explorer](#).

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[APS Using a Container Interface with ATM Encapsulation Overview | 97](#)

[SONET/SDH Interfaces Overview | 2](#)

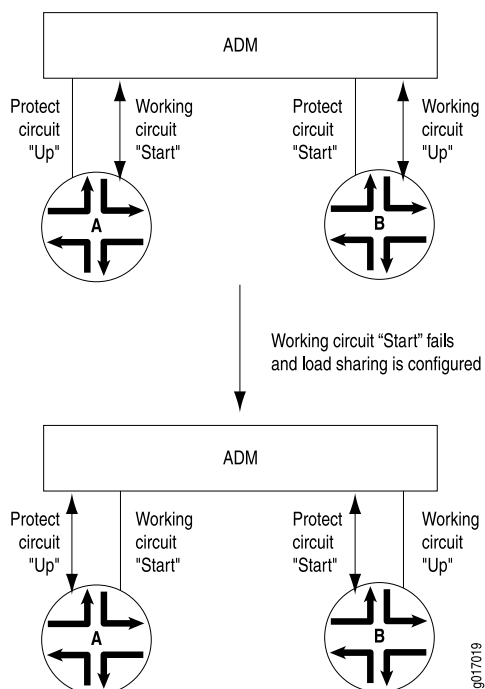
APS Load Sharing Between Circuit Pairs Overview

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 3 on page 102](#) 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 3: APS Load Sharing Between Circuit Pairs



RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring APS Load Sharing | 102](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring APS Load Sharing

To configure load sharing between two working-protect circuit pair:

1. In configuration mode, go to the `[edit interfaces interface-name sonet-options aps]` hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options aps
```

2. Configure the **paired-group** option when configuring one of the circuits on one of the routers. In this statement, the *group-name* variable is the name of the group you assigned to one of the circuits with the working-circuit and protect-circuit statements.


```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set paired-group group-name
```

The Junos OS automatically configures the remainder of the load-sharing setup based on the group name.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Interfaces Overview | 2](#)

Example: Configuring APS Load Sharing Between Circuit Pairs

IN THIS SECTION

- [Requirements for APS Load Sharing Between Circuit Pairs | 103](#)
- [Overview | 103](#)
- [Configuring APS Load Sharing Between Circuit Pairs | 104](#)

Requirements for APS Load Sharing Between Circuit Pairs

This example uses the following hardware and software components:

- Two MX Series, M Series, or T Series routers.
- Junos OS Release 7.4 or later

Overview

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.

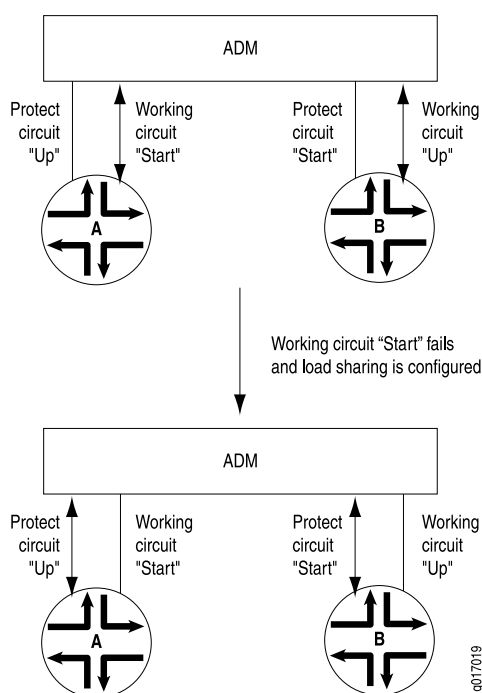
[Figure 4 on page 104](#) illustrates load sharing between circuits on two routers. Router A has a working circuit “Start” and a protect circuit “Up,” and Router B has a working circuit “Up” and a protect circuit “Start.” Under normal circumstances, Router A carries the “Start” circuit traffic and Router 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.”

Topology

Figure 4: APS Load Sharing Between Circuit Pairs



Configuring APS Load Sharing Between Circuit Pairs

IN THIS SECTION

- [Configuring APS Load Sharing on Router A | 105](#)
- [Configuring APS Load Sharing on Router B | 106](#)

To configure APS load sharing to match the configuration shown in [Figure 4 on page 104](#), perform the following tasks:

Configuring APS Load Sharing on Router A

Step-by-Step Procedure

Perform the following steps on the first interface—that is, on the so-7/0/0 interface:

1. Configure the working circuit as **start**.

```
[edit interfaces so-7/0/0 sonet-options aps]  
user@host# set working-circuit start
```

2. Configure the authentication key as **linsey**.

```
[edit interfaces so-7/0/0 sonet-options aps]  
user@host# set authentication-key linsey
```

3. Configure the paired group as **Router A-Router B**.

```
[edit interfaces so-7/0/0 sonet-options aps]  
user@host# set paired-group "Router A-Router B"
```

Configure the other options as needed.

Step-by-Step Procedure

Perform the following steps on the other interface—on the so-0/0/0 interface:

1. Configure the protect circuit as **up**.

```
[edit interfaces so-0/0/0 sonet-options aps]  
user@host# set protect-circuit up
```

2. Configure the authentication key as **woolsey**.

```
[edit interfaces so-0/0/0 sonet-options aps]  
user@host# set authentication-key woolsey
```

3. Configure the paired group as **Router A-Router B**.

```
[edit interfaces so-0/0/0 sonet-options aps]  
user@host# sset paired-group "Router A-Router B"
```

Configure the other options as needed.

Configuring APS Load Sharing on Router B

Step-by-Step Procedure

Perform the following steps on the first interface—that is, on the so-1/0/0 interface:

1. Configure the working circuit as **up**.

```
[edit interfaces so-1/0/0 sonet-options aps]  
user@host# set working-circuit up
```

2. Configure the authentication key as **woolsey**.

```
[edit interfaces so-1/0/0 sonet-options aps]  
user@host# set authentication-key woolsey
```

3. Configure the paired group as Router A-Router B.

```
[edit interfaces so-1/0/0 sonet-options aps]  
user@host# set paired-group "Router A-Router B"
```

Configure the other options as needed.

Step-by-Step Procedure

Perform the following steps on the other interface—that is, on the so-6/0/0 interface:

1. Configure the protect circuit as **start**.

```
[edit interfaces so-6/0/0 sonet-options aps]  
user@host# set protect-circuit start
```

2. Configure the authentication key as **linsey**.

```
[edit interfaces so-6/0/0 sonet-options aps]  
user@host# set authentication-key linsey
```

3. Configure the paired group as Router A-Router B.

```
[edit interfaces so-6/0/0 sonet-options aps]  
user@host# set paired-group "Router A-Router B"
```

Configure the other options as needed.

RELATED DOCUMENTATION

[Automatic Protection Switching and Multiplex Section Protection Overview | 76](#)

[Basic Automatic Protect Switching Overview | 81](#)

[Configuring Basic Automatic Protect Switching | 82](#)

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[SONET/SDH Interfaces Overview | 2](#)

Link PIC Redundancy Overview

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 Library for Routing Devices*.

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.

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring Link PIC Redundancy | 108](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring Link PIC Redundancy

IN THIS SECTION

- [Configuring Link State Replication | 108](#)
- [Displaying Link PIC Redundancy | 108](#)

Configuring Link State Replication

To configure link state replication:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options aps
```

2. Configure the **preserve-interface** option.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set preserve-interface
```

Displaying Link PIC Redundancy

Purpose

To display the link state replication configuration.

Action

To display link state replication options between the ports coc3-1/0/0 and coc3-2/0/0:

1. In configuration mode, go to the **[edit interfaces coc3-1/0/0]** hierarchy level.

```
[edit]
user@host# edit interfaces coc3-1/0/0
```

2. Display the link state replication details by issuing the **show** operational mode command.

```
[edit interfaces coc3-1/0/0]  
user@host# show
```

3. The following output is displayed.

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

4. In configuration mode, go to the **[edit interfaces coc3-2/0/0]** hierarchy level.

```
[edit]  
user@host# edit interfaces coc3-1/0/0
```

5. Display the link state replication details by issuing the **show** operational mode command.

```
[edit interfaces coc3-2/0/0]  
user@host# show
```

6. The following output is displayed.

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

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Link PIC Redundancy Overview | 107](#)

Switching Between the Working and Protect Circuits Overview

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** operational mode 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** operational mode 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** operational mode 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.

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.

RELATED DOCUMENTATION

[Configuring Switching Between the Working and Protect Circuits | 111](#)

[Configuring Lockout of Protection for SDH Interfaces | 88](#)

[Configuring Switching Between the Working and Protect Circuits | 111](#)

[Configuring SONET/SDH Physical Interface Properties | 6](#)

Configuring Switching Between the Working and Protect Circuits

You can perform a manual switch between the working and protect circuits.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# [edit interfaces interface-name sonet-options aps]
```

2. Configure the **request** option as protect or working to perform a manual switch. This option is honored only if there are no higher-priority reasons to switch.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set request (protect | working)
```

To switch the circuit manually to being the working circuit or to override the revert timer when the working circuit is operating in nonrevertive mode:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# [edit interfaces interface-name sonet-options aps]
```

2. Configure the **request working** option to switch the circuit manually to being the working circuit or to override the revert timer when the working circuit is operating in nonrevertive mode.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set request working
```

To perform a forced switch:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# [edit interfaces interface-name sonet-options aps]
```

2. Configure the **force** option to perform a forced switch. This option 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]
user@host# set 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.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# [edit interfaces interface-name sonet-options aps]
```

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

```
[edit interfaces so-fpc/pic/port sonet-options aps annex-b]
user@host# set lockout
```

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

RELATED DOCUMENTATION

- [Configuring SONET/SDH Physical Interface Properties | 6](#)
- [Switching Between the Working and Protect Circuits Overview | 110](#)
- [Configuring Lockout of Protection for SDH Interfaces | 88](#)
- [Switching Between the Working and Protect Circuits Overview | 110](#)

Revertive Mode Overview

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.

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).

RELATED DOCUMENTATION

- [Configuring SONET/SDH Physical Interface Properties | 6](#)
- [Configuring Revertive Mode | 113](#)
- [SONET/SDH Interfaces Overview | 2](#)

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 APS in revertive mode:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options aps
```

2. Configure revertive mode by setting the **revert-time** option in seconds which specifies 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]  
user@host# set revert-time seconds
```

To configure APS in nonrevertive mode:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]  
user@host# edit interfaces interface-name sonet-options aps
```

2. Configure the nonrevertive mode by setting the **request working** option to switch the circuit manually to being the working circuit or to override the revert timer. This is configured with the **revert-time** option.

```
[edit interfaces so-fpc/pic/port sonet-options aps]  
user@host# set request working
```

NOTE:

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).

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Revertive Mode Overview | 113](#)

[SONET/SDH Interfaces Overview | 2](#)

Switching Mode Overview

There are two types of switching mode:

- Unidirectional mode
- Bidirectional mode

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)

RELATED DOCUMENTATION

[Configuring SONET/SDH Physical Interface Properties | 6](#)

[Configuring Switching Mode | 116](#)

[SONET/SDH Interfaces Overview | 2](#)

Configuring Switching Mode

To configure switching mode in unidirectional mode:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options aps
```

2. Configure unidirectional mode by setting the **unidirectional** option.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set switching-mode unidirectional
```

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

To configure switching mode in bidirectional mode:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options aps
```

2. Configure bidirectional mode to restore the default behavior by setting the **bidirectional** option.

```
[edit interfaces so-fpc/pic/port sonet-options aps]
user@host# set switching-mode bidirectional
```

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

RELATED DOCUMENTATION

Configuring SONET/SDH Physical Interface Properties | 6

Switching Mode Overview | 115

SONET/SDH Interfaces Overview | 2

Configuring Aggregated SONET/SDH Interfaces for High Availability

IN THIS CHAPTER

- [Understanding Aggregated SONET/SDH Interfaces | 118](#)
- [Configuring Aggregated SONET/SDH Interfaces | 121](#)

Understanding Aggregated SONET/SDH Interfaces

Junos OS enables link aggregation of SONET/SDH interfaces; this is similar to Ethernet link aggregation, but is not defined in a public standard. 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 Library*.

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.

NOTE: Channelized OC IQ, IQE, and SONET/SDH OC48/STM16 IQE PICs do not support SONET aggregation.

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

Understanding Aggregated SONET/SDH Properties

IN THIS SECTION

- [Creating Aggregated SONET/SDH Interfaces | 119](#)
- [SONET/SDH Link Aggregation Overview | 119](#)
- [Aggregated SONET/SDH Link Speed Overview | 119](#)
- [Configuring Aggregated SONET/SDH Minimum Links | 120](#)

Creating Aggregated SONET/SDH Interfaces

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. For information about configuring device count, see [“Configuring Aggregated SONET/SDH Interfaces” on page 121](#).

Starting with Junos OS Release 13.2, a maximum of 64 aggregated interfaces are supported for link aggregation of SONET/SDH interfaces. Prior to Junos OS Release 13.2, a maximum of 16 aggregated interfaces were supported for link aggregation of SONET/SDH interfaces. The aggregated SONET/SDH interfaces are numbered from **as0** through **as63**. For more information, see the *Junos OS Services Interfaces Library for Routing Devices*.

Additionally, you must assign a number for the variable **x** for the aggregated SONET/SDH interface **asx** at the **[edit interfaces]** hierarchy level and also specify the constituent physical interfaces by including the **aggregate** statement at the **[edit interfaces interface-name sonet-options]** hierarchy level.

You can optionally specify other physical properties that apply specifically to the aggregated SONET/SDH interfaces; for details, see [“SONET/SDH Interfaces Overview” on page 2](#)

SONET/SDH Link Aggregation Overview

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.

x is the interface instance number and can be from 0 through 63, for a total of 64 aggregated interfaces. You should not mix SONET and SDH mode on the same aggregated interface. In addition, you must also include a statement configuring **asx** at the **[edit interfaces]** hierarchy level.

Aggregated SONET/SDH Link Speed Overview

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.

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**.

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**.

RELATED DOCUMENTATION

| [Configuring Aggregated SONET/SDH Interfaces](#) | 121

Configuring Aggregated SONET/SDH Interfaces

IN THIS SECTION

- [Configuring Aggregated SONET/SDH Interfaces | 121](#)
- [Deleting an Aggregated SONET/SDH Interface | 124](#)
- [Configuring Filtering on a Aggregated SONET/SDH Interface | 125](#)
- [Configuring Sampling on Aggregated SONET/SDH Interfaces | 127](#)

Configuring Aggregated SONET/SDH Interfaces

To configure the aggregated SONET/SDH interfaces, perform the following tasks:

1. [Configuring Device Count | 121](#)
2. [Configuring Constituent Physical Interface | 121](#)
3. [Configuring an Aggregated SONET/SDH Interfaces | 122](#)
4. [Displaying the Aggregated SONET/SDH Interface Configuration | 123](#)

Configuring Device Count

To configure the number of aggregated SONET/SDH interfaces as per requirement.

1. In configuration mode, go to the `[edit chassis aggregated-devices sonet]` hierarchy level.

```
[edit]
user@host# edit chassis aggregated-devices sonet
```

2. Configure the number of aggregated SONET interfaces from 1 through 64.

```
[edit chassis aggregated-devices sonet]
user@host# set device-count device-count
```

For example, if you set the **device-count** statement as 12, you can configure the aggregated SONET/SDH interfaces from **as0** through **as11**.

Configuring Constituent Physical Interface

After you set the device count at the `[edit chassis aggregated-devices sonet]` hierarchy level, you can associate a physical interface with an aggregated SONET/SDH interface.

To associate the physical interface with an aggregated SONET/SDH link.

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options]** hierarchy level. For example, set the interface name as so-1/3/0.

```
[edit]
user@host# [edit interfaces so-1/3/0 aggregated-sonet-options]
```

2. Configure the **aggregate** statement with the aggregated interface to join a SONET aggregate.

```
[edit interfaces so-1/3/0 aggregated-sonet-options]
user@host# set aggregate asx
```

NOTE: *x* is the interface instance number and can be from 0 through 63, for a total of 64 aggregated interfaces. You should not mix SONET and SDH mode on the same aggregated interface.

You can optionally specify other physical properties that apply specifically to the aggregated SONET/SDH interface; for details, see [“SONET/SDH Interfaces Overview” on page 2](#).

Configuring an Aggregated SONET/SDH Interfaces

To configure an aggregated SONET/SDH interface, for example as0 interface.

1. In configuration mode, go to the **[edit interfaces as0 aggregated-sonet-options]** hierarchy level.

```
[edit]
user@host# edit interfaces as0 aggregated-sonet-options
```

2. Configure the aggregated links speed of the as0 interface as **mixed**, **oc12**, **oc192**, **oc3**, **oc48**, or **oc768**.

```
[edit interfaces as0 aggregated-sonet-options]
user@host# set link-speed mixed | oc12 | oc192 | oc48 | oc768
```

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.

3. Configure the minimum bandwidth necessary to sustain the bundle in bits per second (bps).

```
[edit interfaces as0 aggregated-sonet-options]
user@host# set minimum-bandwidth minimum-bandwidth
```

4. Configure the minimum number of aggregated links that must be up for the bundle as a whole to be labeled **up** on the ae0 interface from 1 through 32. By default, only one link must be up for the bundle to be labeled **up**

```
[edit interfaces as0 aggregated-sonet-options]
user@host# set minimum-links minimum-links
```

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**.

Displaying the Aggregated SONET/SDH Interface Configuration

Purpose

To display the aggregated SONET/SDH configuration for the as0 interface when the following options are set to get an aggregated SONET/SDH interface up and running:

- Minimum links—1
- Link speed—oc3
- Device count—15
- SONET interface name—so-1/3/0

Action

Run the **show** command after setting the aforementioned parameters.

```
[edit]
user@host# show
interfaces {
  as0 {
    aggregated-sonet-options {
      minimum-links 1;
      link-speed oc3;
    }
    unit 0 {
      family inet {
        address 10.2.11.1/30;
      }
    }
  }
  so-1/3/0 {
    sonet-options {
      aggregate as0;
    }
  }
  chassis {
    aggregated-devices {
      sonet {
        device-count 15;
      }
    }
  }
}
```

Deleting an Aggregated SONET/SDH Interface

To delete an aggregated SONET/SDH interface (for example as0 interface) and to set the aggregated SONET/SDH interface to down state, perform the following tasks:

1. [Deleting the Interface | 124](#)
2. [Deleting Device Count | 125](#)

Deleting the Interface

To delete an aggregated SONET/SDH interface, for example the as0 interface.

1. In configuration mode, go to the **[edit interfaces]** hierarchy level.

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

2. Delete the aggregated SONET/SDH interface.

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

To set the aggregated SONET/SDH interface to down state

1. In configuration mode, go to the **[edit chassis aggregated-devices sonet]** hierarchy level.

```
[edit]
user@host# edit chassis aggregated-devices sonet
```

2. Delete the aggregated SONET/SDH interface.

```
[edit interfaces]
user@host# delete device-count
```

Deleting Device Count

To delete the device count for the aggregated SONET/SDH interfaces.

To set the aggregated SONET/SDH interface to down state

1. In configuration mode, go to the **[edit chassis aggregated-devices sonet]** hierarchy level.

```
[edit]
user@host# edit chassis aggregated-devices sonet
```

2. Delete the aggregated SONET/SDH interface.

```
[edit interfaces]
user@host# delete device-count
```

Configuring Filtering on a Aggregated SONET/SDH Interface

1. [Configuring Filters or Sampling on Aggregated SONET/SDH Links | 126](#)
2. [Configuring Filter Options | 126](#)

Configuring Filters or Sampling on Aggregated SONET/SDH Links

To set up firewall filters or sampling on the aggregated SONET/SDH interfaces, you must configure the **asx** interface with the following properties.

1. In configuration mode, go to the **[edit interfaces asx unit logical-unit-number filter]** hierarchy level.

```
[edit]
user@host# edit interfaces asx unit logical-unit-number filter
```

2. Configure the **input** option with a name for the filter to be applied to received packets.

```
[edit interfaces asx unit logical-unit-number filter]
user@host# set input input-filter-name
```

3. Configure the **output** option with a name for the filter to be applied to transmitted packets.

```
[edit interfaces asx unit logical-unit-number filter]
user@host# set output output-filter-name
```

Configuring Filter Options

To configure firewall filters options for input filter **input-filter-name** and output filter **output-filter-name**.

1. In configuration mode, go to the **[edit firewall]** hierarchy level.

```
[edit]
user@host# edit firewall
```

2. Configure the input filter.

```
[edit firewall]
user@host# edit filter input-filter-name
```

3. Configure the input filter options.

```
[edit firewall filter input-filter-name]
user@host# set term match-any-input then accept
```

4. Configure the output filter.


```
[edit firewall]
user@host# up
user@host# edit filter output-filter-name
```

5. Configure the output filter options.

```
[edit firewall filter input-filter-name]
user@host# set term match-any-output then accept
```

Configuring Sampling on Aggregated SONET/SDH Interfaces

1. [Configuring Sampling on a Aggregated SONET/SDH Interface | 127](#)
2. [Configuring Sampling Filter Options | 127](#)
3. [Configuring Forwarding Options For a Sampling Filter | 128](#)

Configuring Sampling on a Aggregated SONET/SDH Interface

To set up sampling on the aggregated SONET/SDH interfaces, you must configure the **asx** interface with the following properties.

1. In configuration mode, go to the **[edit interfaces asx unit logical-unit-number filter]** hierarchy level.

```
[edit]
user@host# edit interfaces asx unit logical-unit-number filter
```

2. Configure the **input** option with a name for the filter to be applied to received packets.

```
[edit interfaces asx unit logical-unit-number filter]
user@host# set input input-sampler-name
```

Configuring Sampling Filter Options

To configure firewall sampling filters options for input sampling filter **input-sampler-name**.

1. In configuration mode, go to the **[edit firewall]** hierarchy level.

```
[edit]
user@host# edit firewall
```

2. Configure the input filter.

```
[edit firewall]
user@host# edit filter input-sampler-name
```

3. Configure the input filter options.

```
[edit firewall filter input-filter-name
user@host# set term match-any-input then sample
user@host# set term match-any-input then accept
```

Configuring Forwarding Options For a Sampling Filter

To configure the forwarding options for a sampling filter.

1. In configuration mode, go to the **[edit forwarding-options sampling input]** hierarchy level.

```
[edit]
user@host# edit forwarding-options sampling input
```

2. Configure the ratio of packets to be sampled (1 out of N number of packets) from 1 through 65535.

```
[edit forwarding-options sampling input]
user@host# set rate rate
```

3. Configure the number of samples after initial trigger from 0 through 20.

```
[edit forwarding-options sampling input]
user@host# set run-length length
```

4. Configure the threshold of samples per second before dropping.

```
[edit forwarding-options sampling input]
user@host# set max-packets-per-second
```

5. Configure the maximum length of the sampled packet from 0 through 9192 bytes.

```
[edit forwarding-options sampling input]
user@host# set maximum-packet-length length
```

RELATED DOCUMENTATION

| [Understanding Aggregated SONET/SDH Interfaces](#) | 118

3

PART

Monitoring and Troubleshooting Information

Monitoring SONET/SDH Interfaces | **131**

Troubleshooting SONET/SDH Interfaces | **138**

Monitoring SONET/SDH Interfaces

IN THIS CHAPTER

- [Packet Flow Monitoring on SONET/SDH Interfaces Overview | 131](#)
- [Enabling Packet Flow Monitoring on SONET/SDH Interfaces | 132](#)
- [Configuring Multicast Statistics Collection on SONET Interfaces | 135](#)
- [Configuring Multicast Statistics Collection on Aggregated SONET Interfaces | 136](#)

Packet Flow Monitoring on SONET/SDH Interfaces Overview

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.

For information about enabling packet flow monitoring on SONET/SDH interfaces, see [“Enabling Packet Flow Monitoring on SONET/SDH Interfaces” on page 132](#).

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 Library for Routing Devices*.

To Monitor Packets with MPLS Labels

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.

For information about removing MPLS labels from an incoming packet to a Monitoring Services PIC, see [“Enabling Packet Flow Monitoring on SONET/SDH Interfaces” on page 132](#).

NOTE: On T Series routers, the **pop-all-labels** command can remove up to five MPLS labels from incoming packets.

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

- By default, the **pop-all-labels** statement takes effect for incoming packets with one or two labels.
- 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.

RELATED DOCUMENTATION

| [Enabling Packet Flow Monitoring on SONET/SDH Interfaces](#) | 132

Enabling Packet Flow Monitoring on SONET/SDH Interfaces

IN THIS SECTION

- [Configuring Packet Flow Monitoring on a SONET/SDH Interface](#) | 133
- [Configuring Packet Flow Monitoring on a Monitoring Services Interface](#) | 133
- [Removing MPLS Labels from Incoming Packets](#) | 134

You can enable packet flow monitoring on SONET/SDH interfaces.

This topic includes the following tasks:

Configuring Packet Flow Monitoring on a SONET/SDH Interface

To configure packet flow monitoring on SONET/SDH interfaces:

1. In configuration mode, go to the **[edit interfaces so-fpc/pic/port unit logical-unit-number]** hierarchy level.

```
[edit]
user@host# edit interfaces so-fpc/pic/port unit logical-unit-number
```

2. Configure packet flow monitoring to monitor packet flows from another router.

```
[edit interfaces so-fpc/pic/port unit logical-unit-number]
user@host# set passive-monitor-mode
```

NOTE:

- If you include this statement in the configuration, the SONET/SDH interface does not send keepalives or alarms, and does not participate actively on the network.
- For SONET/SDH interfaces, you can include this statement on the logical interface only.

Configuring Packet Flow Monitoring on a Monitoring Services Interface

To configure packet flow monitoring on a monitoring services interface:

1. In configuration mode, go to the **[edit interfaces mo-fpc/pic/port unit logical-unit-number]** hierarchy level.

```
[edit]
user@host# edit interfaces mo-fpc/pic/port unit logical-unit-number
```

2. Enable packet flow monitoring to monitor packet flows from another router on a monitoring services interface by specifying the **family** option as **inet**.

```
[edit interfaces mo-fpc/pic/port unit logical-unit-number]
user@host# set family inet
```

3. Configure the **receive-options-packets** and the **receive-ttl-exceeded** statements for conformity with cflowd record structure.

```
[edit interfaces mo-fpc/pic/port unit logical-unit-number family inet]
user@host# set receive-options-packets
user@host# set 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 Library for Routing Devices*.

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 to a Monitoring Services PIC.

To remove MPLS labels from an incoming packet to a Monitoring Services PIC:

1. In configuration mode, go to the **[edit interfaces *interface-name* sonet-options mpls]** hierarchy level.

```
[edit]
user@host# edit interfaces interface-name sonet-options mpls
```

2. Configure the **pop-all-labels** statement to remove up to two MPLS labels from incoming IP packets. Note that on T Series routers, the **pop-all-labels** statement removes up to five MPLS labels from incoming IP packets.

```
[edit interfaces interface-name sonet-options mpls]
user@host# set pop-all-labels
```

3. Configure the **required-depth *number*** statement to specify the number of MPLS labels an incoming packet must have for the **pop-all-labels** statement to take effect.

```
[edit interfaces interface-name sonet-options mpls pop-all-labels]
user@host# set 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.

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

- By default, the **pop-all-labels** statement takes effect for incoming packets with one or two labels.
- 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.

RELATED DOCUMENTATION

| [Packet Flow Monitoring on SONET/SDH Interfaces Overview](#) | 131

Configuring Multicast Statistics Collection on SONET Interfaces

T Series and TX Matrix routers support multicast statistics collection on 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 a SONET interface follows:

```
[edit interfaces]
so-fpc/pic/port {
  multicast-statistics;
}
```

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

RELATED DOCUMENTATION

multicast-statistics

[Configuring Multicast Statistics Collection on Aggregated SONET Interfaces | 136](#)

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 | 135](#)

Troubleshooting SONET/SDH Interfaces

IN THIS CHAPTER

- [Configuring Interface Diagnostics Tools to Test the Physical Layer Connections | 138](#)
- [Investigating Interface Steps and Commands | 146](#)
- [Monitoring SONET Interfaces | 151](#)
- [Using Loopback Testing for SONET Interfaces | 162](#)
- [Locating SONET Alarms and Errors | 179](#)
- [Enabling SONET Payload Scrambling | 209](#)
- [Checking the SONET Frame Checksum | 214](#)

Configuring Interface Diagnostics Tools to Test the Physical Layer Connections

IN THIS SECTION

- [Configuring Loopback Testing | 138](#)
- [Configuring BERT Testing | 141](#)
- [Starting and Stopping a BERT Test | 144](#)

Configuring Loopback Testing

Loopback testing allows you to verify the connectivity of a circuit. You can configure any of the following interfaces to execute a loopback test: aggregated Ethernet, Fast Ethernet, Gigabit Ethernet, E1, E3, NxDS0, serial, SONET/SDH, T1, and T3.

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

isolate the problem by using a loopback test. Loopback tests allow you to isolate segments of the circuit and test them separately.

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

The following types of loopback testing are supported by Junos OS:

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

Table 14 on page 139 shows the loopback modes supported on the various interface types.

Table 14: Loopback Modes by Interface Type

Interface	Loopback Modes	Usage Guidelines
Aggregated Ethernet, Fast Ethernet, Gigabit Ethernet	Local	<i>Configuring Ethernet Loopback Capability</i>
Circuit Emulation E1	Local and remote	<i>Configuring E1 Loopback Capability</i>

Table 14: Loopback Modes by Interface Type *(continued)*

Interface	Loopback Modes	Usage Guidelines
Circuit Emulation T1	Local and remote	<i>Configuring T1 Loopback Capability</i>
E1 and E3	Local and remote	<i>Configuring E1 Loopback Capability and Configuring E3 Loopback Capability</i>
NxDS0	Payload	<i>Configuring NxDS0 IQ and IQE Interfaces, Configuring T1 and NxDS0 Interfaces, Configuring Channelized OC12/STM4 IQ and IQE Interfaces (SONET Mode), Configuring Fractional E1 IQ and IQE Interfaces, and Configuring Channelized T3 IQ Interfaces</i>
Serial (V.35 and X.21)	Local and remote	<i>Configuring Serial Loopback Capability</i>
Serial (EIA-530)	DCE local, DCE remote, local, and remote	<i>Configuring Serial Loopback Capability</i>
SONET/SDH	Local and remote	“Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External” on page 42
T1 and T3	Local, payload, and remote	<i>Configuring T1 Loopback Capability and Configuring T3 Loopback Capability</i> <i>See also Configuring the T1 Remote Loopback Response</i>

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

```
user@host# loopback mode;
```

You can include this statement at the following hierarchy levels:

- [edit interfaces *interface-name* aggregated-ether-options]
- [edit interfaces *interface-name* ds0-options]
- [edit interfaces *interface-name* e1-options]
- [edit interfaces *interface-name* e3-options]
- [edit interfaces *interface-name* fastether-options]

- [edit interfaces *interface-name* *gether-options*]
- [edit interfaces *interface-name* *serial-options*]
- [edit interfaces *interface-name* *sonet-options*]
- [edit interfaces *interface-name* *t1-options*]
- [edit interfaces *interface-name* *t3-options*]

Configuring BERT Testing

To configure BERT:

- Configure the duration of the test.

```
[edit interfaces interface-name interface-type-options]
user@host#bert-period seconds;
```

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

- Configure the error rate to monitor when the inbound pattern is received.

```
[edit interfaces interface-name interface-type-options]
user@host#bert-error-rate rate;
```

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

- Configure the bit pattern to send on the transmit path.

```
[edit interfaces interface-name interface-type-options]
user@host#bert-algorithm algorithm;
```

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

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

```
user@host# set bert-algorithm ?
```

Possible completions:

```
pseudo-2e11-o152      Pattern is 2^11 -1 (per 0.152 standard)
pseudo-2e15-o151      Pattern is 2^15 - 1 (per 0.152 standard)
```

```

pseudo-2e20-o151    Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e20-o153    Pattern is 2^20 - 1 (per 0.153 standard)
...

```

For specific hierarchy information, see the individual interface types.

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

```

pseudo-2e11-o152    Pattern is 2^11 -1 (per 0.152 standard)
pseudo-2e15-o151    Pattern is 2^15 - 1 (per 0.151 standard)
pseudo-2e20-o151    Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e23-o151    Pattern is 2^23 (per 0.151 standard)

```

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

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

```

all-ones-repeating   Repeating one bits
all-zeros-repeating  Repeating zero bits
alternating-double-ones-zeros Alternating pairs of ones and zeros
alternating-ones-zeros Alternating ones and zeros
pseudo-2e11-o152    Pattern is 2^11 -1 (per 0.152 standard)
pseudo-2e15-o151    Pattern is 2^15 - 1 (per 0.151 standard)
pseudo-2e20-o151    Pattern is 2^20 - 1 (per 0.151 standard)
pseudo-2e7          Pattern is 2^7 - 1
pseudo-2e9-o153     Pattern is 2^9 - 1 (per 0.153 standard)
repeating-1-in-4     1 bit in 4 is set
repeating-1-in-8     1 bit in 8 is set
repeating-3-in-24    3 bits in 24 are set

```

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

NOTE: The IQE PICs support only the following algorithms:

```
all-ones-repeating    Repeating one bits
all-zeros-repeating   Repeating zero bits
alternating-double-ones-zeros Alternating pairs of ones and zeros
alternating-ones-zeros Alternating ones and zeros
pseudo-2e9-o153      Pattern is 2^9 -1 (per 0.153 (511 type) standard)
pseudo-2e11-o152     Pattern is 2^11 -1 (per 0.152 and 0.153 (2047 type)
standards)
pseudo-2e15-o151     Pattern is 2^15 -1 (per 0.151 standard)
pseudo-2e20-o151     Pattern is 2^20 -1 (per 0.151 standard)
pseudo-2e20-o153     Pattern is 2^20 -1 (per 0.153 standard)
pseudo-2e23-o151     Pattern is 2^23 -1 (per 0.151 standard)
repeating-1-in-4      1 bit in 4 is set
repeating-1-in-8      1 bit in 8 is set
repeating-3-in-24     3 bits in 24 are set
```

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

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

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

Table 15 on page 144 shows the BERT capabilities for various interface types.

Table 15: BERT Capabilities by Interface Type

Interface	T1 BERT	T3 BERT	Comments
12-port T1/E1 Circuit Emulation	Yes (ports 0–11)	—	<ul style="list-style-type: none"> • Limited algorithms
4-port Channelized OC3/STM1 Circuit Emulation	Yes (port 0–3)	—	<ul style="list-style-type: none"> • Limited algorithms
E1 or T1	Yes (port 0–3)	Yes (port 0–3)	<ul style="list-style-type: none"> • Single port at a time • Limited algorithms
E3 or T3	Yes (port 0–3)	Yes (port 0–3)	<ul style="list-style-type: none"> • Single port at a time
Channelized OC12	—	Yes (channel 0–11)	<ul style="list-style-type: none"> • Single channel at a time • Limited algorithms • No bit count
Channelized STM1	Yes (channel 0–62)	—	<ul style="list-style-type: none"> • Multiple channels • Only one algorithm • No error insert • No bit count
Channelized T3 and Multichannel T3	Yes (channel 0–27)	Yes (port 0–3 on channel 0)	<ul style="list-style-type: none"> • Multiple ports and channels • Limited algorithms for T1 • No error insert for T1 • No bit count for T1

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

Starting and Stopping a BERT Test

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

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

```
disable;
```

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

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

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

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

For example:

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

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

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

For more information about running and evaluating the results of the BERT procedure, see the [CLI Explorer](#).

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

RELATED DOCUMENTATION

show interfaces diagnostics optics (Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, 100-Gigabit Ethernet, and Virtual Chassis Port)

Investigating Interface Steps and Commands

IN THIS SECTION

- [Investigating Interface Steps and Commands Overview | 146](#)
- [Monitoring Interfaces | 146](#)
- [Performing a Loopback Test on an Interface | 147](#)
- [Locating Interface Alarms | 150](#)

This section includes the following information to assist you when troubleshooting interfaces:

Investigating Interface Steps and Commands Overview

The [“Monitoring Interfaces” on page 146](#) section helps you determine the nature of the interface problem. The [“Performing a Loopback Test on an Interface” on page 147](#) section provides information to help you isolate the source of the problem. The [“Locating Interface Alarms” on page 150](#) section explains some of the alarms and errors for the media.

SEE ALSO

[Monitoring Interfaces | 146](#)

[Performing a Loopback Test on an Interface | 147](#)

[Locating Interface Alarms | 150](#)

Monitoring Interfaces

Problem

Description: 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 [Table 16 on page 147](#) lists and describes the operational mode commands you use to monitor interfaces.

Table 16: Commands Used to Monitor Interfaces

CLI Command	Description
show interfaces terse <i>interface-name</i> For example: show interfaces terse t1*	Displays summary information about the named interfaces.
show interfaces <i>interface-name</i> For example: show interfaces t1-x/y/z	Displays static status information about a specific interface.
show interfaces <i>interface-name</i> extensive For example: show interfaces t1-x/y/z extensive	Displays very detailed interface information about a specific interface.
monitor interface <i>interface-name</i> For example: monitor interface t1-x/y/z	Displays real-time statistics about a physical interface, updated every second.

SEE ALSO

[Investigating Interface Steps and Commands Overview | 146](#)

[Performing a Loopback Test on an Interface | 147](#)

[Locating Interface Alarms | 150](#)

Performing a Loopback Test on an Interface

Problem

Description: 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. To 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. To 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 [Table 17 on page 148](#) 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 17: Commands Used to Perform Loopback Testing on Interfaces

CLI Statement or Command	Interface Type	Description
[edit interfaces <i>interface-name</i> 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.

Table 17: Commands Used to Perform Loopback Testing on Interfaces (*continued*)

CLI Statement or Command	Interface Type	Description
[edit interfaces <i>interface-name</i>] 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 <i>interface-name</i>	Used for all interfaces	Display static status information about a specific interface.
[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet address <i>ip-address</i>] set arp <i>ip-address</i> mac <i>mac-address</i>	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 <i>interface-name</i>	All interfaces	Reset the statistics for an interface to zero.
[edit interfaces <i>interface-name</i>] 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.
[edit interfaces <i>interface-name</i>] 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 <i>interface-name</i> terse	T1, T3, and SONET interfaces	Display summary information about interfaces. (Use to display the status of the logical interfaces for these interfaces.)

Table 17: Commands Used to Perform Loopback Testing on Interfaces (*continued*)

CLI Statement or Command	Interface Type	Description
ping interface t1-x/y/z local-ip-address bypass-routing count 1000 rapid	All interfaces	<p>Check the reachability of network hosts by sending ICMP ECHO_REQUEST messages to elicit ICMP ECHO_RESPONSE messages from the specified host.</p> <p>Use the bypass-routing option to ping a local system through an interface that has no route through it.</p> <p>The count option sends 1000 ping requests through the system.</p> <p>Type Ctrl+C to interrupt a ping command.</p>
show interfaces interface-name extensive	All interfaces	Display very detailed interface information about a specific interface.

SEE ALSO

[Investigating Interface Steps and Commands Overview | 146](#)

[Monitoring Interfaces | 146](#)

[Locating Interface Alarms | 150](#)

Locating Interface Alarms**Problem**

Description: 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.

SEE ALSO

[Investigating Interface Steps and Commands Overview | 146](#)

[Monitoring Interfaces | 146](#)

[Performing a Loopback Test on an Interface | 147](#)

Monitoring SONET Interfaces

IN THIS SECTION

- [Checklist for Monitoring SONET Interfaces | 151](#)
- [Monitoring SONET Interfaces | 151](#)
- [Verifying the Status of the Logical Interface | 160](#)

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 18 on page 151](#) provides the links and commands for monitoring SONET interfaces.

Table 18: Checklist for Monitoring SONET Interfaces

Tasks	Command or Action
“Monitoring SONET Interfaces” on page 151	
1. Displaying the Status of SONET Interfaces on page 152	<code>show interfaces terse so*</code>
2. Displaying the Status of a Specific SONET Interface on page 153	<code>show interfaces so-fpc/pic/port</code>
3. Displaying Extensive Status Information for a Specific SONET Interface on page 155	<code>show interfaces so-fpc/pic/port extensive</code>
4. Monitoring Statistics for a SONET Interface on page 157	<code>monitor interface so-fpc/pic/port</code>

Monitoring 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. [Displaying the Status of SONET Interfaces | 152](#)
2. [Displaying the Status of a Specific SONET Interface | 153](#)
3. [Displaying Extensive Status Information for a Specific SONET Interface | 155](#)
4. [Monitoring Statistics for a SONET Interface | 157](#)

Displaying 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 19 on page 152](#).

Table 19: 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.
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).

Table 19: Status of SONET Interfaces (continued)

Physical Interface	Logical Interface	Status Description
so-5/3/0	so-5/3/0.0	This interface has the physical link down and the logical interface is down also.
Admin Up	Admin Up	
Link Down	Link Down	

SEE ALSO

SONET Interfaces
Monitoring SONET Interfaces 151
Checklist for Monitoring SONET Interfaces 151

Displaying 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 1

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

```

Sample Output 2

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

In the first sample output, 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 [“Displaying Extensive Status Information for a Specific SONET Interface” on page 155](#) to display more extensive information about the SONET interface and the physical interface that is down.

In the second sample output, 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 [“Monitoring Statistics for a SONET Interface” on page 157](#) to monitor statistics for the SONET interface and the logical interface that is down.

Displaying 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 179](#) for an explanation of SONET alarms.

Monitoring 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:
  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 20 on page 159](#) 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 20: 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).
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.

SEE ALSO

[Configuring Multicast Statistics Collection on SONET Interfaces | 135](#)

[Clearing SONET Interface Statistics | 170](#)

[Checklist for Monitoring SONET Interfaces | 151](#)

[Checking for SONET Interface Error Statistics | 175](#)

Verifying 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
```

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

In the sample output 1, the **show interfaces** command in sample output 1 shows 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.

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.

SEE ALSO

| *Configuring Logical Interface Properties*

RELATED DOCUMENTATION

Monitoring Interfaces 146
Performing a Loopback Test on an Interface 147

Using Loopback Testing for SONET Interfaces

IN THIS SECTION

- [Checklist for Using Loopback Testing for SONET Interfaces | 162](#)
- [Diagnosing a Suspected Hardware Problem with a SONET Interface | 164](#)
- [Creating a Loopback | 164](#)
- [Setting Clocking to Internal | 166](#)
- [Verifying That the SONET Interface Is Up | 167](#)
- [Clearing SONET Interface Statistics | 170](#)
- [Checking That the Received and Transmitted Path Trace Are the Same | 170](#)
- [Forcing the Link Layer to Stay Up | 172](#)
- [Pinging the SONET Interface | 174](#)
- [Checking for SONET Interface Error Statistics | 175](#)
- [Diagnosing a Suspected Circuit Problem | 177](#)

This section includes the following information to assist you when troubleshooting SONET interfaces:

Checklist for Using Loopback Testing for SONET Interfaces

Purpose

To use loopback testing to isolate SONET interface problems.

Action

[Table 21 on page 162](#) provides the links and commands for using loopback testing for SONET interfaces.

Table 21: Checklist for Using Loopback Testing for SONET Interfaces

Tasks	Command or Action
-------	-------------------

[“Diagnosing a Suspected Hardware Problem with a SONET Interface” on page 164](#)

Table 21: Checklist for Using Loopback Testing for SONET Interfaces (*continued*)

Tasks	Command or Action
1. Creating a Loopback on page 164	Create a loopback.
a. Creating a Physical Loopback on page 165	Connect the transmit port to the receive port.
b. Configuring a Local Loopback on page 165	<code>[edit interfaces <i>interface-names</i>sonet-options] set loopback local show commit</code>
2. Setting Clocking to Internal on page 166	<code>[edit interfaces <i>interface-name</i>] set clocking internal show commit</code>
3. Verifying That the SONET Interface Is Up on page 167	<code>show interfaces so-fpc/pic/port</code>
4. Clearing SONET Interface Statistics on page 170	<code>clear interfaces statistics so-fpc/pic/port</code>
5. Checking That the Received and Transmitted Path Trace Are the Same on page 170	<code>show interfaces so-fpc/pic/port extensive</code>
6. Forcing the Link Layer to Stay Up on page 172	
a. Configuring Encapsulation to Cisco-HDLC on page 172	<code>[edit interfaces <i>interface-name</i>] set encapsulation cisco-hdlc show commit</code>
b. Configuring No-Keepalives on page 173	<code>[edit interfaces <i>interface-name</i>] set no-keepalives show commit</code>
7. Verifying the Status of the Logical Interface on page 160	<code>show interfaces so-fpc/pic/port show interfaces so-fpc/pic/port terse</code>
8. Pinging the SONET Interface on page 174	<code>ping interface so-fpc/pic/port local-IP-address bypass-routing count 1000 rapid</code>
9. Checking for SONET Interface Error Statistics on page 175	<code>show interfaces so-fpc/pic/port extensive</code>
“Diagnosing a Suspected Circuit Problem” on page 177	

Table 21: Checklist for Using Loopback Testing for SONET Interfaces (*continued*)

Tasks	Command or Action
1. Creating a Loop from the Router to the Network on page 177	[edit interfaces <i>interface-name</i> sonet-options] set loopback remote show commit
2. Creating a Loop to the Router from Various Points in the Network on page 178	Perform Steps 2 through 8 from “ Diagnosing a Suspected Hardware Problem with a SONET Interface ” on page 164.

Diagnosing a Suspected Hardware Problem with a SONET Interface

Problem

Description: 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:

- [Creating a Loopback on page 164](#)
- [Setting Clocking to Internal on page 166](#)
- [Verifying That the SONET Interface Is Up on page 167](#)
- [Clearing SONET Interface Statistics on page 170](#)
- [Checking That the Received and Transmitted Path Trace Are the Same on page 170](#)
- [Forcing the Link Layer to Stay Up on page 172](#)
- [Verifying the Status of the Logical Interface on page 160](#)
- [Pinging the SONET Interface on page 174](#)
- [Checking for SONET Interface Error Statistics on page 175](#)

Creating 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. [Creating a Physical Loopback | 165](#)
2. [Configuring a Local Loopback | 165](#)

Creating 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 attenuation.)

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.

SEE ALSO

[Checklist for Using Loopback Testing for SONET Interfaces | 162](#)

[Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External | 42](#)

Loopback Interface Configuration

Configuring 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 option.

```
[edit interfaces interface-name sonet-options]  
user@host# set loopback local
```

3. Verify the configuration.

```
[edit interfaces interface-name sonet-options]  
user@host# show  
loopback local;
```

4. Commit the change.

```
user@host# commit
```

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.

SEE ALSO

[Creating a Physical Loopback | 165](#)

SEE ALSO

[Setting Clocking to Internal | 166](#)

[Diagnosing a Suspected Hardware Problem with a SONET Interface | 164](#)

Setting 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
```

3. Verify the configuration.

```
[edit interfaces interface-name]
user@host# show
clocking internal;
```

4. Commit the change.

```
user@host# commit
```

Meaning

The clock source for the interface is set to the internal Stratum 3 clock.

SEE ALSO

[Creating a Loopback | 164](#)

[Verifying That the SONET Interface Is Up | 167](#)

Verifying 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
```

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

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 [“Checking That the Received and Transmitted Path Trace Are the Same” on page 170](#).

The sample output 2 shows that the physical link is down, the device flags and interface flags are down, and there are SONET alarms and defects.

[Table 22 on page 169](#) lists problem situations and actions for a physical link that is down.

Table 22: 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.

SEE ALSO

[Setting Clocking to Internal | 166](#)[Clearing SONET Interface Statistics | 170](#)

Clearing 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.

SEE ALSO

[Verifying That the SONET Interface Is Up | 167](#)[Checking That the Received and Transmitted Path Trace Are the Same | 170](#)

Checking 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 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 [“Forcing the Link Layer to Stay Up” on page 172](#).

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.

SEE ALSO

Clearing SONET Interface Statistics 170
Forcing the Link Layer to Stay Up 172

Forcing 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. [Configuring Encapsulation to Cisco-HDLC | 172](#)
2. [Configuring No-Keepalives | 173](#)

Configuring 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 encapsulation on the interface.

```
[edit interfaces interface-name]
user@host# set encapsulation cisco-hdlc
```

3. Verify the configuration.

```
[edit interfaces interface-name]
user@host# show
encapsulation hdlc;
```

4. Commit the change.

```
user@host# commit
```

Meaning

This command sets the interface encapsulation to the Cisco High-level Data-Link Control (HDLC) transport protocol.

SEE ALSO

| [Configuring No-Keepalives](#) | 173

Configuring 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 the **no-keepalives** statement.

```
[edit interfaces interface-name]
user@host# set no-keepalives
```

3. Verify the configuration.

```
[edit interfaces interface-name]
user@host# show
no-keepalives;
```

4. Commit the change.

```
user@host# commit
```

Meaning

By setting the **no-keepalives** statement, 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.

SEE ALSO

| [Configuring Encapsulation to Cisco-HDLC](#) | 172

SEE ALSO

Checking 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).

SEE ALSO

[Pinging the SONET Interface | 174](#)

[Diagnosing a Suspected Circuit Problem | 177](#)

Diagnosing 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. [Creating a Loop from the Router to the Network | 177](#)
2. [Creating a Loop to the Router from Various Points in the Network | 178](#)

Creating 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 option.

```
[edit interfaces interface-name sonet-options]
user@host# set loopback remote
```

3. Verify the configuration.

```
[edit interfaces interface-name sonet-options]
user@host# show
loopback remote;
```

4. Commit the change.

```
user@host# commit
```

Meaning

This command loops any traffic from the network back into the network.

SEE ALSO

| [SONET Interfaces](#)

Creating 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 [“Diagnosing a Suspected Hardware Problem with a SONET Interface” on page 164](#). 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.

SEE ALSO

| [Creating a Loop from the Router to the Network | 177](#)

SEE ALSO

| [Checking for SONET Interface Error Statistics | 175](#)

| [Creating a Loop to the Router from Various Points in the Network | 178](#)

RELATED DOCUMENTATION

| [Investigating Interface Steps and Commands | 146](#)

| [Monitoring SONET Interfaces | 151](#)

| [Locating SONET Alarms and Errors | 179](#)

| [Enabling SONET Payload Scrambling | 209](#)

| [Checking the SONET Frame Checksum | 214](#)

Locating SONET Alarms and Errors

IN THIS SECTION

- [List of Common SONET Alarms and Errors | 179](#)
- [Displaying SONET Alarms and Errors | 181](#)
- [Locating Most Common SONET Alarms and Errors | 185](#)
- [Locating Loss of Signal Alarms | 186](#)
- [Locating Alarm Indication Signal Alarms | 188](#)
- [Locating Remote Defect Indication Alarms | 191](#)
- [Locating Remote Error Indication Line Errors | 193](#)
- [Locating Bit Error Rate Alarms | 196](#)
- [Locating Payload Label Mismatch Path Alarms | 198](#)
- [Locating Loss of Pointer Path Alarms | 201](#)
- [Locating Unequipped Payload Alarms | 203](#)
- [Locating Phase Lock Loop Alarms | 205](#)

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 23 on page 179](#) provides links and commands for checking SONET alarms and errors.

Table 23: List of Common SONET Alarms and Errors

Tasks	Command or Action
“Displaying SONET Alarms and Errors” on page 181	<code>show interfaces so-fpc/pic/port extensive</code>
“Locating Most Common SONET Alarms and Errors” on page 185	

Table 23: List of Common SONET Alarms and Errors (*continued*)

Tasks	Command or Action
1. Locating Loss of Signal Alarms on page 186	Check the connection between the router port and the first SONET network element.
2. Locating Alarm Indication Signal Alarms on page 188	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. Locating Remote Defect Indication Alarms on page 191	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. Locating Remote Error Indication Line Errors on page 193	Upstream from the router, check the line-terminating equipment and path-terminating equipment for an error in the B2 or B3 byte.
5. Locating Bit Error Rate Alarms on page 196	Check the following: <ul style="list-style-type: none"> • Optical fiber • Optical transmitter and receiver • Clocking • Attenuation in the optical signal
6. Locating Payload Label Mismatch Path Alarms on page 198	Check the received and transmitted C2 byte.
7. Locating Loss of Pointer Path Alarms on page 201	Check that both sides of the connection are configured for concatenate mode or nonconcatenate mode.
8. Locating Unequipped Payload Alarms on page 203	Check provisioning with the SONET provider, and if possible, check the configuration of the add/drop multiplexer (ADM).
9. Locating Phase Lock Loop Alarms on page 205	Investigate the timing source, and configure the clocking to external or internal depending on the situation.

SEE ALSO

[Displaying SONET Alarms and Errors | 181](#)

[Locating Most Common SONET Alarms and Errors | 185](#)

[Locating Loss of Signal Alarms | 186](#)

Locating Alarm Indication Signal Alarms	188
Locating Remote Defect Indication Alarms	191
Locating Remote Error Indication Line Errors	193
Locating Bit Error Rate Alarms	196
Locating Payload Label Mismatch Path Alarms	198
Locating Loss of Pointer Path Alarms	201
Locating Unequipped Payload Alarms	203
Locating Phase Lock Loop Alarms	205

Displaying 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...]

```

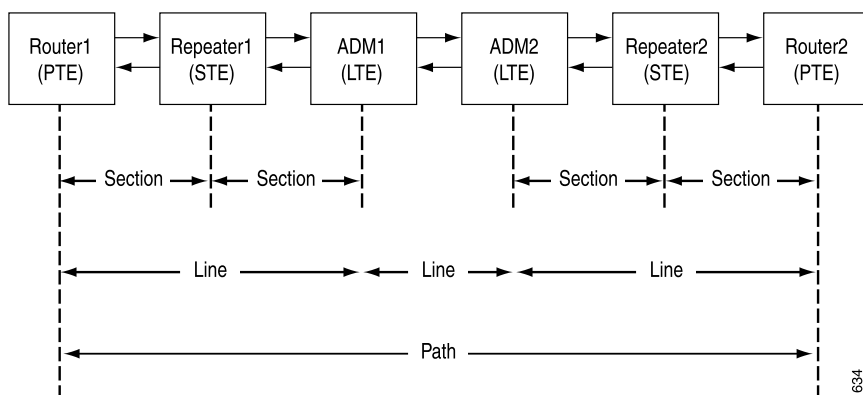
Meaning

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 5 on page 183](#) shows an example of a SONET network with the section, line, and path areas delimited. [Figure 5 on page 183](#) 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 5: 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 and Router 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.

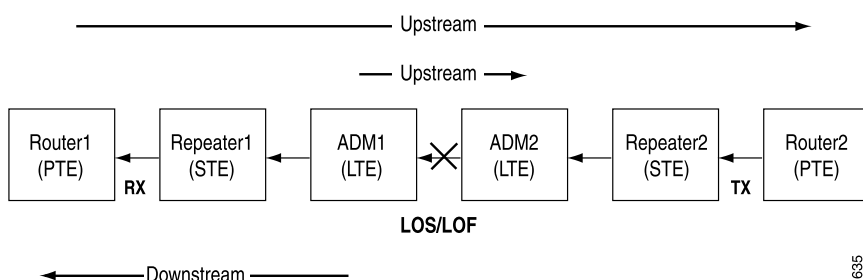
- The main role of an LTE is to read the line overhead bytes. However, it also reads the section overhead bytes. Therefore the LTE also plays the role of an STE.
- An STE reads only the section overhead bytes of the SONET frame. (See [Figure 6 on page 184.](#))

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 6 on page 184](#) 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.

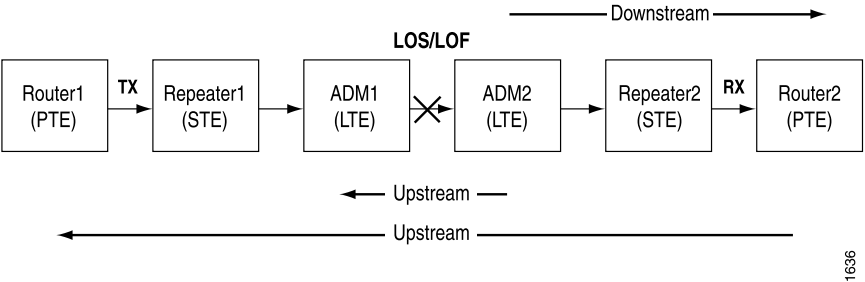
Figure 6: Example of an Upstream or Downstream Failure



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 7 on page 185](#), 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 7: 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.

SEE ALSO

- [List of Common SONET Alarms and Errors | 179](#)
- [Locating Most Common SONET Alarms and Errors | 185](#)
- [Locating Loss of Signal Alarms | 186](#)
- [Locating Alarm Indication Signal Alarms | 188](#)
- [Locating Remote Defect Indication Alarms | 191](#)
- [Locating Remote Error Indication Line Errors | 193](#)
- [Locating Bit Error Rate Alarms | 196](#)
- [Locating Payload Label Mismatch Path Alarms | 198](#)
- [Locating Loss of Pointer Path Alarms | 201](#)
- [Locating Unequipped Payload Alarms | 203](#)
- [Locating Phase Lock Loop Alarms | 205](#)

Locating Most Common SONET Alarms and Errors

Problem

Description: 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:

- [Locating Loss of Signal Alarms on page 186](#)
- [Locating Alarm Indication Signal Alarms on page 188](#)
- [Locating Remote Defect Indication Alarms on page 191](#)
- [Locating Remote Error Indication Line Errors on page 193](#)
- [Locating Bit Error Rate Alarms on page 196](#)
- [Locating Payload Label Mismatch Path Alarms on page 198](#)
- [Locating Loss of Pointer Path Alarms on page 201](#)
- [Locating Unequipped Payload Alarms on page 203](#)
- [Locating Phase Lock Loop Alarms on page 205](#)

SEE ALSO

List of Common SONET Alarms and Errors 179
Displaying SONET Alarms and Errors 181
Locating Loss of Signal Alarms 186
Locating Alarm Indication Signal Alarms 188
Locating Remote Defect Indication Alarms 191
Locating Remote Error Indication Line Errors 193
Locating Bit Error Rate Alarms 196
Locating Payload Label Mismatch Path Alarms 198
Locating Loss of Pointer Path Alarms 201
Locating Unequipped Payload Alarms 203
Locating Phase Lock Loop Alarms 205

Locating Loss of Signal Alarms

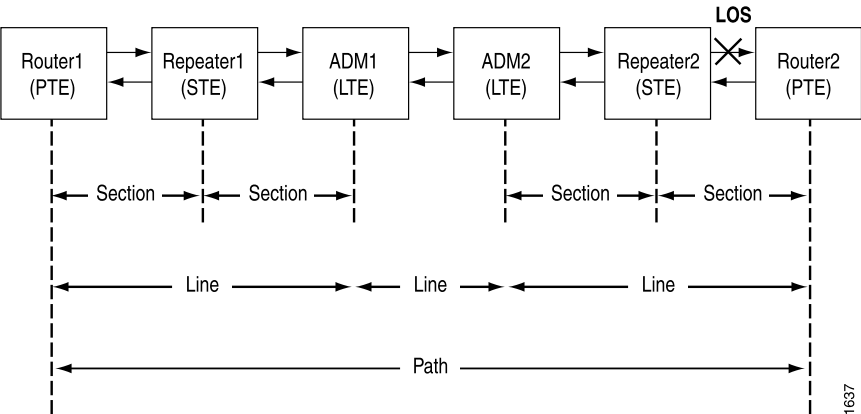
Problem

Description: 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 8 on page 187](#), the X indicates that there is a connection problem between Repeater 2 and Router 2.

Figure 8: 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.

SEE ALSO

Displaying SONET Alarms and Errors	181
Locating Most Common SONET Alarms and Errors	185
Locating Alarm Indication Signal Alarms	188
Locating Remote Defect Indication Alarms	191
Locating Remote Error Indication Line Errors	193
Locating Bit Error Rate Alarms	196
Locating Payload Label Mismatch Path Alarms	198
Locating Loss of Pointer Path Alarms	201
Locating Unequipped Payload Alarms	203
Locating Phase Lock Loop Alarms	205

Locating 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 | 188](#)
 2. [Example of a Router Receiving Both an AIS-L and AIS-P Alarm | 189](#)

Example of a Router Receiving Only an AIS-P Alarm

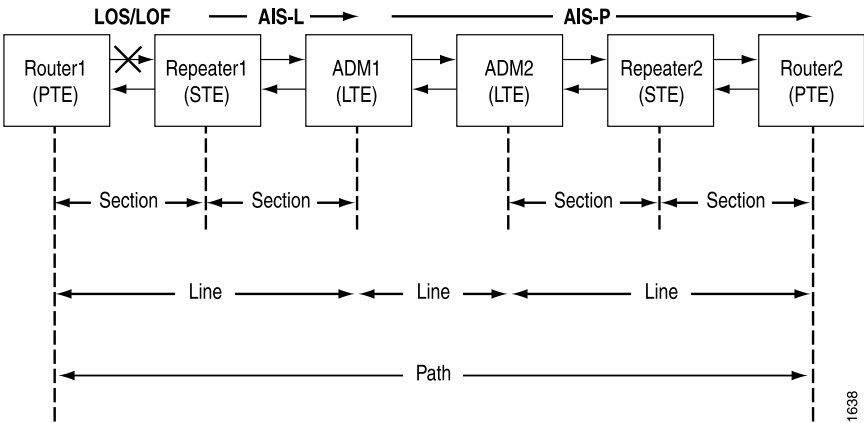
Problem

Description: [Figure 9 on page 189](#) 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 9: Example of a Router Receiving Only an AIS-P Alarm



Meaning

In [Figure 9 on page 189](#), 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.

SEE ALSO

[Example of a Router Receiving Both an AIS-L and AIS-P Alarm | 189](#)

Example of a Router Receiving Both an AIS-L and AIS-P Alarm

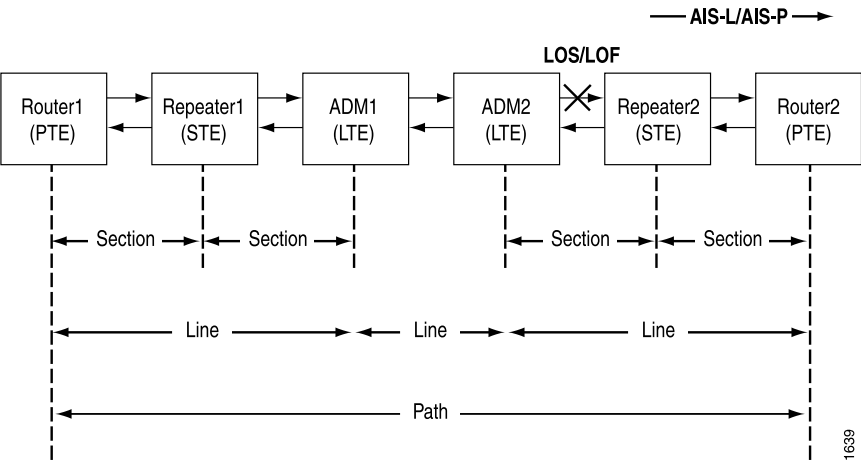
Problem

Description: [Figure 10 on page 190](#) shows a router receiving both an AIS-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 10: Example of a Router Receiving Both an AIS-L and an AIS-P Alarm



What It Means

In [Figure 10 on page 190](#), 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.

SEE ALSO

| [Example of a Router Receiving Only an AIS-P Alarm | 188](#)

SEE ALSO

	List of Common SONET Alarms and Errors 179
	Displaying SONET Alarms and Errors 181
	Locating Most Common SONET Alarms and Errors 185
	Locating Loss of Signal Alarms 186
	Locating Remote Defect Indication Alarms 191
	Locating Remote Error Indication Line Errors 193
	Locating Bit Error Rate Alarms 196
	Locating Payload Label Mismatch Path Alarms 198
	Locating Loss of Pointer Path Alarms 201

Locating 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.

1. [Example of a Router Receiving Only an RDI-P Alarm | 191](#)
2. [Example of a Router Receiving Both an RDI-L and RDI-P Alarm | 192](#)

Example of a Router Receiving Only an RDI-P Alarm

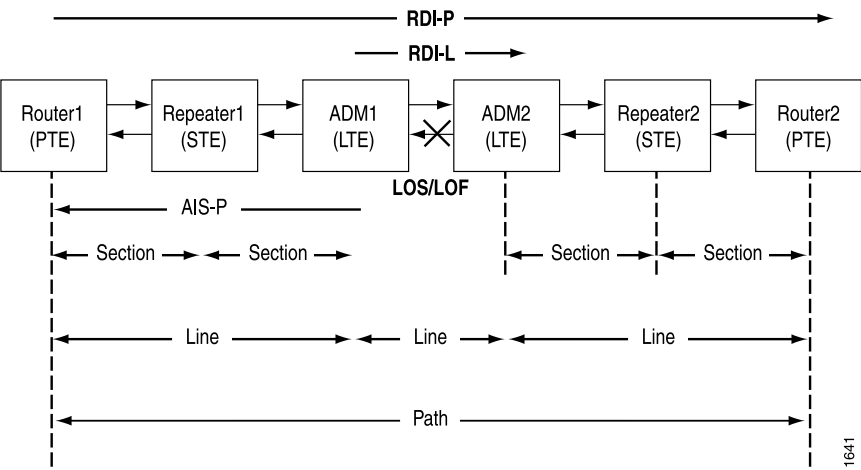
Problem

Description: [Figure 11 on page 191](#) 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 11: Example of a Router Receiving Only an RDI-P Alarm



What It Means

In [Figure 11 on page 191](#), 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.

SEE ALSO

[Example of a Router Receiving Both an RDI-L and RDI-P Alarm | 192](#)

[Locating Remote Defect Indication Alarms | 191](#)

Example of a Router Receiving Both an RDI-L and RDI-P Alarm

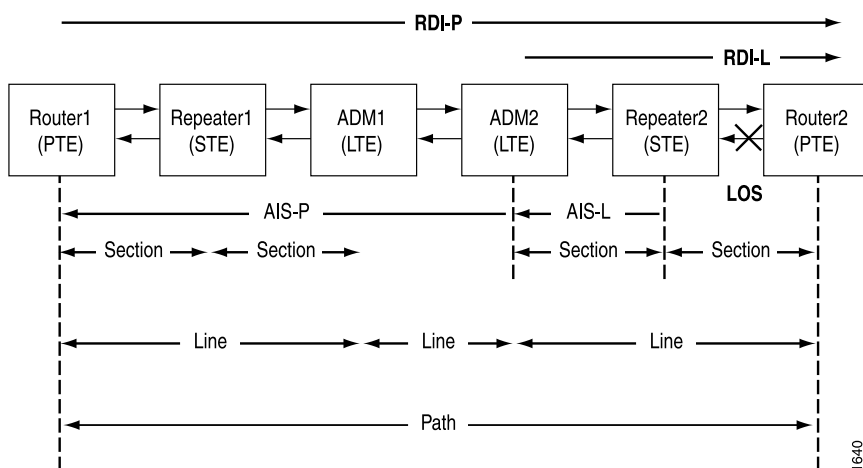
Problem

Description: Figure 12 on page 192 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 12: Example of a Router Receiving Both an RDI-L and RDI-P Alarm



Meaning

In Figure 12 on page 192, 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.

SEE ALSO

[Example of a Router Receiving Only an RDI-P Alarm | 191](#)
[Locating Remote Defect Indication Alarms | 191](#)

SEE ALSO

[List of Common SONET Alarms and Errors | 179](#)
[Displaying SONET Alarms and Errors | 181](#)
[Locating Most Common SONET Alarms and Errors | 185](#)
[Locating Loss of Signal Alarms | 186](#)
[Locating Alarm Indication Signal Alarms | 188](#)
[Locating Remote Error Indication Line Errors | 193](#)
[Locating Bit Error Rate Alarms | 196](#)
[Locating Payload Label Mismatch Path Alarms | 198](#)
[Locating Loss of Pointer Path Alarms | 201](#)
[Locating Unequipped Payload Alarms | 203](#)
[Locating Phase Lock Loop Alarms | 205](#)

Locating 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 | 194](#)
 2. [Example of Both REI-L and REI-P Counters Incrementing | 194](#)

Example of Only an REI-P Counter Incrementing

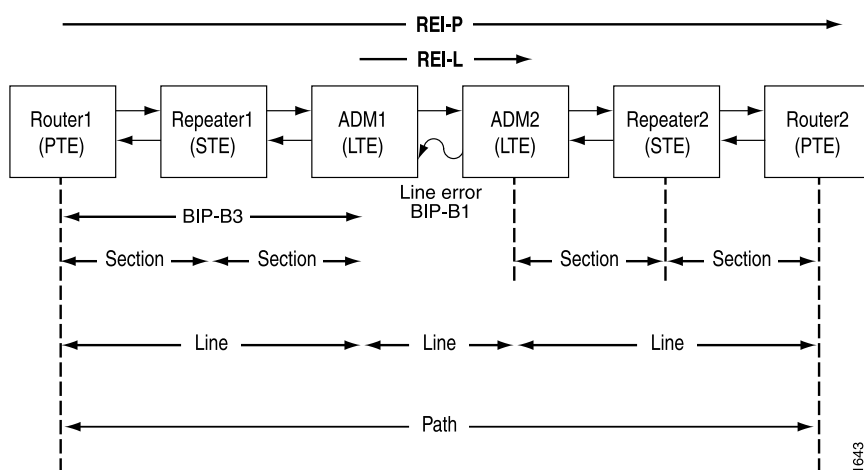
Problem

Description: Figure 13 on page 194 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 13: Example of a Router Receiving Only an REI-P Counter Incrementing



Meaning

In Figure 13 on page 194, 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.

SEE ALSO

[Example of Both REI-L and REI-P Counters Incrementing](#) | 194

Example of Both REI-L and REI-P Counters Incrementing

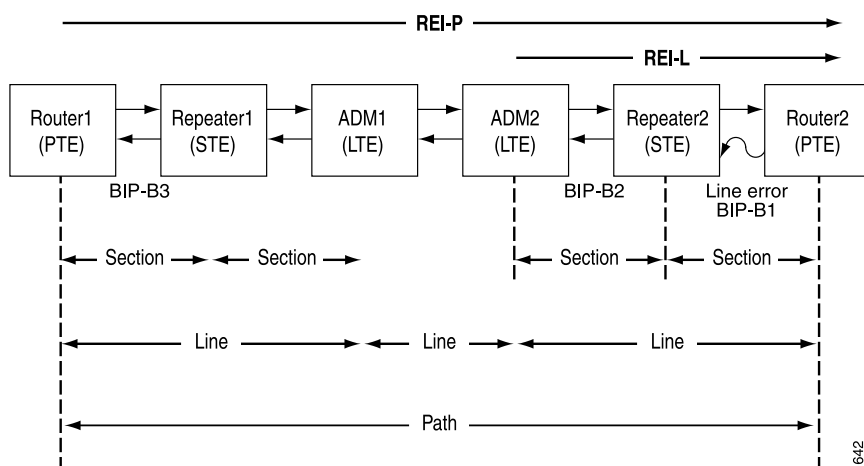
Problem

Description: Figure 14 on page 195 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 14: Example of a Router Receiving Both An REI-L and REI-P Counter Incrementing



Meaning

In Figure 14 on page 195, 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.

SEE ALSO

[Example of Only an REI-P Counter Incrementing | 194](#)

SEE ALSO

[List of Common SONET Alarms and Errors | 179](#)

Displaying SONET Alarms and Errors 181
Locating Most Common SONET Alarms and Errors 185
Locating Loss of Signal Alarms 186
Locating Alarm Indication Signal Alarms 188
Locating Remote Defect Indication Alarms 191
Locating Bit Error Rate Alarms 196
Locating Payload Label Mismatch Path Alarms 198
Locating Loss of Pointer Path Alarms 201
Locating Unequipped Payload Alarms 203
Locating Phase Lock Loop Alarms 205

Locating Bit Error Rate Alarms

Problem

Description: 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

SEE ALSO

List of Common SONET Alarms and Errors 179
Displaying SONET Alarms and Errors 181
Locating Most Common SONET Alarms and Errors 185
Locating Loss of Signal Alarms 186
Locating Alarm Indication Signal Alarms 188
Locating Remote Defect Indication Alarms 191
Locating Remote Error Indication Line Errors 193
Locating Payload Label Mismatch Path Alarms 198
Locating Loss of Pointer Path Alarms 201
Locating Unequipped Payload Alarms 203
Locating Phase Lock Loop Alarms 205

Locating Payload Label Mismatch Path Alarms

Problem

Description: Payload mismatch path (PLM-P; also called signal label mismatch) 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 **0xcf**, the transmitted C2 value must also be **0xcf**.

NOTE: When the received C2 byte has a value of **0x01**—indicating *equipped-nonspecific payload*—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 24 on page 200](#) shows the synchronous transport signal (STS) path signal label assignments as described in Issue 3 (Sept. 2000) of the GR-253 CORE.

Table 24: 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)
```

SEE ALSO

List of Common SONET Alarms and Errors 179
Displaying SONET Alarms and Errors 181
Locating Most Common SONET Alarms and Errors 185
Locating Loss of Signal Alarms 186
Locating Alarm Indication Signal Alarms 188
Locating Remote Defect Indication Alarms 191
Locating Remote Error Indication Line Errors 193
Locating Bit Error Rate Alarms 196
Locating Loss of Pointer Path Alarms 201
Locating Unequipped Payload Alarms 203
Locating Phase Lock Loop Alarms 205

Locating Loss of Pointer Path Alarms

Problem

Description: 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 Networks routers do not report pointer adjustments, an LOP-P alarm will not occur as long as the pointer adjustments stay within tolerance levels.

SEE ALSO

List of Common SONET Alarms and Errors 179
Displaying SONET Alarms and Errors 181
Locating Most Common SONET Alarms and Errors 185
Locating Loss of Signal Alarms 186
Locating Alarm Indication Signal Alarms 188
Locating Remote Defect Indication Alarms 191
Locating Remote Error Indication Line Errors 193
Locating Bit Error Rate Alarms 196
Locating Payload Label Mismatch Path Alarms 198
Locating Unequipped Payload Alarms 203
Locating Phase Lock Loop Alarms 205

Locating Unequipped Payload Alarms

Problem

Description: 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.

SEE ALSO

List of Common SONET Alarms and Errors 179
Displaying SONET Alarms and Errors 181
Locating Most Common SONET Alarms and Errors 185
Locating Loss of Signal Alarms 186
Locating Alarm Indication Signal Alarms 188
Locating Remote Defect Indication Alarms 191
Locating Remote Error Indication Line Errors 193
Locating Bit Error Rate Alarms 196
Locating Payload Label Mismatch Path Alarms 198
Locating Loss of Pointer Path Alarms 201
Locating Phase Lock Loop Alarms 205

Locating Phase Lock Loop Alarms

Problem

Description: 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 25 on page 207](#).) 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 25 on page 207](#) shows the location of the onboard clock on the various system boards of Juniper Networks routers.

Table 25: 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)

Table 25: Location of the Onboard Clock (*continued*)

Router	System Board
M40e and M160 routers	Miscellaneous Control Subsystem (MCS)
T-series routing platforms	SONET Clock Generator (SCG)

SEE ALSO

[List of Common SONET Alarms and Errors | 179](#)
[Displaying SONET Alarms and Errors | 181](#)
[Locating Most Common SONET Alarms and Errors | 185](#)
[Locating Loss of Signal Alarms | 186](#)
[Locating Alarm Indication Signal Alarms | 188](#)
[Locating Remote Defect Indication Alarms | 191](#)
[Locating Remote Error Indication Line Errors | 193](#)
[Locating Bit Error Rate Alarms | 196](#)
[Locating Payload Label Mismatch Path Alarms | 198](#)
[Locating Loss of Pointer Path Alarms | 201](#)
[Locating Unequipped Payload Alarms | 203](#)

RELATED DOCUMENTATION

[Investigating Interface Steps and Commands | 146](#)
[Monitoring SONET Interfaces | 151](#)
[Using Loopback Testing for SONET Interfaces | 162](#)
[Enabling SONET Payload Scrambling | 209](#)
[Checking the SONET Frame Checksum | 214](#)

Enabling SONET Payload Scrambling

IN THIS SECTION

- [Checklist for Enabling SONET Payload Scrambling | 209](#)
- [Understanding SONET Payload Scrambling | 209](#)

This section includes the following information to assist you when troubleshooting SONET interfaces:

Checklist for Enabling SONET Payload Scrambling

[Table 26 on page 209](#) provides links and commands for SONET payload scrambling and how to check and configure it.

Table 26: Checklist for Enabling SONET Payload Scrambling

Tasks	Command or Action
“Understanding SONET Payload Scrambling” on page 209	
1. Checking SONET HDLC Payload Scrambling on page 210	<code>show configuration interfaces interface-name</code> <code>show interfaces interface-name</code>
2. Configuring SONET HDLC Payload Scrambling on page 213	<code>[edit]</code> <code>edit interfaces so-fpc/pic/port sonet-options</code> <code>set payload-scrambler</code> <code>show</code> <code>commit</code>

SEE ALSO

[Understanding SONET Payload Scrambling | 209](#)

Understanding 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 $1 + x^6 + x^7$ 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 *Junos OS Network Interfaces Library for Routing Devices*.

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. [Checking SONET HDLC Payload Scrambling | 210](#)
2. [Configuring SONET HDLC Payload Scrambling | 213](#)

Checking 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 10.0.0.2/32 {  
            destination 10.0.0.1;  
        }  
    }  
    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 10.0.0.2/32 {  
            destination 10.0.0.1;  
        }  
    }  
    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 [“Configuring SONET HDLC Payload Scrambling” on page 213](#).

SEE ALSO

| [Configuring SONET HDLC Payload Scrambling](#) | 213

Configuring 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.

```
[edit interfaces interface-name sonet-options]
user@host# show
payload-scrambler;
```

4. Commit the configuration.

```
user@host# commit
```

SEE ALSO

[Checking SONET HDLC Payload Scrambling](#) | 210

SEE ALSO

| [Checklist for Enabling SONET Payload Scrambling](#) | 209

RELATED DOCUMENTATION

	Investigating Interface Steps and Commands 146
	Monitoring SONET Interfaces 151
	Using Loopback Testing for SONET Interfaces 162
	Locating SONET Alarms and Errors 179
	Checking the SONET Frame Checksum 214

Checking the SONET Frame Checksum

IN THIS SECTION

- [Checklist for Checking the SONET Frame Checksum](#) | 214
- [Understand the SONET Frame Checksum](#) | 215
- [Checking the SONET Frame Checksum](#) | 216
- [Configuring a SONET Frame Checksum](#) | 222

This section includes the following information to assist you when troubleshooting SONET interfaces:

Checklist for Checking the SONET Frame Checksum

Purpose

To check and configure SONET frame checksum.

Action

[Table 27 on page 215](#) provides the links and commands for SONET frame checksum.

Table 27: Checklist for Checking the SONET Frame Checksum

Tasks	Command or Action
“Understand the SONET Frame Checksum” on page 33	
“Checking the SONET Frame Checksum” on page 216	
1. Examining Output for Framing Errors on page 216	<code>show interfaces <i>interface-name</i> extensive</code>
2. Checking the FCS Configuration on page 219	<code>show configuration interfaces <i>interface-name</i></code> <code>show interfaces <i>interface-name</i></code>
“Configuring a SONET Frame Checksum” on page 222	
1. Returning to the Default 16-Bit Checksum on page 222	<code>[edit]</code> <code>edit interfaces <i>so-fpc/pic/port</i> sonet-options</code> <code>delete fcs 32</code> <code>show</code> <code>commit</code>
2. Configuring a 16-Bit Checksum on page 223	<code>[edit]</code> <code>edit interfaces <i>so-fpc/pic/port</i> sonet-options</code> <code>set fcs 16</code> <code>show</code> <code>commit</code>
3. Configuring a 32-Bit Checksum on page 224	<code>[edit]</code> <code>edit interfaces <i>so-fpc/pic/port</i> sonet-options</code> <code>set (fcs 32 rfc-2615)</code> <code>show</code> <code>commit</code>

SEE ALSO

[Checking the SONET Frame Checksum | 216](#)[Configuring a SONET Frame Checksum | 222](#)

Understand the SONET Frame Checksum

Problem

Description: The SONET frame checksum is a calculation that is added to a frame for error control purposes. SONET frame checksum is used in High-Level Data Link Control (HDLC), Frame Relay, and other data-link

layer protocols. For example, Router A calculates the frame check sequence (FCS) and adds it to the outgoing message. Router B, on receiving the message recalculates the FCS and compares it to the FCS from Router A. If there is a difference, both sides of the connection might not match in relation to the FCS configuration.

Solution

If you are having problems with a connection, check whether the FCS matches on both sides of the connection. To check the SONET frame checksum, see [“Checking the SONET Frame Checksum” on page 216](#).

After you have checked the FCS and determined that a problem exists, you must configure a SONET frame checksum. For more information, see [“Configuring a SONET Frame Checksum” on page 222](#).

SEE ALSO

[Checklist for Checking the SONET Frame Checksum | 214](#)

Checking 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. [Examining Output for Framing Errors | 216](#)
2. [Checking the FCS Configuration | 219](#)

Examining 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 , 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

```



```

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 .....
HDLCD 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.

SEE ALSO

[Checking the FCS Configuration](#) | 219

Checking 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 interfacesinterface-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 10.0.0.2/32 {
            destination 10.0.0.1;
        }
    }
    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 [“Returning to the Default 16-Bit Checksum” on page 222](#), [“Configuring a 16-Bit Checksum” on page 223](#), or [“Configuring a 32-Bit Checksum” on page 224](#).

SEE ALSO

[Examining Output for Framing Errors | 216](#)

SEE ALSO

[Checklist for Checking the SONET Frame Checksum | 214](#)

[Configuring a SONET Frame Checksum | 222](#)

Configuring a SONET Frame Checksum

IN THIS SECTION

- [Returning to the Default 16-Bit Checksum | 222](#)
- [Configuring a 16-Bit Checksum | 223](#)
- [Configuring a 32-Bit Checksum | 224](#)

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.

Returning 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 interfaces interface-name sonet-options]
user@host# delete fcs 32
```

3. Verify the configuration.

```
[edit interfaces interface-name sonet-options]
user@host# show
```

4. Commit the configuration.


```
user@host# commit
```

SEE ALSO

[Configuring a 16-Bit Checksum | 223](#)

[Configuring a 32-Bit Checksum | 224](#)

Configuring 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.

```
[edit interfaces interface-name sonet-options]  
user@host# show  
fcs 16;
```

4. Commit the configuration.

```
user@host# commit
```

SEE ALSO

[Returning to the Default 16-Bit Checksum | 222](#)

[Configuring a 32-Bit Checksum | 224](#)

Configuring 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.

```
[edit interfaces interface-name sonet-options]
user@host# show
fcs 32;
```

or

```
[edit interfaces interface-name sonet-options]
user@host# show
rfc-2615;
```

4. 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.

SEE ALSO

[Returning to the Default 16-Bit Checksum | 222](#)

[Configuring a 16-Bit Checksum | 223](#)

SEE ALSO

[Checklist for Checking the SONET Frame Checksum | 214](#)

[Checking the SONET Frame Checksum | 216](#)

RELATED DOCUMENTATION

[Investigating Interface Steps and Commands | 146](#)

[Monitoring SONET Interfaces | 151](#)

[Using Loopback Testing for SONET Interfaces | 162](#)

[Locating SONET Alarms and Errors | 179](#)

[Enabling SONET Payload Scrambling | 209](#)

4

PART

Configuration Statements and Operational Commands

Configuration Statements | **227**

Operational Commands | **320**

Configuration Statements

IN THIS CHAPTER

- [advertise-interval](#) | 229
- [aggregate \(SONET/SDH\)](#) | 230
- [aggregate-ports](#) | 231
- [aggregated-sonet-options](#) | 232
- [annex](#) | 233
- [aps](#) | 234
- [atm-options](#) | 236
- [authentication-key](#) | 238
- [bytes](#) | 239
- [clocking](#) | 241
- [container-devices](#) | 242
- [container-list](#) | 243
- [container-options](#) | 244
- [container-type](#) | 245
- [encapsulation \(Container Interface\)](#) | 246
- [encapsulation \(Logical Interface\)](#) | 247
- [family](#) | 252
- [fast-aps-switch](#) | 258
- [fcs](#) | 260
- [filter](#) | 262
- [force](#) | 264
- [framing](#) | 265
- [framing \(SONET and SDH Interfaces\)](#) | 266
- [hold-time \(Physical Interface\)](#) | 268
- [hold-time \(APS\)](#) | 270
- [hold-time \(SONET/SDH Defect Triggers\)](#) | 271
- [ignore](#) | 273
- [link-speed \(Aggregated SONET/SDH\)](#) | 274

- [lockout](#) | 275
- [loop-timing](#) | 276
- [loopback \(ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3\)](#) | 277
- [member-interface-speed](#) | 279
- [member-interface-type](#) | 280
- [minimum-links](#) | 281
- [mpls \(Interfaces\)](#) | 283
- [mtu](#) | 284
- [neighbor \(Automatic Protection Switching for SONET/SDH\)](#) | 288
- [overflow \(Receive Bucket\)](#) | 289
- [overflow \(Transmit Bucket\)](#) | 290
- [paired-group](#) | 291
- [passive-monitor-mode](#) | 292
- [path-trace](#) | 293
- [payload-scrambler](#) | 294
- [pop-all-labels](#) | 296
- [preserve-interface](#) | 297
- [protect-circuit](#) | 298
- [rate](#) | 299
- [receive-bucket](#) | 300
- [receive-options-packets](#) | 301
- [receive-ttl-exceeded](#) | 302
- [request](#) | 303
- [required-depth](#) | 304
- [revert-time \(Interfaces\)](#) | 305
- [rfc-2615](#) | 306
- [sonet-options](#) | 307
- [speed \(SONET/SDH\)](#) | 310
- [switching-mode](#) | 311
- [t3-options](#) | 312
- [threshold](#) | 313
- [transmit-bucket](#) | 314
- [trigger](#) | 315
- [vtmapping](#) | 317

- [working-circuit](#) | 318
- [z0-increment](#) | 319

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](#) | 90

aggregate (SONET/SDH)

Syntax

```
aggregate asx;
```

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

asx—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](#) | 121

aggregate-ports

Syntax

```
aggregate-ports;
```

Hierarchy Level

```
[edit chassis fpc slot-number pic pic-number]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

For T Series routers only, specify OC768-over-OC192 mode on the 4-port OC192C PIC. Four OC192 links are aggregated into one OC768 link with one logical interface.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

[Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode](#) | 55

aggregated-sonet-options

Syntax

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

Hierarchy Level

```
[edit interfaces asx]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure aggregated SONET/SDH-specific interface properties.

The remaining statements are explained separately. See [CLI Explorer](#).

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](#) | 121

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 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.

aps

Syntax

```
aps {
  advertise-interval milliseconds;
  annex-b
  authentication-key key;
  (break-before-make | no-break-before-make);
  fast-aps-switch;
  force;
  hold-time milliseconds;
  lockout;
  neighbor address;
  paired-group group-name;
  preserve-interface;
  protect-circuit group-name;
  request;
  revert-time seconds;
  switching-mode (bidirectional | unidirectional);
  working-circuit group-name;
}
```

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 remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

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.
Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description

Configure ATM-specific physical interface properties.

The remaining statements are explained separately. Search for a statement in [CLI Explorer](#) or click a linked statement in the Syntax section for details.

 **NOTE:** Certain options apply only to specific platforms.

Required Privilege Level

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

RELATED DOCUMENTATION

<i>Interface Encapsulations Overview</i>
<i>multipoint-destination</i>
<i>shaping</i>
<i>vci</i>

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 Automatic Protect Switching | 82](#)

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 *High Availability User 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 to Identify Error Conditions | 32](#)

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.

Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

Description

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

NOTE: On Channelized SONET/SDH PICs, if you set the parent (or the master) controller clock to **external**, then you must set the child controller clocks to the default value—that is, **internal**.

For example, on the Channelized STM1 PIC, if the clock on the Channelized STM1 interface (which is the master controller) is set to **external**, then you must not configure the CE1 interface (which is the child controller) clock to **external**. Instead you must configure the CE1 interface clock to **internal**.

Options

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

interface *interface-name*—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 | 48](#)

Clock Sources on Channelized Interfaces

Configuring a Channelized T1/E1 Interface to Drop and Insert Time Slots

[loop-timing | 276](#)

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

[Displaying APS Using a Container Interface with ATM Encapsulation | 98](#)

[Configuring Container Interfaces for APS on SONET Links | 92](#)

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: **ci0**, **ci1**, and up to **ci127**.

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

[Displaying APS Using a Container Interface with ATM Encapsulation](#) | 98

[Configuring Container Interfaces for APS on SONET Links](#) | 92

[container-options](#) | 244

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

[Displaying APS Using a Container Interface with ATM Encapsulation | 98](#)

[Configuring Container Interfaces for APS on SONET Links | 92](#)

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

[Displaying APS Using a Container Interface with ATM Encapsulation](#) | 98

[Configuring Container Interfaces for APS on SONET Links](#) | 92

encapsulation (Container Interface)

Syntax

```
encapsulation (cisco-hdlc | ppp);
```

Hierarchy Level

```
[edit interfaces cin]
```

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

[Displaying APS Using a Container Interface with ATM Encapsulation | 98](#)

[Configuring Container Interfaces for APS on SONET Links | 92](#)

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 | ethernet-ccc | ethernet-vpls |
ethernet-vpls-fr | frame-relay-ccc | frame-relay-ether-type | frame-relay-ether-type-tcc | frame-relay-ppp |
frame-relay-tcc | gre-fragmentation | 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 | vxlan);
```

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]
[edit protocols evpn]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers

(**ethernet**, **vlan-ccc**, and **vlan-tcc** options only).

Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers. Only the **atm-ccc-cell-relay** and **atm-ccc-vc-mux** options are supported on ACX Series routers.

Statement introduced in Junos OS Release 17.3R1 for QFX10000 Series switches (**ethernet-ccc** and **vlan-ccc** options only).

Description

Configure a logical link-layer encapsulation type. Not all encapsulation types are supported on the switches. See the switch CLI.

Starting in Junos OS Release 20.1R1, aggregated ethernet interfaces supports VLAN TCC (Translational cross-connect) encapsulation on MX series platforms. See *Configuring VLAN TCC Encapsulation* for more details. Non-ethernet media types, SONET and ATM interfaces are only supported. It is expected that the user will have the member links of aggregated ethernet with supported hardware for configuring VLAN TCC encapsulation and no commit check is performed externally for the aggregated ethernet (AE) interfaces.

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 identifier (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 Point-to-Point (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—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over AAL5 LLC encapsulation.

atm-ppp-vc-mux—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over ATM AAL5 multiplex encapsulation.

atm-snap—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) 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—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

ether-over-atm-llc—(All IP interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) For interfaces that carry IP 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, per RFC 2427, *Multiprotocol Interconnect over Frame Relay*.

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-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces.

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.

ethernet-vpls-fr—Use in a VPLS setup when a CE device is connected to a PE router over a time-division multiplexing (TDM) link. This encapsulation type enables the PE router to terminate the outer layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

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-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 different media. The physical interface must be configured with flexible-frame-relay encapsulation.

frame-relay-ppp—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the **ppp** family only.

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

gre-fragmentation—For adaptive services interfaces only, use GRE fragmentation encapsulation to enable fragmentation of IPv4 packets in GRE tunnels. This encapsulation clears the do not fragment (DF) bit in the packet header. If the packet's size exceeds the tunnel's maximum transmission unit (MTU) value, the packet is fragmented before encapsulation.

multilink-frame-relay-end-to-end—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services, and 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—Use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface on M120 and M320 routers with Intelligent Queuing 2 (IQ2) PICs, and on MX Series routers with MPCs.

ppp-over-ether-over-atm-llc—(MX Series routers with MPCs using the ATM MIC with SFP only) For underlying ATM interfaces, 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.

vxlan—Use VXLAN data plane encapsulation for EVPN.

Required Privilege Level

interface—To view this statement in the configuration.

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

Release History Table

Release	Description
20.1R1	Starting in Junos OS Release 20.1R1, aggregated ethernet interfaces supports VLAN TCC (Translational cross-connect) encapsulation on MX series platforms.

RELATED DOCUMENTATION

Configuring Layer 2 Switching Cross-Connects Using CCC

Configuring the Encapsulation for Layer 2 Switching TCCs

Configuring Interface Encapsulation on Logical Interfaces

Configuring the CCC Encapsulation for LSP Tunnel Cross-Connects

Circuit and Translational Cross-Connects Overview

Identifying the Access Concentrator

Configuring ATM Interface Encapsulation

Configuring VLAN and Extended VLAN Encapsulation

Configuring ATM-to-Ethernet Interworking

Configuring Interface Encapsulation on PTX Series Packet Transport Routers

Configuring CCC Encapsulation for Layer 2 VPNs

Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits

Configuring ATM for Subscriber Access

Understanding CoS on ATM IMA Pseudowire Interfaces Overview

Configuring Policing on an ATM IMA Pseudowire

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 ...
    }
    bundle interface-name;
    core-facing;
    demux-destination {
        destination-prefix;
    }
    demux-source {
        source-prefix;
    }
    direct-connect;
    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;
    keep-address-and-control;
    mac-validate (loose | strict);
    max-sessions number;
    max-sessions-vs-a-ignore;
    mtu bytes;
    multicast-only;
    nd6-stale-time seconds;
    negotiate-address;
    no-neighbor-learn;
```

```

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> <filter [aci]>;
(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 dlcid dlcid-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 group-id {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-key key;
    authentication-type authentication;
    fast-interval milliseconds;
    (preempt | no-preempt) {
      hold-time seconds;
    }
    priority number;
    track {
      interface interface-name {
        bandwidth-threshold bits-per-second priority-cost priority;
        priority-cost priority;
      }
      priority-hold-time seconds;
      route prefix routing-instance instance-name priority-cost priority;
    }
  }
  virtual-address [ addresses ];
}

```



```

    }
    virtual-link-local-address ipv6-address;
  }
}

```

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-vs-a-ignore** introduced in Junos OS Release 11.4.

Description

Configure protocol family information for the logical interface.

Starting in Junos OS Release 20.1R1, aggregated ethernet interfaces supports VLAN TCC (Translational cross-connect) encapsulation on MX series platforms. See *Configuring VLAN TCC Encapsulation* for more details.

NOTE: Not all subordinate statements are available to every protocol family.

Options

family—Protocol family:

- **any**—Protocol-independent family used for Layer 2 packet filtering

NOTE: This option is not supported on T4000 Type 5 FPCs.

- **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. You can optionally configure this protocol family for the logical interface on which you configure VPLS.
- **ethernet-switching**—(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. You can configure this protocol family for the logical interface of CCC physical interfaces. When you use this encapsulation type, you can configure the **ccc** family only.
- **inet**—Internet Protocol version 4 suite. You must configure this protocol family for the logical interface to support IP protocol traffic, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Internet Control Message Protocol (ICMP), and Internet Protocol Control Protocol (IPCP).
- **inet6**—Internet Protocol version 6 suite. You must configure this protocol family for the logical interface to support IPv6 protocol traffic, including Routing Information Protocol for IPv6 (RIPng), Intermediate System-to-Intermediate System (IS-IS), BGP, and Virtual Router Redundancy Protocol for IPv6 (VRRP).
- **iso**—International Organization for Standardization Open Systems Interconnection (ISO OSI) protocol suite. You must configure this protocol family for the logical interface to support IS-IS traffic.
- **mlfr-end-to-end**—Multilink Frame Relay FRF.15. You must configure this protocol or multilink Point-to-Point Protocol (MLPPP) for the logical interface to support multilink bundling.
- **mlfr-uni-nni**—Multilink Frame Relay FRF.16. You must configure this protocol or **mlfr-end-to-end** for the logical interface to support link services and voice services bundling.
- **multilink-ppp**—Multilink Point-to-Point Protocol. You must configure this protocol (or **mlfr-end-to-end**) for the logical interface to support multilink bundling.
- **mpls**—Multiprotocol Label Switching (MPLS). You must configure this protocol family for the logical interface to participate in an MPLS path.
- **pppoe**—Point-to-Point Protocol over Ethernet
- **tcc**—Translational cross-connect protocol suite. You can configure this protocol family for the logical interface of TCC physical interfaces.

- **tnp**—Trivial Network Protocol. This protocol is used to communicate between the Routing Engine and the router’s packet forwarding components. The Junos OS automatically configures this protocol family on the router’s internal interfaces only, as discussed in *Understanding Internal Ethernet Interfaces*.
- **vpls**—(M Series and T Series routers only) Virtual private LAN service. You can optionally configure this protocol family for the logical interface on which you configure VPLS. VPLS provides an Ethernet-based point-to-multipoint Layer 2 VPN to connect customer edge (CE) routers across an MPLS backbone. When you configure a VPLS encapsulation type, the **family vpls** statement is assumed by default.

MX Series routers support dynamic profiles for VPLS pseudowires, VLAN identifier translation, and automatic bridge domain configuration.

For more information about VPLS, see the *Junos OS VPNs Library for Routing Devices*.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

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

Release History Table

Release	Description
20.1R1	Starting in Junos OS Release 20.1R1, aggregated ethernet interfaces supports VLAN TCC (Translational cross-connect) encapsulation on MX series platforms.

RELATED DOCUMENTATION

| *Configuring the Protocol Family*

fast-aps-switch

Syntax

```
fast-aps-switch;
```

Hierarchy Level

```
[edit interfaces interface-name sonet-options aps]
```

Release Information

Statement introduced in Junos OS Release 12.1.

Description

(M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only, EX Series switches, and MX series routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP only using container interfaces) Reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits.

NOTE:

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

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

Reducing APS Switchover Time in Layer 2 Circuits

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.

Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

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 NxDS3 to NxVC3 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

<i>Configuring the E1 Frame Checksum</i>
<i>Configuring the E3 Frame Checksum</i>
Configuring the SONET/SDH Frame Checksum 34
<i>Configuring the T1 Frame Checksum</i>
<i>Configuring the T3 Frame Checksum</i>

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

NOTE: On EX Series switches, the **group**, **input-list**, **output-filter** statements are not supported under the [edit interfaces *interface-name* unit *logical-unit-number* family inet], [edit interfaces *interface-name* unit *logical-unit-number* family inet6], and [edit interfaces *interface-name* unit *logical-unit-number* family mpls] hierarchies.

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. See [CLI Explorer](#).

Required Privilege Level

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

RELATED DOCUMENTATION

<i>Applying a Filter to an Interface</i>
<i>Junos OS Administration Library</i>
<i>Configuring Gigabit Ethernet Interfaces (CLI Procedure)</i>
<i>Configuring Firewall Filters (CLI Procedure)</i>
<i>family</i>

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](#) | 111

[request](#) | 303

framing

Syntax

```
framing (sdh | sonet);
```

Hierarchy Level

```
[edit chassis fpc slot-number pic pic-number],  
[edit chassis lcc number fpc slot-number pic pic-number] (Routing Matrix)
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

On SONET/SDH PICs only, configure the framing type.

Default

sonet

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 the Junos OS to Enable SONET/SDH Framing for SONET/SDH PICs](#) | 36

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

This functionality allows you to mix SONET and SDH modes on interfaces on the same PIC.

- 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.
- For 1-port OC192/STM64 MICs with XFP on MX Series routers, configure the SONET or SDH framing on the single port.

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. For per-port framing on SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP (MIC-3D-8OC3OC12-4OC48) in MX series routers, set the framing at the **[edit chassis fpc slot-number pic pic-number port port-number]** hierarchy level.

Default

Default framing mode is **SONET**.

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 Mode for Ports](#) | 18

hold-time (Physical Interface)

Syntax

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

Hierarchy Level

```
[edit interfaces interface-name],  
[edit interfaces interface-range interface-range-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 10.4R5 for EX Series switches.

Statement introduced in Junos OS Release 11.1 for the QFX Series.

Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Statement introduced in Junos OS Release 12.1 for the SRX Series.

Description

Specify the **hold-time** value to use to damp shorter interface transitions milliseconds. The hold timer enables interface damping by not advertising interface transitions until the hold timer duration has passed. When a hold-down timer is configured and the interface goes from up to down, the down hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still down, then the router begins to advertise the interface as being down. Similarly, when a hold-up timer is configured and an interface goes from down to up, the up hold-time timer is triggered. Every interface transition that occurs during the hold-time is ignored. When the timer expires and the interface state is still up, then the router begins to advertise the interface as being up.

NOTE:

- We recommend that you configure the **hold-time** value after determining an appropriate value by performing repeated tests in the actual hardware environment. This is because the appropriate value for **hold-time** depends on the hardware (XFP, SFP, SR, ER, or LR) used in the networking environment.
- The **hold-time** option is not available for controller interfaces.

NOTE: On MX Series routers with MPC3E and MPC4E, we recommend that you do not configure the hold-down timer to be less than 1 second. On MX Series routers with MPC5EQ-100G10G (MPC5EQ) or MPC6E (MX2K-MPC6E) with 100-Gigabit Ethernet MIC with CFP2 OTN interfaces, we recommend that you do not configure the hold-down timer to be less than 3 seconds.

Default

Interface transitions are not damped.

Options

down *milliseconds*—Hold time to use when an interface transitions from up to down. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

Range: 0 through 4,294,967,295

Default: 0 (interface transitions are not damped)

up *milliseconds*—Hold time to use when an interface transitions from down to up. Junos OS advertises the transition within 100 milliseconds of the time value you specify.

Range: 0 through 4,294,967,295

Default: 0 (interface transitions are not damped)

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

[advertise-interval | 229](#)

interfaces (EX Series switches)

Physical Interface Damping Overview

[Damping Shorter Physical Interface Transitions | 52](#)

Damping Longer Physical Interface Transitions

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](#) | 90

[advertise-interval](#) | 229

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:

- When up or down hold times are applied to SONET defect triggers of a 10-Gigabit Ethernet WAN-PHY interface, only the defects generated in the WAN Interface Sublayer (WIS) are damped. Therefore, if the hold times are applied to SONET defect triggers only, a 10-Gigabit Ethernet WAN-PHY interface might be marked up or down because of the faults that are generated in other layers, such as the Physical Coding Sublayer (PCS) or Physical Medium Attachment Sublayer (PMA), 10 Gigabit Media Independent Interface (XGMII) Extender Sublayer (XGXS), and Media Access Control (MAC). To damp the interface up or down events of a 10-Gigabit Ethernet WAN-PHY interface, you need to apply up or down hold-times for the interface at the **[edit interfaces *interface-name*]** hierarchy level.
- 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 Triggers | 72](#)

[hold-time \(Physical Interface\) | 268](#)

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](#) | 72

[hold-time \(Physical Interface\)](#) | 268

link-speed (Aggregated SONET/SDH)

Syntax

```
link-speed (speed | mixed);
```

Hierarchy Level

```
[edit interfaces asx 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 Interfaces](#) | 121

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](#) | 111

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](#) | 50

[Configuring the Channelized T3 Loop Timing](#)

[clocking](#) | 241

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.

Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Metro Routers.

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.

NOTE: When configuring CE1 or CT1 interfaces on the 16-port Channelized E1/T1 MIC (MIC-3D-16CHE1-T1-CE), you must include the **loopback** statement at the **[edit interfaces *ce1-fpc/pic/port*]** hierarchy level, or **[edit interfaces *ct1-fpc/pic/port*]**

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. NxDS0 IQ interfaces do not support local loopback.

payload—For channelized T3, T1, and NxDS0 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. NxDS0 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

<i>Configuring E3 and T3 Parameters on ATM Interfaces</i>
<i>Configuring E1 Loopback Capability</i>
<i>Configuring E3 Loopback Capability</i>
Configuring SONET/SDH Loopback Capability to Identify a Problem as Internal or External 42
<i>Configuring SHDSL Operating Mode on an ATM Physical Interface</i>
<i>Configuring T1 Loopback Capability</i>
<i>Configuring T3 Loopback Capability</i>
<i>feac-loop-respond</i>

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

[Displaying APS Using a Container Interface with ATM Encapsulation](#) | 98

[Configuring Container Interfaces for APS on SONET Links](#) | 92

[container-options](#) | 244

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

[Displaying APS Using a Container Interface with ATM Encapsulation](#) | 98

[Configuring Container Interfaces for APS on SONET Links](#) | 92

[container-options](#) | 244

minimum-links

Syntax (SRX, MX, T, M, EX, QFX Series, EX4600, Qfabric System)

```
minimum-links number;
```

Hierarchy Level (EX Series)

```
[edit interfaces aex aggregated-ether-options],
[edit interfaces aex 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]
```

Hierarchy Level (QFX Series)

```
[edit interfaces aex aggregated-ether-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.

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

Statement introduced in Junos OS Release 11.1 for the QFX Series.

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: On M120, M320, MX Series, T Series, and TX Matrix routers with Ethernet interfaces, the valid range for minimum-links number is 1 through 64. 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 routers and on EX Series switches, other than EX8200 switches, the range of valid values for minimum-links number is 1 through 8. When the maximum value (8) is specified, all configured links of a bundle must be up for the bundle to be labeled up. On EX8200 switches, the range of valid values for minimum-links number is 1 through 12. When the maximum value (12) is specified, all configured links of a bundle must be up for the bundle to be labeled up. On EX4600, QFX Series and Q Fabric Systems, the range of valid values for minimum-links number is 1 through 8. When the maximum value (8) is specified, all configured links of a bundle must be up for the bundle to be labeled up.

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 Interfaces | 121](#)

Configuring Aggregated Ethernet Links (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 Library for Routing Devices

Configuring Link Aggregation

mpls (Interfaces)

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 gige-ether-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. See [CLI Explorer](#).

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

[Enabling Packet Flow Monitoring on SONET/SDH Interfaces](#) | 132

Junos OS Services Interfaces Library for Routing Devices

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],
[edit logical-systems logical-system-name protocols l2circuit local-switching interface interface-name backup-neighbor
address],
[edit logical-systems logical-system-name protocols l2circuit neighbor address interface interface-name],
[edit logical-systems logical-system-name protocols l2circuit neighbor address interface interface-name backup-neighbor
address],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols l2vpn interface
interface-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name protocols vpls],
[edit protocols l2circuit local-switching interface interface-name backup-neighbor address],
[edit protocols l2circuit neighbor address interface interface-name]
[edit protocols l2circuit neighbor address interface interface-name backup-neighbor address],
[edit routing-instances routing-instance-name protocols l2vpn interface interface-name],
[edit routing-instances routing-instance-name protocols vpls],
[edit logical-systems name protocols ospf area name interface ],
[edit logical-systems name routing-instances name protocols ospf area name interface],
[edit protocols ospf area name interface ],
[edit routing-instances name protocols ospf area name interface]
```

Release Information

Statement introduced before Junos OS Release 7.4.

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

Support for Layer 2 VPNs and VPLS introduced in Junos OS Release 10.4.

Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.

Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Support at the **[set interfaces interface-name unit logical-unit-number family ccc]** hierarchy level introduced in Junos OS Release 12.3R3 for MX Series routers.

Statement introduced in Junos OS 17.3R1 Release for MX Series Routers.

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 an integrated routing and bridging (IRB) interface or routed VLAN interface (RVI) on EX Series switches, you must configure the jumbo MTU size on the member physical interfaces of the VLAN that you have associated with the IRB interface or RVI, as well as on the IRB interface or RVI itself (the interface named `irb` or `vlan`, respectively).



CAUTION: For EX Series switches, setting or deleting the jumbo MTU size on an IRB interface or RVI while the switch is transmitting packets might cause packets to be dropped.

NOTE:

The MTU for an IRB interface is calculated by removing the Ethernet header overhead $[6(\text{DMAC})+6(\text{SMAC})+2(\text{EtherType})]$. Because, the MTU is the lower value of the MTU configured on the IRB interface and the MTU configured on the IRB's associated bridge domain IFDs or IFLs, the IRB MTU is calculated as follows:

- In case of Layer 2 IFL configured with the **flexible-vlan-tagging** statement, the IRB MTU is calculated by including 8 bytes overhead (SVLAN+CVLAN).
- In case of Layer 2 IFL configured with the **vlan-tagging** statement, the IRB MTU is calculated by including a single VLAN 4 bytes overhead.

NOTE:

- If a packet whose size is larger than the configured MTU size is received on the receiving interface, the packet is eventually dropped. The value considered for MRU (maximum receive unit) size is also the same as the MTU size configured on that interface.
- 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.
- On ACX Series routers, you can configure the protocol MTU by including the **mtu** statement at the **[edit interfaces interface-name unit logical-unit-number family inet]** or **[edit interfaces interface-name unit logical-unit-number family inet6]** hierarchy level.
 - If you configure the protocol MTU at any of these hierarchy levels, the configured value is applied to all families that are configured on the logical interface.
 - If you are configuring the protocol MTU for both **inet** and **inet6** families on the same logical interface, you must configure the same value for both the families. It is not recommended to configure different MTU size values for **inet** and **inet6** families that are configured on the same logical interface.
- Starting in Release 14.2, MTU for IRB interfaces is calculated by removing the Ethernet header overhead (**6(DMAC)+6(SMAC)+2(EtherType)**), and the MTU is a minimum of the two values:
 - Configured MTU
 - Associated bridge domain's physical or logical interface MTU
 - For Layer 2 logical interfaces configured with **flexible-vlan-tagging**, IRB MTU is calculated by including 8 bytes overhead (**SVLAN+CVLAN**).
 - For Layer 2 logical interfaces configured with **vlan-tagging**, IRB MTU is calculated by including single VLAN 4 bytes overhead.

NOTE: Changing the Layer 2 logical interface option from **vlan-tagging** to **flexible-vlan-tagging** or vice versa adjusts the logical interface MTU by 4 bytes with the existing MTU size. As a result, the Layer 2 logical interface is deleted and re-added, and the IRB MTU is re-computed appropriately.

For more information about configuring MTU for specific interfaces and router or switch combinations, see ["Configuring the Media MTU" on page 14](#).

Options

bytes—MTU size.

Range: 256 through 9192 bytes, 256 through 9216 (EX Series switch interfaces), 256 through 9500 bytes (Junos OS 12.1X48R2 for PTX Series routers), 256 through 9500 bytes (Junos OS 16.1R1 for MX Series routers)

NOTE: Starting in Junos OS Release 16.1R1, the MTU size for a media or protocol is increased from 9192 to 9500 for Ethernet interfaces on the following MX Series MPCs:

- MPC1
- MPC2
- MPC2E
- MPC3E
- MPC4E
- MPC5E
- MPC6E

Default: 1500 bytes (INET, INET6, and ISO families), 1448 bytes (MPLS), 1514 bytes (EX Series switch 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 | 14](#)

Configuring the MTU for Layer 2 Interfaces

Setting the Protocol MTU

neighbor (Automatic Protection Switching for SONET/SDH)

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 Automatic Protect Switching](#) | 82

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 to Reduce Network Congestion](#) | 57

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 to Reduce Network Congestion](#) | 57

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 | 102](#)

[working-circuit | 318](#)

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

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.

This statement is supported on ATM, Ethernet, and SONET/SDH interfaces. For more information, see *ATM Interfaces User Guide for Routing Devices*.

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 Packet Flow Monitoring on SONET/SDH Interfaces | 132](#)

multiservice-options

Junos OS Services Interfaces Library for Routing Devices

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 for a Circuit](#) | 46

[sonet-options](#) | 307

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 for Link Stability | 47](#)

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.

Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

Description

For passive monitoring on ATM, SONET/SDH, Fast Ethernet, and Gigabit Ethernet interfaces only, removes up to two MPLS labels from incoming IP packets. For passive monitoring on T Series devices, removes up to five MPLS labels from incoming IP packets. For passive monitoring on MX Series routers with MPCs, all labels are popped by default and the **required-depth** statement is ignored.

This statement has no effect on IP packets with more than two MPLS labels, or IP packets with more than five MPLS labels on T Series devices. 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. See [CLI Explorer](#).

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

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

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 Automatic Protect Switching | 82](#)

[working-circuit | 318](#)

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 to Reduce Network Congestion](#) | 57

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 remaining statements are explained separately. See [CLI Explorer](#).

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 to Reduce Network Congestion](#) | 57
[transmit-bucket](#) | 314

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 Packet Flow Monitoring on SONET/SDH Interfaces](#) | 132

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 Packet Flow Monitoring on SONET/SDH Interfaces](#) | 132

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](#) | 111

[force](#) | 264

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 gige-ether-options mpls pop-all-labels]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Statement introduced in Junos OS Release 12.2 for ACX Series Universal Metro Routers.

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

[Enabling Packet Flow Monitoring on SONET/SDH Interfaces](#) | 132

Junos OS Services Interfaces Library for Routing Devices

revert-time (Interfaces)

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](#) | 113

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 PPP Support on SONET/SDH Interfaces](#) | 66

sonet-options

Syntax

```
sonet-options {
  aps {
    advertise-interval milliseconds;
    annex-b
    authentication-key key;
    (break-before-make | no-break-before-make);
    fast-aps-switch;
    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 remaining statements are explained separately. See [CLI Explorer](#).

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

[SONET/SDH Interfaces Overview | 2](#)

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.

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, set the port speed at the **[edit chassis fpc slot-number pic pic-number port port-number]** hierarchy level.

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

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

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 remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

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 to Reduce Network Congestion](#) | 57

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 remaining statements are explained separately. See [CLI Explorer](#).

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 to Reduce Network Congestion](#) | 57
[receive-bucket](#) | 300

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 (signal) label mismatch
- **rfl-l**—Line remote failure indication

- **rfi-p**—Path remote failure indication
- **uneq-p**—Path unequipped

The remaining statements are explained separately. See [CLI Explorer](#).

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](#) | 72

vtmapping

Syntax

```
vtmapping (itu-t | klm);
```

Hierarchy Level

```
[edit chassis fpc number pic number],  
[edit interfaces interface-name sonet-options]
```

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.

NOTE: The **vtmapping** statement is not supported for **cau4** interfaces on the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP (H).

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

Configuring the Junos OS to Support Channelized STM1 Interface Virtual Tributary Mapping

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 Automatic Protect Switching | 82](#)
[protect-circuit | 298](#)

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.

Default

no-Z0-increment

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 to Interoperate with Older Equipment in SDH Mode | 21](#)
[sonet-options | 307](#)

Operational Commands

IN THIS CHAPTER

- [show aps | 321](#)
- [show interfaces \(Aggregated SONET/SDH\) | 326](#)
- [show interfaces \(SONET/SDH\) | 336](#)
- [show interfaces diagnostics optics \(SONET\) | 373](#)

show aps

Syntax

```
show aps
<brief | detail | extensive | summary>
<group group | interface so-fpc/pic/port>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display information about Automatic Protection Switching (APS) for SONET configurations and about Multiplex Section Protection (MSP) for SDH configurations.

Options

none—(Same as brief) Display brief information about APS or MSP for all groups and SONET/SDH interfaces.

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

group *group*—(Optional) Display APS or MSP information for the specified group.

interface *so-fpc/pic/port*—(Optional) Display APS information for the specified SONET/SDH interface.

Required Privilege Level

view

RELATED DOCUMENTATION

[Automatic Protection Switching and Multiplex Section Protection Overview | 76](#)

List of Sample Output

[show aps on page 324](#)

[show aps brief on page 324](#)

[show aps detail on page 324](#)

[show aps extensive on page 324](#)

Output Fields

[Table 28 on page 322](#) lists the output fields for the **show aps** command. Output fields are listed in the approximate order in which they appear.

Table 28: show aps Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the SONET/SDH interface.	All levels
Group	Group name.	All levels
Circuit	Circuit type: Working or Protect .	All levels
Intf state	<p>State of the circuit and interface in the format <i>circuit-state</i>, <i>interface-state</i>:</p> <p>For <i>circuit-state</i>:</p> <ul style="list-style-type: none"> • enabled • disabled • invalid • unknown <p>For <i>interface-state</i>:</p> <ul style="list-style-type: none"> • admin down • degraded • down • invalid • nonexistent • unknown • up 	All levels
Neighbor	Address and state of neighbor interface. If the working and protect interfaces are on the same router, the neighbor address is displayed as 0.0.0.0.	detail extensive
adj	<p>State of the neighbor adjacency:</p> <ul style="list-style-type: none"> • Down • Init • Invalid • Unknown • Up 	detail extensive
neighbor interface	State of the neighbor interface: enabled or disabled .	detail extensive
dead	Number of seconds before the neighbor is declared dead	detail extensive

Table 28: show aps Output Fields (*continued*)

Field Name	Field Description	Level of Output
Channel state	Circuit that has been selected: Working or Protect . On SDH configurations using Multiplex Section Protection (MSP), the APS Annex B (G.841) Lockout status is also shown in extensive output.	detail extensive
Local-mode	Mode in which the local router is configured to interoperate with SONET line-terminating equipment (LTE): unidirectional or bidirectional . The parenthetical value represents the mode type in the K2 byte.	extensive
neighbor-mode	Mode in which the neighboring device is operating: unidirectional or bidirectional . The parenthetical value represents the mode type in the K2 byte.	extensive
Protect circuit is on	Interface name of the APS protect circuit, displayed when both the working circuit and protect circuit are on the same router.	detail extensive
Working circuit is on	Interface name of the APS working circuit, displayed when both the working circuit and protect circuit are on the same router.	detail extensive
Req K1	Value of the SONET/SDH K1 byte requested to be transmitted by this circuit.	extensive
rcv K1	Value of the SONET/SDH K1 byte received on this interface. (Valid only on the protect circuit.)	extensive
xmit K1	Value of the SONET/SDH K1 byte being transmitted on this interface. (Valid only on the protect circuit.)	extensive
nbr K1	Value of the SONET/SDH K1 byte requested to be transmitted by the neighbor.	extensive
nbr paired req	Nonzero if the neighbor is requesting a particular K1 value because of a change in the paired circuit.	extensive
Revert time	Configured time to wait after the working circuit has become functional before making the working circuit active again.	extensive
neighbor revert time	Configured time, on the neighbor interface, to wait after the working circuit has again become functional before making the working circuit active again.	extensive
Hello due in	Time until the next hello packet is sent.	extensive

Sample Output

show aps

```
user@host> show aps
```

Interface	Group	Circuit	Intf state
so-0/0/0	aviva-aps	Working	enabled, up
so-0/0/1	aviva-aps	Protect	disabled, up

show aps brief

The output for the **show aps brief** command is identical to that for the **show aps** command. For sample output, see [show aps on page 324](#).

show aps detail

```
user@host> show aps detail
```

Interface	Group	Circuit	Intf state
so-0/0/0	aviva-aps	Working	enabled, up
Neighbor 0.0.0.0, adj up, neighbor interface disabled, dead 2.987			
so-0/0/1	aviva-aps	Protect	disabled, up
Neighbor 0.0.0.0, adj up, neighbor interface enabled, dead 2.147			

show aps extensive

The following sample shows output from a SONET configuration:

```
user@host> show aps extensive
```

Interface	Group	Circuit	Intf state
so-0/0/0	aviva-aps	Working	enabled, up
Neighbor 0.0.0.0, adj up, neighbor interface disabled, dead 2.511			
Channel state Working			
Protect circuit is on interface so-0/0/1			
Local-mode bidirectional(5), neighbor-mode bidirectional(5)			
Req K1 0x00, rcv K1 0x00, xmit K1 0x00, nbr K1 0x00, nbr paired req 0			
Revert time 0, neighbor revert time 0			
Hello due in 0.055			
so-0/0/1	aviva-aps	Protect	disabled, up
Neighbor 0.0.0.0, adj up, neighbor interface enabled, dead 2.230			
Channel state Working			
Working circuit is on interface so-0/0/0			

```

Local-mode bidirectional(5), neighbor-mode bidirectional(5)
Req K1 0x00, rcv K1 0x00, xmit K1 0x00, nbr K1 0x00, nbr paired req 0
Revert time 0, neighbor revert time 0
Hello due in 0.416

```

The following sample shows output from an SDH configuration:

user@host> **show aps extensive**

```

Interface      Group              Circuit      Intf state
cstm4-1/1/0    TO_MALIBU          Working      enabled, up
Neighbor 0.0.0.0, adj up, neighbor interface disabled, dead 2.833
Channel state Working, annex-b, lockout
Protect circuit is on interface cstm4-1/2/0
Local-mode bidirectional(5), neighbor-mode bidirectional(5)
Req K1 0x00, rcv K1 0x00, xmit K1 0x00, nbr K1 0x00
      , rcv K2 0x10, xmit K2 0x10, nbr paired req 0
Wait to restore time 30, neighbor wait to restore time 30
Hello due in 0.945
cstm4-1/2/0    TO_MALIBU          Protect      disabled, up
Neighbor 0.0.0.0, adj up, neighbor interface enabled, dead 2.955
Channel state Working, annex-b
Working circuit is on interface cstm4-1/1/0
Local-mode bidirectional(5), neighbor-mode bidirectional(5)
Req K1 0x00, rcv K1 0x00, xmit K1 0x00, nbr K1 0x00
      , rcv K2 0x10, xmit K2 0x10, nbr paired req 0
Wait to restore time 30, neighbor wait to restore time 30
Hello due in 0.735

```

show interfaces (Aggregated SONET/SDH)

Syntax

```
show interfaces asnumber
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified aggregated SONET/SDH interface.

Options

asnumber—Display standard information about the specified aggregated SONET/SDH interface.

brief | detail | extensive | terse—(Optional) Display brief, detail, or extensive information about the interface.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

RELATED DOCUMENTATION

[Understanding Aggregated SONET/SDH Interfaces](#) | 118

List of Sample Output

[show interfaces \(Aggregated SONET\) on page 331](#)

[show interfaces brief \(Aggregated SONET\) on page 332](#)

[show interfaces detail \(Aggregated SONET\) on page 332](#)

[show interfaces extensive \(Aggregated SONET\) on page 333](#)

Output Fields

Table 29 on page 327 lists the output fields for the **show interfaces** (aggregated SONET/SDH) command. Output fields are listed in the approximate order in which they appear.

Table 29: Aggregated SONET/SDH show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Link-level type	Encapsulation being used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Minimum links needed	Number of child links that must be operational for the aggregated interface to be operational.	detail extensive none
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Link flags	Information about the link. Possible values are described in the “Link Flags” section under <i>Common Output Fields Description</i> .	All levels

Table 29: Aggregated SONET/SDH show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Keepalive settings	<p>(PPP and HDLC) Configured settings for keepalives.</p> <ul style="list-style-type: none"> • interval seconds—The time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds. • up-count number—The number of keepalive packets a destination must receive to change a link's status from down to up. The range is 1 through 255, with a default of 1. • down-count number—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3. 	All levels
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive none
Input rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	<p>Number of bytes and packets received and transmitted on the physical interface, and the traffic rate in bits per seconds (bps).</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive

Table 29: Aggregated SONET/SDH show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Input errors	<p>Input errors on the interface whose definitions are as follows:</p> <ul style="list-style-type: none"> • Errors—Sum of the incoming frame aborts and FCS errors. • Drops—Number of packets dropped by the input 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. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Giants—Number of frames received that are larger than the giant threshold. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • Resource errors—Sum of transmit drops. 	extensive
Output errors	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • 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. • MTU errors—Number of packets whose size exceeds the MTU of the interface. • Resource errors—Sum of transmit drops. 	extensive
Egress queues	Total number of egress queues supported on the specified interface.	detail extensive

Table 29: Aggregated SONET/SDH show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Queue counters	CoS queue number and its associated user-configured forwarding class name. <ul style="list-style-type: none"> • Queued packets—Number of queued packets. • Transmitted packets—Number of transmitted packets. • Dropped packets—Number of packets dropped by the ASIC's RED mechanism. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface's index number (which reflects its initialization sequence).	detail extensive none
SNMP ifIndex	Logical interface's SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Encapsulation on the logical interface.	All levels
Bandwidth	Interface bandwidth.	detail extensive none
Statistics	Information about fragments and packets received and sent by the router. All references to traffic direction (input or output) are defined with respect to the router. Input fragments received by the router are assembled into input packets; output packets are segmented into output fragments for transmission out of the router. Statistics include input and output counts for packets, packets per second (pps), bytes, and bytes per second (Bps) for the following entities: <ul style="list-style-type: none"> • Bundle—Information about bundles. • Link—Information about links used in the multilink operation. 	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. If the protocol is inet , the source and destination address are also displayed.	brief
Protocol	Protocol family configured on the logical interface.	detail extensive none

Table 29: Aggregated SONET/SDH show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
MTU	MTU size on the logical interface.	detail extensive none
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	detail extensive
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	detail extensive

Sample Output

show interfaces (Aggregated SONET)

```
user@host> show interfaces as0
```

```
Physical interface: as0, Enabled, Physical link is Up
Interface index: 149, SNMP ifIndex: 45
Link-level type: PPP, MTU: 4474, Speed: 466560kbps, Minimum links needed: 1
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
```

```

Link flags      : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Last flapped    : Never
Input rate      : 216 bps (1 pps)
Output rate     : 48 bps (0 pps)

Logical interface as0.0 (Index 79) (SNMP ifIndex 55)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  Bandwidth: 311040kbps
  Statistics
  Bundle:
    Input :      1178      1      11772      176
    Output:         0      0         0         0
  Protocol inet, MTU: 4470
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.100.1.1, Local: 10.100.1.2

```

show interfaces brief (Aggregated SONET)

```
user@host> show interfaces as0 brief
```

```

Physical interface: as0, Enabled, Physical link is Up
Link-level type: PPP, MTU: 4474, Speed: 466560kbps
Device flags    : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags      : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3

Logical interface as0.0
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  inet  10.100.1.2      --> 10.100.1.1

```

show interfaces detail (Aggregated SONET)

```
user@host> show interfaces as0 detail
```

```

Physical interface: as0, Enabled, Physical link is Up
Interface index: 149, SNMP ifIndex: 45, Generation: 32
Link-level type: PPP, MTU: 4474, Speed: 466560kbps, Minimum links needed: 1
Device flags    : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags      : Keepalives

```

```

Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Last flapped      : Never
Statistics last cleared: Never
Traffic statistics:
  Input  bytes   :           15888           272 bps
  Output bytes   :           6189           48 bps
  Input  packets :           1547           2 pps
  Output packets :           393           0 pps
Egress queues: 4 supported, 4 in use
Queue counters:
  Queued packets  Transmitted packets  Dropped packets
0 best-effort      0                   0                0
1 expedited-fo     0                   0                0
2 assured-forw     0                   0                0
3 network-cont    196806             196806           0

Logical interface as0.0 (Index 79) (SNMP ifIndex 55) (Generation 18)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Bandwidth: 311040kbps
Statistics          Packets          pps          Bytes          bps
Bundle:
  Input  :           1334            2          13332          232
  Output:              0            0              0            0
Link:
  so-0/0/0.0 <-- down
  Input  :              0            0              0            0
  Output:              0            0              0            0
  so-0/0/1.0
  Input  :           541            1          5406          120
  Output:              0            0              0            0
  so-0/0/2.0
  Input  :           793            1          7926          112
  Output:              0            0              0            0
Protocol inet, MTU: 4470, Generation: 38, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 10.100.1.1, Local: 10.100.1.2, Broadcast: Unspecified,
  Generation: 40

```

show interfaces extensive (Aggregated SONET)

userhost1> show interfaces as0 extensive

```

Physical interface: as0, Enabled, Physical link is Up
Interface index: 149, SNMP ifIndex: 45, Generation: 32

```

```

Link-level type: PPP, MTU: 4474, Speed: 466560kbps, Minimum links needed: 1
Device flags      : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Link flags       : Keepalives
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Last flapped    : Never
Statistics last cleared: Never
Traffic statistics:
  Input  bytes :           17562           136 bps
  Output bytes :           6862           72 bps
  Input  packets:           1710           1 pps
  Output packets:           436           0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0
Egress queues: 4 supported, 4 in use
Queue counters:
  Queued packets  Transmitted packets  Dropped packets
0 best-effort    0                    0                    0
1 expedited-fo   0                    0                    0
2 assured-forw   0                    0                    0
3 network-cont   196848               196848               0

Logical interface as0.0 (Index 79) (SNMP ifIndex 55) (Generation 18)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
Bandwidth: 311040kbps
Statistics      Packets      pps      Bytes      bps
Bundle:
  Input :          1475          1      14742      136
  Output:           0           0           0       0
Link:
  so-0/0/0.0 <-- down
    Input :           0           0           0       0
    Output:           0           0           0       0
  so-0/0/1.0
    Input :          598           0      5976       24
    Output:           0           0           0       0
  so-0/0/2.0
    Input :          877           1      8766      112
    Output:           0           0           0       0
Protocol inet, MTU: 4470, Generation: 38, Route table: 0
Flags: None

```


Addresses, Flags: Is-Preferred Is-Primary

Destination: 10.100.1.1, Local: 10.100.1.2, Broadcast: Unspecified,

Generation: 40

show interfaces (SONET/SDH)

Syntax

```
show interfaces so-fpc/pic/port
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified SONET/SDH interface.

Options

so-*fpc/pic/port*—Display standard information about the specified SONET/SDH interface.

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

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

RELATED DOCUMENTATION

[SONET/SDH Interfaces Overview](#) | 2

List of Sample Output

[show interfaces \(SDH Mode, PPP\) on page 353](#)

[show interfaces brief \(SDH Mode, PPP\) on page 354](#)

[show interfaces detail \(SDH Mode, PPP\) on page 354](#)

[show interfaces extensive \(SDH Mode, PPP\) on page 355](#)

[show interfaces brief \(SONET Mode, Frame Relay\) on page 358](#)

[show interfaces \(SONET Mode, Frame Relay\) on page 359](#)

[show interfaces detail \(SONET Mode, Frame Relay\) on page 360](#)

[show interfaces extensive \(SONET Mode, Frame Relay\) on page 362](#)

[show interfaces extensive \(OC768-over-4xOC192 Mode\) on page 366](#)

[show interfaces detail \(IPv6 Tracking\) on page 369](#)

[show interfaces \(Shared Interface\) on page 371](#)

Output Fields

[Table 30 on page 337](#) lists the output fields for the **show interfaces** (SONET/SDH) command. Output fields are listed in the approximate order in which they appear.

Table 30: SONET/SDH show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Link-level type	Encapsulation being used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Clocking	SONET/SDH reference clock source: Internal or External . Clocking is configured and displayed only for channel 0.	All levels
Framing mode	Framing mode: SONET or SDH .	All levels
Speed	Speed at which the interface is running.	All levels
Loopback	Whether loopback is enabled and the type of loopback (local or remote).	All levels
FCS	Frame check sequence on the interface (either 16 or 32). The default is 16 bits.	All levels

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
Payload scrambler	Whether payload scrambling is enabled.	All levels
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Shared-interface	Indicates whether the routing domain is the owner or non-owner of the shared interface. If the routing domain is the Root System Domain (RSD), the value is Owner . If the routing domain is a Protected System Domain (PSD) under the RSD, the value is Non-owner .	All levels
Link flags	Information about the link. Possible values are described in the “Link Flags” section under <i>Common Output Fields Description</i> .	All levels
ANSI or ITU LMI settings	(Frame Relay) Settings for Local Management Interface (LMI). The format is (ANSI or ITU) LMI settings: value, value... xx seconds , where <i>value</i> can be: <ul style="list-style-type: none"> • n391dte—DTE full status polling interval (1-255) • n392dce—DCE error threshold (1-10) • n392dte—DTE error threshold (1-10) • n393dce—DCE monitored event count (1-10) • n393dte—DTE monitored event count (1-10) • t391dte—DTE polling timer (5-30 seconds) • t392dce—DCE polling verification timer (5-30 seconds) 	All levels
LMI	Input: value (hh:mm:ss ago), Output: value (hh:mm:ss ago)	brief none
LMI statistics	(Frame Relay) LMI packet statistics: <ul style="list-style-type: none"> • Input—Number of packets coming in on the interface (<i>nn</i>) and how much time has passed since the last packet arrived. The format is Input: nn (last seen hh:mm:ss ago). • Output—Number of packets sent out on the interface (<i>nn</i>) and how much time has passed since the last packet was sent. The format is Output: nn (last sent hh:mm:ss ago). 	detail extensive

Table 30: SONET/SDH show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
DTE statistics	<p>(Frame Relay) Statistics about messages transmitted from the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE):</p> <ul style="list-style-type: none"> • Enquiries sent—Number of link status enquiries sent from the DTE to the DCE. • Full enquiries sent—Number of full enquiries sent from the DTE to the DCE. • Enquiry responses received—Number of enquiry responses received by the DTE from the DCE. • Full enquiry responses received—Number of full enquiry responses sent from the DTE to the DCE. 	detail extensive none
DCE statistics	<p>(Frame Relay) Statistics about messages transmitted from the DCE to the DTE:</p> <ul style="list-style-type: none"> • Enquiries received—Number of enquiries received by the DCE from the DTE. • Full enquiries received—Number of full enquiries received by the DCE from the DTE. • Enquiry responses sent—Number of enquiry responses sent from the DCE to the DTE. • Full enquiry responses sent—Number of full enquiry responses sent from the DCE to the DTE. 	detail extensive none
Common statistics	<p>(Frame Relay) Statistics about messages sent between the DTE and the DCE:</p> <ul style="list-style-type: none"> • Unknown messages received—Number of received packets that do not fall into any category. • Asynchronous updates received—Number of link status peer changes received. • Out-of-sequence packets received—Number of packets for which the sequence of the packets received is different from the expected sequence. • Keepalive responses timedout—Number of keepalive responses that timed out when no LMI packet was reported for n392dte or n393dce intervals. (See LMI settings.) 	detail extensive none
Nonmatching DCE-end DLCIs	(Frame Relay. Displayed only from the DTE) Number of DLCIs configured from the DCE.	detail extensive
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
Keepalive settings	<p>(PPP and HDLC) Configured settings for keepalives.</p> <ul style="list-style-type: none"> • interval seconds—The time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds. • down-count number—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3. • up-count number—The number of keepalive packets a destination must receive to change a link's status from down to up. The range is 1 through 255, with a default of 1. 	All levels
Keepalive or Keepalive statistics	<p>(PPP and HDLC) Information about keepalive packets.</p> <ul style="list-style-type: none"> • Input—Number of keepalive packets received by PPP. <ul style="list-style-type: none"> • (last seen 00:00:00 ago)—Time since the last keepalive packet was received, in the format hh:mm:ss. • Output—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received. <ul style="list-style-type: none"> • (last seen 00:00:00 ago)—Time since the last keepalive packet was sent, in the format hh:mm:ss. 	All levels
LCP state	<p>(PPP) Link Control Protocol state.</p> <ul style="list-style-type: none"> • Conf-ack-received—Acknowledgement was received. • Conf-ack-sent—Acknowledgement was sent. • Conf-req-sent—Request was sent. • Down—LCP negotiation is incomplete (not yet completed or has failed). • Not-configured—LCP is not configured on the interface. • Opened—LCP negotiation is successful. 	detail extensive none
NCP state	<p>(PPP) Network Control Protocol state.</p> <ul style="list-style-type: none"> • Conf-ack-received—Acknowledgement was received. • Conf-ack-sent—Acknowledgement was sent. • Conf-req-sent—Request was sent. • Down—NCP negotiation is incomplete (not yet completed or has failed). • Not-configured—NCP is not configured on the interface. • Opened—NCP negotiation is successful. 	detail extensive none

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
CHAP state	<p>(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction.</p> <ul style="list-style-type: none"> • Chap-Chal-received—Challenge was received but response not yet sent. • Chap-Chal-sent—Challenge was sent. • Chap-Resp-received—Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.) • Chap-Resp-sent—Response was sent for the challenge received. • Closed—CHAP authentication is incomplete. • Failure—CHAP authentication failed. • Not-configured—CHAP is not configured on the interface. • Success—CHAP authentication was successful. 	detail extensive none
CoS queues	Number of CoS queues configured.	detail extensive none
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute: second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive none
Input rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	<p>Number of bytes and packets received and transmitted on the physical interface, and the traffic rate in bits per seconds (bps).</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive

Table 30: SONET/SDH show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Label-switched interface (LSI) traffic statistics	<p>(Frame Relay) LSI traffic statistics:</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes and speed, in bits per second (bps), received on the interface. • Output packets—Number of packets and speed, in bps, transmitted on the interface. 	extensive
Input errors	<p>Input errors on the interface whose definitions are as follows:</p> <ul style="list-style-type: none"> • Errors—Sum of the incoming frame aborts and FCS errors. • Drops—Number of packets dropped by the input 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. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Giants—Number of frames received that are larger than the giant threshold. • Bucket Drops—Drops resulting from the traffic load exceeding the interface transmit/receive leaky bucket configuration. The default is off. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • L3 incompletes—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. • L2 channel errors—Number of times the software did not find a valid logical interface for an incoming frame. • L2 mismatch timeouts—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable. • HS link CRC errors—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces. • HS link FIFO overflows—Number of FIFO overflows on the high-speed links between the ASICs responsible for handling the router interfaces. 	extensive

Table 30: SONET/SDH show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Output errors	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • 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. • Aged packets—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware. • HS link FIFO underflows—Number of FIFO underflows on the high-speed links between the ASICs responsible for handling the router interfaces. • MTU errors—Number of packets whose size exceeds the MTU of the interface. 	extensive
IPv6 transit statistics	<p>Number of transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Egress queues	Total number of egress queues supported on the specified interface.	detail extensive
Queue counters	<p>CoS queue number and its associated user-configured forwarding class name.</p> <ul style="list-style-type: none"> • Queued packets—Number of queued packets. • Transmitted packets—Number of transmitted packets. • Dropped packets—Number of packets dropped by the ASIC's RED mechanism. 	extensive

Table 30: SONET/SDH show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
SONET alarms SONET defects	(SONET) SONET media-specific alarms and defects that prevents the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SONET PHY , SONET section , SONET line , and SONET path .	All levels
Link	(For 4-port OC192c PIC operating in OC768-over-4xOC192 mode) The link number. Errors and alarms are displayed for each link.	extensive
SONET PHY	Counts of specific SONET errors with detailed information. <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. Subfields are: <ul style="list-style-type: none"> • PLL Lock—Phase-locked loop • PHY Light—Loss of optical signal 	extensive
SONET section	Counts of specific SONET errors with detailed information. <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. Subfields are: <ul style="list-style-type: none"> • BIP-B1—Bit interleaved parity for SONET section overhead • SEF—Severely errored framing • LOL—Loss of light • LOF—Loss of frame • ES-S—Errored seconds (section) • SES-S—Severely errored seconds (section) • SEFS-S—Severely errored framing seconds (section) 	extensive

Table 30: SONET/SDH show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
SONET line	<p>Active alarms and defects, plus counts of specific SONET errors with detailed information.</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B2—Bit interleaved parity for SONET line overhead • REI-L—Remote error indication (near-end line) • RDI-L—Remote defect indication (near-end line) • AIS-L—Alarm indication signal (near-end line) • BERR-SF—Bit error rate fault (signal failure) • BERR-SD—Bit error rate defect (signal degradation) • ES-L—Errored seconds (near-end line) • SES-L—Severely errored seconds (near-end line) • UAS-L—Unavailable seconds (near-end line) • ES-LFE—Errored seconds (far-end line) • SES-LFE—Severely errored seconds (far-end line) • UAS-LFE—Unavailable seconds (far-end line) 	extensive

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
SONET path	<p>Active alarms and defects, plus counts of specific SONET errors with detailed information.</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B3—Bit interleaved parity for SONET section overhead • REI-P—Remote error indication • LOP-P—Loss of pointer (path) • AIS-P—Path alarm indication signal • RDI-P—Path remote defect indication • UNEQ-P—Path unequipped • PLM-P—Path payload (signal) label mismatch • ES-P—Errored seconds (near-end STS path) • SES-P—Severely errored seconds (near-end STS path) • UAS-P—Unavailable seconds (near-end STS path) • ES-PFE—Errored seconds (far-end STS path) • SES-PFE—Severely errored seconds (far-end STS path) • UAS-PFE—Unavailable seconds (far-end STS path) 	extensive
Received SONET overhead Transmitted SONET overhead	<p>Values of the received and transmitted SONET overhead:</p> <ul style="list-style-type: none"> • C2—Signal label. Allocated to identify the construction and content of the STS-level SPE and for PDI-P. • F1—Section user channel byte. This byte is set aside for the purposes of users. • K1 and K2—These bytes are allocated for APS signaling for the protection of the multiplex section. • J0—Section trace. This byte is defined for STS-1 number 1 of an STS-N signal. Used to transmit a 1-byte fixed-length string or a 16-byte message so that a receiving terminal in a section can verify its continued connection to the intended transmitter. • S1—Synchronization status. The S1 byte is located in the first STS-1 of an STS-N. • Z3 and Z4—Allocated for future use. 	extensive

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
SDH alarms SDH defects	SDH media-specific defects that can prevent the interface from passing packets. When a defect persists for a certain period, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router or light the red or yellow alarm LED on the craft interface. See these fields for possible alarms and defects: SDH PHY , SDH regenerator section , SDH multiplex section , and SDH path .	All levels
SDH PHY	Active alarms and defects, plus counts of specific SDH errors with detailed information. <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. Subfields are: <ul style="list-style-type: none"> • PLL Lock—Phase-locked loop • PHY Light—Loss of optical signal 	extensive
SDH regenerator section	Active alarms and defects, plus counts of specific SDH errors with detailed information. <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. Subfields are: <ul style="list-style-type: none"> • RS-BIP8—24-bit BIP for multiplex section overhead (B2 bytes) • OOF—Out of frame • LOS—Loss of signal • LOF—Loss of frame • RS-ES—Errored seconds (near-end regenerator section) • RS-SES—Severely errored seconds (near-end regenerator section) • RS-SEFS—Severely errored framing seconds (regenerator section) 	extensive

Table 30: SONET/SDH show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
SDH multiplex section	<p>Active alarms and defects, plus counts of specific SDH errors with detailed information.</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • MS-BIP24—8-bit BIP for high-order path overhead (B3 byte) • MS-FEBE—Far-end block error (multiplex section) • MS-FERF—Far-end remote fail (multiplex section) • MS-AIS—Alarm indication signal (multiplex section) • BERR-SF—Bit error rate fault (signal failure) • BERR-SD—Bit error rate defect (signal degradation) • MS-ES—Errored seconds (near-end multiplex section) • MS-SES—Severely errored seconds (near-end multiplex section) • MS-UAS—Unavailable seconds (near-end multiplex section) • MS-ES-FE—Errored seconds (far-end multiplex section) • MS-SES-FE—Severely errored seconds (far-end multiplex section) • MS-UAS-FE—Unavailable seconds (far-end multiplex section) 	extensive

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
SDH path	<p>Active alarms and defects, plus counts of specific SDH errors with detailed information.</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • HP-BIP8—8-bit BIP for regenerator section overhead (B1 byte) • HP-FEBE—Far-end block error (high-order path) • HP-LOP—Loss of pointer (high-order path) • HP-AIS—High-order-path alarm indication signal • HP-FERF—Far-end remote fail (high-order path) • HP-UNEQ—Unequipped (high-order path) • HP-PLM—Payload label mismatch (high-order path) • HP-ES—Errored seconds (near-end high-order path) • HP-SES—Severely errored seconds (near-end high-order path) • HP-UAS—Unavailable seconds (near-end high-order path) • HP-ES-FE—Errored seconds (far-end high-order path) • HP-SES-FE—Severely errored seconds (far-end high-order path) • HP-UAS-FE—Unavailable seconds (far-end high-order path) 	extensive
Received SDH overhead Transmitted SDH overhead	<p>Values of the received and transmitted SONET overhead:</p> <ul style="list-style-type: none"> • C2—Signal label. Allocated to identify the construction and content of the STS-level SPE and for PDI-P. • F1—Section user channel byte. This byte is set aside for the purposes of users. • K1 and K2—These bytes are allocated for APS signaling for the protection of the multiplex section. • J0—Section trace. This byte is defined for STS-1 number 1 of an STS-N signal. Used to transmit a 1-byte fixed-length string or a 16-byte message so that a receiving terminal in a section can verify its continued connection to the intended transmitter. • S1—Synchronization status. The S1 byte is located in the first STS-1 of an STS-N. • Z3 and Z4—Allocated for future use. 	extensive

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
Received path trace Transmitted path trace	SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the router at the other end of the fiber. The transmitted path trace value is the message that this router transmits.	extensive
HDLC configuration	Information about the HDLC configuration. <ul style="list-style-type: none"> • Policing bucket—Configured state of the receiving policer. • Shaping bucket—Configured state of the transmitting shaper. • Giant threshold—Giant threshold programmed into the hardware. • Runt threshold—Runt threshold programmed into the hardware. 	extensive
CoS information	Information about the CoS queue for the physical interface. <ul style="list-style-type: none"> • CoS transmit queue—Queue number and its associated user-configured forwarding class name. • Bandwidth %—Percentage of bandwidth allocated to the queue. • Bandwidth bps—Bandwidth allocated to the queue (in bps). • Buffer %—Percentage of buffer space allocated to the queue. • Buffer usec—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time. • Priority—Queue priority: low or high. • Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available. 	extensive
Packet Forwarding Engine configuration	Information about the configuration of the Packet Forwarding Engine: <ul style="list-style-type: none"> • Destination slot—FPC slot number. • PLP byte—Packet Level Protocol byte. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Encapsulation on the logical interface.	All levels
PPP parameters	The PPP loopback clear timer value.	extensive
Shared interface	Provides the following information: <ul style="list-style-type: none"> • shared with—(RSD only) Indicates which PSD owns the logical shared interface. For example, psd3. • peer interface—(PSD only) Lists the logical tunnel interface that peers with the logical shared interface. For example, ut-2/1/0.2. • tunnel token—Specifies the receive (RX) and transmit (TX) tunnel tokens. For example, Rx: 5.519, Tx: 13.514. 	All levels
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified
Traffic statistics	Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
Protocol	Protocol family configured on the logical interface, such as iso , inet6 , or mpls .	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. If the protocol is inet , the IP address of the interface is also displayed.	brief
Multilink bundle	(If the logical interface is configured as part of a multilink bundle.) Interface name for the multilink bundle.	detail extensive none
AS bundle	(If the logical interface is configured as part of an aggregated SONET bundle.) AS bundle number.	detail extensive
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0 .	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address of the interface.	detail extensive none

Table 30: SONET/SDH show interfaces Output Fields (continued)

Field Name	Field Description	Level of Output
DLCI	<p>(Frame Relay) DLCI number of the logical interface. The following DLCI information is displayed: Flags, Total down time, Last down, and Traffic statistics. Flags is one or more of the following:</p> <ul style="list-style-type: none"> • Active—Set when the link is active and the DTE and DCE are exchanging information. • Down—Set when the link is active, but no information is received from the DCE. • Unconfigured—Set when the corresponding DLCI in the DCE is not configured. • Configured—Set when the corresponding DLCI in the DCE is configured. • Dce-configured—Displayed when the command is issued from the DTE. 	detail extensive
DLCI statistics	<p>(Frame Relay) Data-link connection identifier (DLCI) statistics.</p> <ul style="list-style-type: none"> • Active DLCI—Number of active DLCIs. • Inactive DLCI—Number of inactive DLCIs. 	detail extensive none

Sample Output

show interfaces (SDH Mode, PPP)

user@host> show interfaces so-0/0/0

```
Physical interface: so-0/0/0, Enabled, Physical link is Up
  Interface index: 149, SNMP ifIndex: 66
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SDH mode, Speed: OC3,
  Loopback: None, FCS: 16, Payload scrambler: Enabled
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 30 (00:00:07 ago), Output: 29 (00:00:05 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
  Not-configured
  CHAP state: Closed
  CoS queues      : 4 supported, 4 maximum usable queues
  Last flapped    : 2006-03-24 13:20:56 PST (00:05:09 ago)
  Input rate      : 0 bps (0 pps)
```

```

Output rate      : 0 bps (0 pps)
SDH  alarms     : None
SDH  defects    : None

Logical interface so-0/0/0.0 (Index 66) (SNMP ifIndex 43)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  Protocol inet, MTU: 4470
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 10.0.12.0/30, Local: 10.0.12.1, Broadcast: 10.0.12.3
  Protocol iso, MTU: 4470
    Flags: Protocol-Down
  Protocol mpls, MTU: 4458, Maximum labels: 3
    Flags: Protocol-Down, Is-Primary

```

show interfaces brief (SDH Mode, PPP)

user@host> **show interfaces so-0/0/0 brief**

```

Physical interface: so-0/0/0, Enabled, Physical link is Up
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SDH mode, Speed: OC3,
  Loopback: None, FCS: 16, Payload scrambler: Enabled
  Device flags      : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags        : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 25 (00:00:01 ago), Output: 24 (00:00:04 ago)
  SDH  alarms     : None
  SDH  defects    : None

Logical interface so-0/0/0.0
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  inet  10.0.12.1/30
  iso
  mpls

```

show interfaces detail (SDH Mode, PPP)

user@host> **show interfaces so-0/0/0 detail**

```

Physical interface: so-0/0/0, Enabled, Physical link is Up
  Interface index: 149, SNMP ifIndex: 66, Generation: 35
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SDH mode, Speed: OC3,

```

```

Loopback: None, FCS: 16, Payload scrambler: Enabled
Device flags   : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
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 : 33 (last seen 00:00:05 ago)
  Output: 32 (last sent 00:00:06 ago)
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
Not-configured
CHAP state: Closed
CoS queues      : 4 supported, 4 maximum usable queues
Last flapped    : 2006-03-24 13:20:56 PST (00:05:38 ago)
Statistics last cleared: Never
Traffic statistics:
  Input  bytes :                862                0 bps
  Output bytes :               3592               64 bps
  Input  packets:                 70                 0 pps
  Output packets:                330                0 pps
Egress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets  Dropped packets
  0 best-effort      0                0                  0
  1 expedited-fo     0                0                  0
  2 assured-forw     0                0                  0
  3 network-cont    329              329                  0
SDH  alarms   : None
SDH  defects  : None

Logical interface so-0/0/0.0 (Index 66) (SNMP ifIndex 43) (Generation 19)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  Protocol inet, MTU: 4470, Generation: 48, Route table: 0
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 10.0.12.0/30, Local: 10.0.12.1, Broadcast: 10.0.12.3,
      Generation: 48
  Protocol iso, MTU: 4470, Generation: 49, Route table: 0
    Flags: Protocol-Down
  Protocol mpls, MTU: 4458, Maximum labels: 3, Generation: 50, Route table: 0
    Flags: Protocol-Down, Is-Primary

```

show interfaces extensive (SDH Mode, PPP)

```
user@host> show interfaces so-0/0/0 extensive
```

```

Physical interface: so-0/0/0, Enabled, Physical link is Up
  Interface index: 149, SNMP ifIndex: 66, Generation: 35
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SDH mode, Speed: OC3,
  Loopback: None, FCS: 16, Payload scrambler: Enabled
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  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 : 36 (last seen 00:00:01 ago)
    Output: 35 (last sent 00:00:10 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
  Not-configured
  CHAP state: Closed
  CoS queues   : 4 supported, 4 maximum usable queues
  Last flapped : 2006-03-24 13:20:56 PST (00:06:08 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes   :                922                0 bps
    Output bytes  :               3850               64 bps
    Input packets :                75                0 pps
    Output packets:               356                0 pps
  Label-switched interface (LSI) traffic statistics:
    Input bytes   :                0                0 bps
    Input packets :                0                0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Bucket drops: 0, Policed discards: 218, L3 incompletes: 0,
    L2 channel errors: 0, L2 mismatch timeouts: 2, HS link CRC errors: 0,
    HS link FIFO overflows: 0
  Output errors:
    Carrier transitions: 3, Errors: 0, Drops: 0, Aged packets: 0,
    HS link FIFO underflows: 0, MTU errors: 0
  Egress queues: 4 supported, 4 in use
  Queue counters:
    Queued packets  Transmitted packets  Dropped packets
    0 best-effort    0                0                0
    1 expedited-fo   0                0                0
    2 assured-forw    0                0                0
    3 network-cont    354              354              0
  SDH alarms   : None
  SDH defects  : None
  SDH PHY:
    Seconds      Count  State

```

PLL Lock	0	0	OK
PHY Light	2	1	OK
SDH regenerator section:			
RS-BIP8	0	0	
OOF	3	8	OK
LOS	3	2	OK
LOF	3	2	OK
RS-ES	3		
RS-SES	3		
RS-SEFS	3		
SDH multiplex section:			
MS-BIP24	0	0	
MS-FEBE	0	0	
MS-FERF	3	2	OK
MS-AIS	2	1	OK
BERR-SF	0	0	OK
BERR-SD	0	0	OK
MS-ES	3		
MS-SES	3		
MS-UAS	0		
MS-SES-FE	3		
MS-UAS-FE	0		
SDH path:			
HP-BIP8	0	0	
HP-FEBE	0	0	
HP-LOP	1	1	OK
HP-AIS	2	1	OK
HP-FERF	3	2	OK
HP-UNEQ	0	0	OK
HP-PLM	1	1	OK
HP-ES	3		
HP-SES	3		
HP-UAS	0		
HP-ES-FE	3		
HP-SES-FE	3		
HP-UAS-FE	0		
Received SDH 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
Transmitted SDH overhead:			
F1	: 0x00, J0	: 0x01, K1	: 0x00, K2 : 0x00
S1	: 0x00, C2	: 0xcf, F2	: 0x00, Z3 : 0x00
Z4	: 0x00		

```

Received path trace: R2 so-0/0/0
  52 32 20 73 6f 2d 30 2f 30 2f 30 00 00 00 00 00  R2 so-0/0/0.....
Transmitted path trace: R1 so-0/0/0
  52 31 20 73 6f 2d 30 2f 30 2f 30 00 00 00 00 00  R1 so-0/0/0.....
HDLCD configuration:
  Policing bucket: Disabled
  Shaping bucket : Disabled
  Giant threshold: 4484, Runt threshold: 3
Packet Forwarding Engine configuration:
  Destination slot: 0, PLP byte: 1 (0x00)
CoS information:
  CoS transmit queue      Bandwidth      Buffer Priority  Limit
                           %          bps      %    usec
  0 best-effort           95    147744000  95      0      low  none
  3 network-control       5      7776000   5      0      low  none

Logical interface so-0/0/0.0 (Index 66) (SNMP ifIndex 43) (Generation 19)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
PPP parameters:
  PPP loopback clear timer: 3 sec
Protocol inet, MTU: 4470, Generation: 48, Route table: 0
  Flags: None
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.0.12.0/30, Local: 10.0.12.1, Broadcast: 10.0.12.3,
    Generation: 48
Protocol iso, MTU: 4470, Generation: 49, Route table: 0
  Flags: Protocol-Down
Protocol mpls, MTU: 4458, Maximum labels: 3, Generation: 50, Route table: 0
  Flags: Protocol-Down, Is-Primary
MS-ES-FE                      3

```

show interfaces brief (SONET Mode, Frame Relay)

user@host> **show interfaces so-0/0/0 brief**

```

Physical interface: so-0/0/0, Enabled, Physical link is Up
Link-level type: Frame-Relay, 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 Internal: 0x4000
Link flags        : Keepalives DTE
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
LMI: Input: 29 (00:00:02 ago), Output: 28 (00:00:01 ago)
SONET alarms      : None

```



```
SONET defects   : None
```

```
Logical interface so-0/0/0.0
```

```
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
```

```
inet 10.0.12.1      --> 10.0.12.2
```

```
iso
```

```
mpls
```

```
DLCI 16
```

```
Flags: Down, DCE-Unconfigured
```

```
Total down time: 00:04:12 sec, Last down: 00:04:12 ago
```

show interfaces (SONET Mode, Frame Relay)

```
user@host> show interfaces so-0/0/0
```

```
Physical interface: so-0/0/0, Enabled, Physical link is Up
```

```
Interface index: 128, SNMP ifIndex: 66
```

```
Link-level type: Frame-Relay, 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 Internal: 0x4000
```

```
Link flags     : Keepalives DTE
```

```
ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
```

```
LMI: Input: 23 (00:00:05 ago), Output: 22 (00:00:03 ago)
```

```
DTE statistics:
```

```
Enquiries sent                : 19
```

```
Full enquiries sent           : 3
```

```
Enquiry responses received    : 20
```

```
Full enquiry responses received : 3
```

```
DCE statistics:
```

```
Enquiries received            : 0
```

```
Full enquiries received       : 0
```

```
Enquiry responses sent        : 0
```

```
Full enquiry responses sent    : 0
```

```
Common statistics:
```

```
Unknown messages received     : 0
```

```
Asynchronous updates received : 0
```

```
Out-of-sequence packets received : 0
```

```
Keepalive responses timeout   : 1
```

```
CoS queues      : 4 supported, 4 maximum usable queues
```

```
Last flapped    : 2006-03-06 11:53:20 PST (3d 03:09 ago)
```

```
Input rate      : 0 bps (0 pps)
```

```
Output rate     : 56 bps (0 pps)
```

```
SONET alarms    : None
```

```

SONET defects   : None

Logical interface so-0/0/0.0 (Index 79) (SNMP ifIndex 43)
  Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
  Input packets : 0
  Output packets: 0
  Protocol inet, MTU: 4470
    Flags: None
    Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
      Destination: 10.0.12.2, Local: 10.0.12.1
  Protocol iso, MTU: 4470
    Flags: None
  Protocol mpls, MTU: 4450, Maximum labels: 3
  DLCI 16
    Flags: Down, DCE-Unconfigured
    Total down time: 00:03:11 sec, Last down: 00:03:11 ago
      Input packets : 0
      Output packets: 0
  DLCI statistics:
    Active DLCI   :0   Inactive DLCI   :1

```

show interfaces detail (SONET Mode, Frame Relay)

user@host> show interfaces so-0/0/0 detail

```

Physical interface: so-0/0/0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 66, Generation: 11
  Link-level type: Frame-Relay, 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 Internal: 0x4000
  Link flags     : Keepalives DTE
  Hold-times     : Up 0 ms, Down 0 ms
  ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
  LMI statistics:
    Input : 33 (last seen 00:00:09 ago)
    Output: 32 (last sent 00:00:01 ago)
  DTE statistics:
    Enquiries sent                : 27
    Full enquiries sent           : 5
    Enquiry responses received    : 28
    Full enquiry responses received : 5
  DCE statistics:
    Enquiries received            : 0

```

```

Full enquiries received      : 0
Enquiry responses sent       : 0
Full enquiry responses sent   : 0
Common statistics:
Unknown messages received    : 0
Asynchronous updates received : 0
Out-of-sequence packets received : 0
Keepalive responses timeout   : 1
CoS queues      : 4 supported, 4 maximum usable queues
Last flapped    : 2006-03-06 11:53:20 PST (3d 03:10 ago)
Statistics last cleared: Never
Traffic statistics:
Input  bytes :          495368          0 bps
Output bytes :        2765014        56 bps
Input  packets:         41165          0 pps
Output packets:        133530          0 pps
Egress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets
0 best-effort          18              18              0
1 expedited-fo          0              0              0
2 assured-forw          0              0              0
3 network-cont       133506         133506              0
SONET alarms   : None
SONET defects  : None
Logical interface so-0/0/0.0 (Index 79) (SNMP ifIndex 43) (Generation 28)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
Traffic statistics:
Input  bytes :          0
Output bytes :          0
Input  packets:          0
Output packets:          0
Local statistics:
Input  bytes :          0
Output bytes :          0
Input  packets:          0
Output packets:          0
Transit statistics:
Input  bytes :          0          0 bps
Output bytes :          0          0 bps
Input  packets:          0          0 pps
Output packets:          0          0 pps
Protocol inet, MTU: 4470, Generation: 49, Route table: 0
Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary

```

```

    Destination: 10.0.12.2, Local: 10.0.12.1, Broadcast: Unspecified,
    Generation: 61
Protocol iso, MTU: 4470, Generation: 50, Route table: 0
  Flags: None
Protocol mpls, MTU: 4450, Maximum labels: 3, Generation: 51, Route table: 0
DLCI 16
  Flags: Down, DCE-Unconfigured
  Total down time: 00:04:54 sec, Last down: 00:04:54 ago
  Traffic statistics:
    Input  bytes   :                0
    Output bytes   :                0
    Input  packets :                0
    Output packets :                0
  DLCI statistics:
    Active DLCI   :0  Inactive DLCI :1

```

show interfaces extensive (SONET Mode, Frame Relay)

user@host> **show interfaces so-0/0/0 extensive**

```

Physical interface: so-0/0/0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 66, Generation: 11
  Link-level type: Frame-Relay, 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 Internal: 0x4000
  Link flags     : Keepalives DTE
  Hold-times    : Up 0 ms, Down 0 ms
  ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
  LMI statistics:
    Input : 39 (last seen 00:00:02 ago)
    Output: 36 (last sent 00:00:07 ago)
  DTE statistics:
    Enquiries sent                : 30
    Full enquiries sent           : 6
    Enquiry responses received    : 33
    Full enquiry responses received : 6
  DCE statistics:
    Enquiries received            : 0
    Full enquiries received       : 0
    Enquiry responses sent        : 0
    Full enquiry responses sent   : 0
  Common statistics:
    Unknown messages received     : 0

```

```

Asynchronous updates received      : 0
Out-of-sequence packets received   : 0
Keepalive responses timedout        : 1
CoS queues      : 4 supported, 4 maximum usable queues
Last flapped    : 2006-03-06 11:53:20 PST (3d 03:11 ago)
Statistics last cleared: Never
Traffic statistics:
Input  bytes   :           495452           56 bps
Output bytes   :           2765074          0 bps
Input  packets :           41171           0 pps
Output packets :           133534           0 pps
Label-switched interface (LSI) traffic statistics:
Input  bytes   :           0              0 bps
Input  packets :           0              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: 3, Errors: 0, Drops: 0, Aged packets: 0,
HS link FIFO underflows: 0, MTU errors: 0
Egress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets
0 best-effort        18              18              0
1 expedited-fo       0              0              0
2 assured-forw       0              0              0
3 network-cont      133510          133510          0
SONET alarms      : None
SONET defects     : None
SONET PHY:        Seconds      Count  State
PLL Lock          0            0  OK
PHY Light         60            1  OK
SONET section:
BIP-B1            0            0
SEF               108          158  OK
LOS               108            2  OK
LOF               108            2  OK
ES-S              108
SES-S              108
SEFS-S            108
SONET line:
BIP-B2            0            0
REI-L             0            0

```

```

RDI-L          1          1 OK
AIS-L          107        1 OK
BERR-SF         0         0 OK
BERR-SD         44        2 OK
ES-L           108
SES-L           108
UAS-L           97
ES-LFE         1
SES-LFE         1
UAS-LFE         0
SONET path:
BIP-B3          0         0
REI-P           0         0
LOP-P           1         1 OK
AIS-P          107        1 OK
RDI-P           1         1 OK
UNEQ-P          0         0 OK
PLM-P           1         1 OK
ES-P           108
SES-P           108
UAS-P           97
ES-PFE          1
SES-PFE          1
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
Transmitted SONET overhead:
F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
S1      : 0x00, C2      : 0xcf, F2      : 0x00, Z3      : 0x00
Z4      : 0x00
Received path trace: R2 so-0/0/0
52 32 20 73 6f 2d 30 2f 30 2f 30 00 00 00 00 00 R2 so-0/0/0.....
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 0d 0a .....
Transmitted path trace: R1 so-0/0/0
52 31 20 73 6f 2d 30 2f 30 2f 30 00 00 00 00 00 R1 so-0/0/0.....
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: 0, PLP byte: 1 (0x00)
CoS information:
  CoS transmit queue      Bandwidth      Buffer  Priority  Limit
                           %      bps      %      usec
  0 best-effort           95      147744000  95      0      low      none
  3 network-control       5       7776000   5      0      low      none

Logical interface so-0/0/0.0 (Index 79) (SNMP ifIndex 43) (Generation 28)
Flags: Device-Down Point-To-Point SNMP-Traps Encapsulation: FR-NLPID
Traffic statistics:
  Input  bytes :           0
  Output bytes :           0
  Input  packets:          0
  Output packets:          0
Local statistics:
  Input  bytes :           0
  Output bytes :           0
  Input  packets:          0
  Output packets:          0
Transit statistics:
  Input  bytes :           0      0 bps
  Output bytes :           0      0 bps
  Input  packets:          0      0 pps
  Output packets:          0      0 pps
Protocol inet, MTU: 4470, Generation: 49, Route table: 0
  Flags: None
  Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
    Destination: 10.0.12.2, Local: 10.0.12.1, Broadcast: Unspecified,
    Generation: 61
Protocol iso, MTU: 4470, Generation: 50, Route table: 0
  Flags: None
Protocol mpls, MTU: 4450, Maximum labels: 3, Generation: 51, Route table: 0
DLCI 16
  Flags: Down, DCE-Unconfigured
  Total down time: 00:05:42 sec, Last down: 00:05:42 ago
Traffic statistics:
  Input  bytes :           0
  Output bytes :           0
  Input  packets:          0
  Output packets:          0

```

```

DLCI statistics:
  Active DLCI   :0   Inactive DLCI   :1

```

show interfaces extensive (OC768-over-4xOC192 Mode)

user@host> show interfaces so-7/0/0 extensive

```

Physical interface: so-7/0/0, Enabled, Physical link is Up
  Interface index: 163, SNMP ifIndex: 23, Generation: 186
  Link-level type: Cisco-HDLC, MTU: 4474, Clocking: Internal, SONET mode, Speed:
OC768,
  Loopback: Local, FCS: 16, Payload scrambler: Enabled
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link flags     : No-Keepalives
  Hold-times    : Up 0 ms, Down 0 ms
  CoS queues    : 8 supported, 8 maximum usable queues
  Last flapped  : 2006-01-13 10:43:39 PST (01:05:33 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input  bytes   :                76992                200 bps
    Output bytes   :                83707                216 bps
    Input  packets :                1343                  0 pps
    Output packets :                1343                  0 pps
  Input errors:
    Errors: 0, Drops: 3885, Framing errors: 68154624, Runts: 0, Giants: 0, Bucket
drops: 0,
    Policed discards: 0, L3 incompletes: 95040248, L2 channel errors: 0, L2 mismatch
timeouts: 0,
    HS link CRC errors: 0, HS link FIFO overflows: 30742070
  Output errors:
    Carrier transitions: 1, Errors: 0, Drops: 0, Aged packets: 0, HS link FIFO
underflows: 0,
    MTU errors: 0
  Egress queues: 8 supported, 4 in use
  Queue counters:
    Queued packets  Transmitted packets  Dropped packets
    0 best-effort    2                2                0
    1 expedited-fo   0                0                0
    2 assured-forw    0                0                0
    3 network-cont    1341             1341             0
  SONET alarms   : None
  SONET defects   : None
  Link           : 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	2	1	OK
LOS	0	0	OK
LOF	3	2	OK
ES-S	2		
SES-S	2		
SEFS-S	2		

SONET line:

BIP-B2	0	0	
REI-L	0	0	
RDI-L	1	1	OK
AIS-L	2	1	OK
BERR-SF	0	0	OK
BERR-SD	0	0	OK
ES-L	3		
SES-L	3		
UAS-L	0		
ES-LFE	1		
SES-LFE	1		
UAS-LFE	0		

SONET path:

BIP-B3	0	0	
REI-P	0	0	
LOP-P	0	0	OK
AIS-P	2	1	OK
RDI-P	0	0	OK
UNEQ-P	0	0	OK
PLM-P	0	0	OK
ES-P	3		
SES-P	3		
UAS-P	0		
ES-PFE	0		
SES-PFE	0		
UAS-PFE	0		

Payload pointer:

Current pointer	: 522
Pointer increment count	: 0
Pointer decrement count	: 0
New pointer NDF count	: 0

Received SONET overhead:

```

F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
S1      : 0x00, C2      : 0xcf, C2(cmp) : 0xcf, F2      : 0x00
Z3      : 0x00, Z4      : 0x00, S1(cmp) : 0x00

```

Transmitted SONET overhead:

```

F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
S1      : 0x00, C2      : 0xcf, F2      : 0x00, Z3      : 0x00
Z4      : 0x00

```

Received path trace: fold so-7/0/0

```

66 6f 6c 64 20 73 6f 2d 37 2f 30 2f 30 00 00 00   fold so-7/0/0...
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 0d 0a .....

```

Transmitted path trace: fold so-7/0/0

```

66 6f 6c 64 20 73 6f 2d 37 2f 30 2f 30 00 00 00   fold so-7/0/0...
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 .....

```

Link : 1

SONET alarms : None

SONET defects : None

SONET PHY:	Seconds	Count	State
PLL Lock	0	0	OK
PHY Light	0	0	OK

SONET section:	Seconds	Count	State
BIP-B1	0	0	
SEF	2	1	OK
LOS	0	0	OK
LOF	3	2	OK
ES-S	2		
SES-S	2		
SEFS-S	2		

SONET line:	Seconds	Count	State
BIP-B2	0	0	
REI-L	0	0	
RDI-L	0	0	OK
AIS-L	2	1	OK
BERR-SF	0	0	OK
BERR-SD	0	0	OK
ES-L	3		
SES-L	3		
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                                2          1 OK
    RDI-P                                0          0 OK
    UNEQ-P                               0          0 OK
    PLM-P                                0          0 OK
    ES-P                                 3
    SES-P                                 3
    UAS-P                                 0
    ES-PFE                               0
    SES-PFE                               0
    UAS-PFE                               0
Payload pointer:
    Current pointer                        : 522
    Pointer increment count                : 0
    Pointer decrement count                : 0
    New pointer NDF count                  : 0
Received SONET overhead:
    F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
    S1      : 0x00, C2      : 0xcf, C2(cmp) : 0xcf, F2      : 0x00
    Z3      : 0x00, Z4      : 0x00, S1(cmp) : 0x00
Transmitted SONET overhead:
    F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
    S1      : 0x00, C2      : 0xcf, F2      : 0x00, Z3      : 0x00
    Z4      : 0x00
Received path trace: fold so-7/0/0
    66 6f 6c 64 20 73 6f 2d 37 2f 30 2f 30 00 00 00   fold so-7/0/0...
    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 0d 0a .....
Transmitted path trace: fold so-7/0/0
    66 6f 6c 64 20 73 6f 2d 37 2f 30 2f 30 00 00 00   fold so-7/0/0...
    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 .....
...

```

show interfaces detail (IPv6 Tracking)

```
user@host> show interfaces so-0/2/0 detail
```

```

Physical interface: so-0/2/0, Enabled, Physical link is Up
  Interface index: 130, SNMP ifIndex: 26, Generation: 131
  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: Point-To-Point SNMP-Traps Internal: 0x4000
  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 : 7 (last seen 00:00:01 ago)
    Output: 6 (last sent 00:00:08 ago)
  LCP state: Opened
  NCP state: inet: Not-configured, inet6: Opened, iso: Not- configured, mpls:
Not-configured
  CHAP state: Closed
  PAP state: Closed
  CoS queues      : 4 supported, 4 maximum usable queues
  Last flapped    : 2007-11-29 08:45:47 PST (1d 03:44 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input  bytes   :           7407782           40 bps
    Output bytes   :           7307322           48 bps
    Input  packets :           107570           0 pps
    Output packets :           108893           0 pps
  IPv6 transit statistics:
    Input  bytes   :           57328
    Output bytes   :           57400
    Input  packets :           1024
    Output packets :           1025
  Egress queues: 4 supported, 4 in use
  Queue counters:
    Queued packets  Transmitted packets  Dropped packets
    0 best-effort   1191                  1191              0
    1 expedited-fo    0                   0                 0
    2 assured-forw    0                   0                 0
    3 network-cont   107700              107700            0
  SONET alarms      : None
  SONET defects     : None

Logical interface so-0/2/0.0 (Index 70) (SNMP ifIndex 47) (Generation 231)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPP
  Protocol inet6, MTU: 4470, Generation: 433, Route table: 0
  Flags: None

```

```

Addresses, Flags: Is-Preferred Is-Primary
  Destination: 2001:db8::2:1/32, Local: 2001:db8::2:2,
  Broadcast: Unspecified, Generation: 683
Addresses, Flags: Is-Preferred
  Destination: 2001:db8::1:2, Local: 2001:db8::1:3,
  Broadcast: Unspecified, Generation: 684

```

show interfaces (Shared Interface)

user@rsd1> **show interfaces so-7/2/0**

```

Physical interface: so-7/2/0, Enabled, Physical link is Down
  Interface index: 128, SNMP ifIndex: 109
  Link-level type: Frame-Relay, MTU: 4474, Clocking: Internal, SONET mode,
  Speed: OC192, Loopback: None, FCS: 16, Payload scrambler: Enabled
  Device flags      : Present Running Down
  Interface flags: Hardware-Down Point-To-Point SNMP-Traps Internal: 0x4000
  Shared-interface  : Owner
  Link flags        : No-Keepalives DTE
  ANSI LMI settings: n391dte 6, n392dte 3, n393dte 4, t391dte 10 seconds
  LMI: Input: 0 (never), Output: 0 (never)
  DTE statistics:
    Enquiries sent                : 0
    Full enquiries sent           : 0
    Enquiry responses received    : 0
    Full enquiry responses received : 0
  DCE statistics:
    Enquiries received            : 0
    Full enquiries received       : 0
    Enquiry responses sent        : 0
    Full enquiry responses sent   : 0
  Common statistics:
    Unknown messages received     : 0
    Asynchronous updates received : 0
    Out-of-sequence packets received : 0
    Keepalive responses timedout  : 0
  CoS queues      : 8 supported, 8 maximum usable queues
  Last flapped    : 2008-08-11 10:51:51 PDT (1w1d 04:47 ago)
  Input rate      : 0 bps (0 pps)
  Output rate     : 0 bps (0 pps)
  SONET alarms    : LOL, PLL
  SONET defects   : LOL, PLL, LOF, SEF, AIS-L, AIS-P

  Logical interface so-7/2/0.0 (Index 67) (SNMP ifIndex 117)

```

```
Flags: Device-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: FR-NLPID
Shared interface:
  Shared with: psd5
  Tunnel token: Rx: 2.517, Tx: 1.517
Input packets : 0
Output packets: 0
DLCI 700
  Flags: Active
  Total down time: 00:01:09 sec, Last down: 284:58:21 ago
    Input packets : 0
    Output packets: 0
DLCI statistics:
  Active DLCI   :1  Inactive DLCI   :0
```

show interfaces diagnostics optics (SONET)

Syntax

```
show interfaces diagnostics optics so-fpc/pic/port
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

(M320, T320, T640, and T1600 routers only) For SONET/SDH interfaces that support optical diagnostics and monitoring, display transceiver diagnostics and data alarms.

Options

so-*fpc/pic/port*—SONET/SDH interface name.

Additional Information

The transceivers are polled in 1-second intervals for diagnostics data, alarms, and warnings and stores them into memory. The alarms will not cause the links to go down or the LEDs to change color or generate SNMP traps. Changes in alarm and warning status will generate system log messages.

Thresholds that trigger a high alarm, low alarm, high warning, or low warning are set by the transceiver vendors. Generally, a high alarm or low alarm indicates that the optics module is not operating properly. This information can be used to diagnose why a PIC is not working.

In the output fields, when an alarm is **On**, this indicates an error condition. Alarm **Off** indicates normal operation.

NOTE: The **show interfaces diagnostics optics** command for optical interfaces does not report the decibel (dBm) value of the received signal if the received power is zero milliwatts (0.0000 mW).

Required Privilege Level

view

RELATED DOCUMENTATION

[SONET/SDH Interfaces Overview](#) | 2

List of Sample Output

[show interfaces diagnostics optics \(OC768 PIC\) on page 382](#)

[show interfaces diagnostics optics \(Multi-rate SONET/SDH PICs with SFP\) on page 383](#)

[show interfaces diagnostics optics \(OC192 PICs with XFP\) on page 384](#)

Output Fields

Table 31 on page 374 lists the output fields for the **show interfaces diagnostics optics** command for OC768 PICs. Output fields are listed in the approximate order in which they appear.

Table 31: OC768 PIC show interfaces diagnostics optics Output Fields

Field Name	Field Description
Physical interface	Name of the physical interface.
Laser bias current	Magnitude of the laser bias power setting current, in milliamperes. This indicator is a software equivalent to the LsBIASMON pin in hardware.
Laser output power	Laser output power, in milliwatts (mW) and decibels, referenced to 1.0 mW (dBm). This is a software equivalent to the LsPOWMON pin in hardware.
Receiver signal average optical power	Average received optical power, in mW and dBm. This indicator is a software equivalent to the RxPOWMON pin in hardware. Average optical power is vendor-specific.
Laser end-of-life alarm	Laser end-of-life alarm: On or Off .
Laser wavelength alarm	Laser wavelength alarm: On or Off .
Laser bias current alarm	Laser bias current alarm: On or Off .
Laser temperature alarm	Laser temperature alarm: On or Off .
Laser power alarm	Laser power alarm: On or Off .
Modulator temperature alarm	Modulator temperature alarm: On or Off . Transceivers from some vendors do not support this field.
Modulator bias alarm	Modulator bias alarm: On or Off .
Tx multiplexer FIFO error alarm	Transmit multiplexer first in, first out (FIFO) error alarm: On or Off .

Table 31: OC768 PIC show interfaces diagnostics optics Output Fields (*continued*)

Field Name	Field Description
Tx loss of PLL lock alarm	Transmit loss of phase-locked loop (PLL) lock alarm: On or Off .
Rx loss of average optical power alarm	Receive loss of average optical power alarm: On or Off .
Rx loss of AC power alarm	Receive loss of AC power alarm: On or Off . Transceivers from some vendors do not support this field.
Rx loss of PLL lock alarm	Receive loss of phase-locked loop (PLL) lock alarm: On or Off .

Table 32 on page 375 lists the output fields for the **show interfaces diagnostics optics** command for multi-rate SONET/SDH PICs with SFP transceivers. Output fields are listed in the approximate order in which they appear.

Table 32: Multi-Rate SONET/SDH PICs with SFP show interfaces diagnostics optics Output Fields

Field Name	Field Description
Physical interface	Name of the physical interface.
Laser bias current	Magnitude of the laser bias power setting current, in milliamperes. The laser bias provides direct modulation of laser diodes and modulates currents.
Laser output power	Laser output power, in milliwatts (mW) and decibels, referenced to 1.0 mW (dBm).
Module temperature	Temperature of the XFP optics module, in Celsius and Fahrenheit.
Module voltage	Internally measured module voltage.
Receiver signal average optical power	Average received optical power, in mW and dBm.
Laser bias current high alarm	Laser bias power setting high alarm. Displays on or off .
Laser bias current low alarm	Laser bias power setting low alarm. Displays on or off .

Table 32: Multi-Rate SONET/SDH PICs with SFP show interfaces diagnostics optics Output Fields (*continued*)

Field Name	Field Description
Laser bias current high warning	Laser bias power setting high warning. Displays on or off .
Laser bias current low warning	Laser bias power setting low warning. Displays on or off .
Laser output power high alarm	Laser output power high alarm. Displays on or off .
Laser output power low alarm	Laser output power low alarm. Displays on or off .
Laser output power high warning	Laser output power high warning. Displays on or off .
Laser output power low warning	Laser output power low warning. Displays on or off .
Module temperature high alarm	Module temperature high alarm. Displays on or off .
Module temperature low alarm	Module temperature low alarm. Displays on or off .
Module temperature high warning	Module temperature high warning. Displays on or off .
Module temperature low warning	Module temperature low warning. Displays on or off .
Module voltage high alarm	Module voltage high alarm. Displays on or off .
Module voltage low alarm	Module voltage low alarm. Displays on or off .
Module voltage high warning	Module voltage high warning . Displays on or off .
Module voltage low warning	Module voltage high warning . Displays on or off .

Table 32: Multi-Rate SONET/SDH PICs with SFP show interfaces diagnostics optics Output Fields (*continued*)

Field Name	Field Description
Laser rx power high alarm	Receive laser power high alarm. Displays on or off .
Laser rx power low alarm	Receive laser power low alarm. Displays on or off .
Laser rx power high warning	Receive laser power high warning. Displays on or off .
Laser rx power low warning	Receive laser power low warning. Displays on or off .
Laser bias current high alarm threshold	Vendor-specified threshold for the laser bias current high alarm: 80.000 mA .
Laser bias current low alarm threshold	Vendor-specified threshold for the laser bias current low alarm: 2.000 mA .
Laser bias current high warning threshold	Vendor-specified threshold for the laser bias current high warning: 70.000 mA .
Laser bias current low warning threshold	Vendor-specified threshold for the laser bias current low warning: 4.000 mA .
Laser output power high alarm threshold	Vendor-specified threshold for the laser output power high alarm: 1.2600 mW or 1.00 dBm .
Laser output power low alarm threshold	Vendor-specified threshold for the laser output power low alarm: 0.0440 mW or -13.57 dBm .
Laser output power high warning threshold	Vendor-specified threshold for the laser output power high warning: 0.7950 mW or -1.00 dBm .
Laser output power low warning threshold	Vendor-specified threshold for the laser output power low warning: 0.0700 mW or -11.55 dBm .
Module temperature high alarm threshold	Vendor-specified threshold for the module temperature high alarm: 110° C or 230° F .

Table 32: Multi-Rate SONET/SDH PICs with SFP show interfaces diagnostics optics Output Fields (*continued*)

Field Name	Field Description
Module temperature low alarm threshold	Vendor-specified threshold for the module temperature low alarm: -40° C or -40° F .
Module temperature high warning threshold	Vendor-specified threshold for the module temperature high warning: 93° C or 199° F .
Module temperature low warning threshold	Vendor-specified threshold for the module temperature low warning: -30° C or -22° F .
Module voltage high alarm threshold	Module voltage high alarm threshold: 3.900 v .
Module voltage low alarm threshold	Module voltage low alarm threshold: 2.700 v .
Module voltage high warning threshold	Module voltage high warning threshold: 3.700 v .
Module voltage low warning threshold	Module voltage high warning threshold: 2.900 v .
Laser rx power high alarm threshold	Vendor-specified threshold for the laser Rx power high alarm: 1.1749 mW or 0.70 dBm .
Laser rx power low alarm threshold	Vendor-specified threshold for the laser Rx power low alarm: 0.0039 mW or -24.09 dBm .
Laser rx power high warning threshold	Vendor-specified threshold for the laser Rx power high warning: 0.7942 mW or 1.00 dBm .
Laser rx power low warning threshold	Vendor-specified threshold for the laser Rx power low warning: 0.0100 mW or -20.00 dBm .

Table 33 on page 379 lists the output fields for the **show interfaces diagnostics optics** command for OC192 PICs with XFP transceivers. Output fields are listed in the approximate order in which they appear.

Table 33: OC192 PIC with XFP show interfaces diagnostics optics Output Fields

Field Name	Field Description
Physical interface	Name of the physical interface.
Link	(For 4-port OC192c PIC operating in OC768-over-4xOC192 mode) The link number. Diagnostics and alarms are displayed for each link.
Laser bias current	Magnitude of the laser bias power setting current, in milliamperes. The laser bias provides direct modulation of laser diodes and modulates currents.
Laser output power	Laser output power, in milliwatts (mW) and decibels, referenced to 1.0 mW (dBm). This is a software equivalent to the LsPOWMON pin in hardware.
Module temperature	Temperature of the XFP optics module, in Celsius and Fahrenheit.
Laser rx power	Laser received optical power, in mW and dBm.
Laser bias current high alarm	Laser bias power setting high alarm. Displays on or off .
Laser bias current low alarm	Laser bias power setting low alarm. Displays on or off .
Laser bias current high warning	Laser bias power setting high warning. Displays on or off .
Laser bias current low warning	Laser bias power setting low warning. Displays on or off .
Laser output power high alarm	Laser output power high alarm. Displays on or off .
Laser output power low alarm	Laser output power low alarm. Displays on or off .
Laser output power high warning	Laser output power high warning. Displays on or off .
Laser output power low warning	Laser output power low warning. Displays on or off .
Module temperature high alarm	Module temperature high alarm. Displays on or off .

Table 33: OC192 PIC with XFP show interfaces diagnostics optics Output Fields (*continued*)

Field Name	Field Description
Module temperature low alarm	Module temperature low alarm. Displays on or off .
Module temperature high warning	Module temperature high warning. Displays on or off .
Module temperature low warning	Module temperature low warning. Displays on or off .
Laser rx power high alarm	Receive laser power high alarm. Displays on or off .
Laser rx power low alarm	Receive laser power low alarm. Displays on or off .
Laser rx power high warning	Receive laser power high warning. Displays on or off .
Laser rx power low warning	Receive laser power low warning. Displays on or off .
Module not ready alarm	Module not ready alarm. When on , indicates the module has an operational fault. Displays on or off .
Module power down alarm	Module power down alarm. When on , module is in a limited power mode, low for normal operation. Displays on or off .
Tx data not ready alarm	Any condition leading to invalid data on the transmit path. Displays on or off .
Tx not ready alarm	Any condition leading to invalid data on the transmit path. Displays on or off .
Tx laser fault alarm	Laser fault condition. Displays on or off .
Tx CDR loss of lock alarm	Transmit clock and data recovery (CDR) loss of lock. Loss of lock on the transmit side of the CDR. Displays on or off .
Rx not ready alarm	Any condition leading to invalid data on the receive path. Displays on or off .
Rx loss of signal alarm	Receive Loss of Signal alarm. When on , indicates insufficient optical input power to the module. Displays on or off .

Table 33: OC192 PIC with XFP show interfaces diagnostics optics Output Fields (continued)

Field Name	Field Description
Rx CDR loss of lock alarm	Receive CDR loss of lock. Loss of lock on the receive side of the CDR. Displays on or off .
Laser bias current high alarm threshold	Vendor-specified threshold for the laser bias current high alarm: 130.000 mA .
Laser bias current low alarm threshold	Vendor-specified threshold for the laser bias current low alarm: 10.000 mA .
Laser bias current high warning threshold	Vendor-specified threshold for the laser bias current high warning: 120.000 mA .
Laser bias current low warning threshold	Vendor-specified threshold for the laser bias current low warning: 12.000 mA .
Laser output power high alarm threshold	Vendor-specified threshold for the laser output power high alarm: 0.8910 mW or -0.50 dBm .
Laser output power low alarm threshold	Vendor-specified threshold for the laser output power low alarm: 0.2230 mW or -6.52 dBm .
Laser output power high warning threshold	Vendor-specified threshold for the laser output power high warning: 0.7940 mW or -100 dBm .
Laser output power low warning threshold	Vendor-specified threshold for the laser output power low warning: 0.2510 mW or -600dBm .
Module temperature high alarm threshold	Vendor-specified threshold for the module temperature high alarm: 90 °C or 194 °F .
Module temperature low alarm threshold	Vendor-specified threshold for the module temperature low alarm: -5 °C or 23 °F .
Module temperature high warning threshold	Vendor-specified threshold for the module temperature high warning: 85 °C or 185 °F .

Table 33: OC192 PIC with XFP show interfaces diagnostics optics Output Fields (*continued*)

Field Name	Field Description
Module temperature low warning threshold	Vendor-specified threshold for the module temperature low warning: 0 °C or 32 °F .
Laser rx power high alarm threshold	Vendor-specified threshold for the laser Rx power high alarm: 1.2589 mW or 1.00 dBm .
Laser rx power low alarm threshold	Vendor-specified threshold for the laser Rx power low alarm: 0.0323 mW or -14.91 dBm .
Laser rx power high warning threshold	Vendor-specified threshold for the laser Rx power high warning: 1.1220 mW or 0.50 dBm .
Laser rx power low warning threshold	Vendor-specified threshold for the laser Rx power low warning: 0.0363 mW or -14.40 dBm .

Sample Output

show interfaces diagnostics optics (OC768 PIC)

user@host> show interfaces diagnostics optics so-4/0/0

```
Physical interface: so-4/0/0
  Laser bias current           : 79.938 mA
  Laser output power          : 1.592 mW / 2.02 dBm
  Receiver signal average optical power : 1.3854 mW / 1.42 dBm
  Laser end-of-life alarm      : Off
  Laser wavelength alarm      : Off
  Laser bias current alarm     : Off
  Laser temperature alarm      : Off
  Laser power alarm            : Off
  Modulator temperature alarm  : Off
  Modulator bias alarm        : Off
  Tx multiplexer FIFO error alarm : Off
  Tx loss of PLL lock alarm    : Off
  Rx loss of average optical power alarm: Off
  Rx loss of AC power alarm    : Off
  Rx loss of PLL lock alarm    : Off
```


show interfaces diagnostics optics (Multi-rate SONET/SDH PICs with SFP)

```
user@host> show interfaces diagnostics optics so-1/0/0
```

```
Physical interface: so-1/0/0
  Laser bias current           : 24.008 mA
  Laser output power           : 0.2620 mW / -5.82 dBm
  Module temperature           : 62 degrees C / 144 degrees F
  Module voltage               : 3.3280 V
  Receiver signal average optical power : 0.2685 mW / -5.71 dBm
  Laser bias current high alarm : Off
  Laser bias current low alarm  : Off
  Laser bias current high warning : Off
  Laser bias current low warning : Off
  Laser output power high alarm  : Off
  Laser output power low alarm   : Off
  Laser output power high warning : Off
  Laser output power low warning : Off
  Module temperature high alarm  : Off
  Module temperature low alarm   : Off
  Module temperature high warning : Off
  Module temperature low warning : Off
  Module voltage high alarm      : Off
  Module voltage low alarm       : Off
  Module voltage high warning    : Off
  Module voltage low warning     : Off
  Laser rx power high alarm      : Off
  Laser rx power low alarm       : Off
  Laser rx power high warning    : Off
  Laser rx power low warning     : Off
  Laser bias current high alarm threshold : 80.000 mA
  Laser bias current low alarm threshold  : 2.000 mA
  Laser bias current high warning threshold : 70.000 mA
  Laser bias current low warning threshold : 4.000 mA
  Laser output power high alarm threshold : 1.2600 mW / 1.00 dBm
  Laser output power low alarm threshold  : 0.0440 mW / -13.57 dBm
  Laser output power high warning threshold : 0.7950 mW / -1.00 dBm
  Laser output power low warning threshold : 0.0700 mW / -11.55 dBm
  Module temperature high alarm threshold : 110 degrees C / 230 degrees F
  Module temperature low alarm threshold  : -40 degrees C / -40 degrees F
  Module temperature high warning threshold : 93 degrees C / 199 degrees F
  Module temperature low warning threshold : -30 degrees C / -22 degrees F
  Module voltage high alarm threshold     : 3.900 V
  Module voltage low alarm threshold       : 2.700 V
  Module voltage high warning threshold    : 3.700 V
```

```

Module voltage low warning threshold      : 2.900 V
Laser rx power high alarm threshold      : 1.1749 mW / 0.70 dBm
Laser rx power low alarm threshold       : 0.0039 mW / -24.09 dBm
Laser rx power high warning threshold    : 0.7942 mW / -1.00 dBm
Laser rx power low warning threshold     : 0.0100 mW / -20.00 dBm

```

show interfaces diagnostics optics (OC192 PICs with XFP)

user@host> show interfaces diagnostics optics so-7/0/0

```

Physical interface: so-7/0/0
Link : 0
Laser bias current                : 50.776 mA
Laser output power                 : 0.4030 mW / -3.95 dBm
Laser temperature                  : 29.0 degrees C / 84.2 degrees F
Laser rx power                    : 0.4671 mW / -3.31 dBm
Laser bias current high alarm      : Off
Laser bias current low alarm       : Off
Laser bias current high warning    : Off
Laser bias current low warning     : Off
Laser output power high alarm      : Off
Laser output power low alarm       : Off
Laser output power high warning    : Off
Laser output power low warning     : Off
Laser temperature high alarm       : Off
Laser temperature low alarm        : Off
Laser temperature high warning     : Off
Laser temperature low warning      : Off
Laser rx power high alarm          : Off
Laser rx power low alarm           : Off
Laser rx power high warning        : Off
Laser rx power low warning         : Off
Module not ready alarm             : Off
Module power down alarm            : Off
Tx data not ready alarm            : Off
Tx not ready alarm                 : Off
Tx laser fault alarm               : Off
Tx CDR loss of lock alarm          : Off
Rx not ready alarm                 : Off
Rx loss of signal alarm            : Off
Rx CDR loss of lock alarm          : Off
Laser bias current high alarm threshold : 130.000 mA
Laser bias current low alarm threshold : 10.000 mA
Laser bias current high warning threshold : 120.000 mA

```

```
Laser bias current low warning threshold : 12.000 mA
Laser output power high alarm threshold  : 0.8910 mW / -0.50 dBm
Laser output power low alarm threshold   : 0.2230 mW / -6.52 dBm
Laser output power high warning threshold : 0.7940 mW / -1.00 dBm
Laser output power low warning threshold  : 0.2510 mW / -6.00 dBm
Laser temperature high alarm threshold    : 90.0 degrees C / 194.0 degrees F
Laser temperature low alarm threshold     : -5.0 degrees C / 23.0 degrees F
Laser temperature high warning threshold  : 85.0 degrees C / 185.0 degrees F
Laser temperature low warning threshold   : 0.0 degrees C / 32.0 degrees F
Laser rx power high alarm threshold       : 1.2589 mW / 1.00 dBm
Laser rx power low alarm threshold        : 0.0323 mW / -14.91 dBm
Laser rx power high warning threshold     : 1.1220 mW / 0.50 dBm
Laser rx power low warning threshold      : 0.0363 mW / -14.40 dBm
...
```