



Junos[®] OS

SONET/SDH Interfaces for Routing Devices

Release
13.2



Published: 2013-08-19

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

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos OS SONET/SDH Interfaces for Routing Devices

13.2

Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

Revision History
August 2013—R1 Junos OS 13.2

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Abbreviated Table of Contents

	About This Guide	xv
Part 1	SONET/SDH Interfaces Configuration Statements Overview	
Chapter 1	SONET/SDH Interfaces Configuration Statements and Hierarchy	3
Part 2	Configuring SONET/SDH Interfaces	
Chapter 2	Configuring SONET/SDH Interfaces	29
Part 3	SONET/SDH Interface Configuration Statements	
Chapter 3	Summary of SONET/SDH Interfaces Configuration Statements	117
Part 4	Troubleshooting	
Chapter 4	Investigating SONET Interfaces	177
Part 5	Index	
	Index	233
	Index of Statements and Commands	241

Table of Contents

	About This Guide	xv
	Documentation and Release Notes	xv
	Supported Routing Platforms	xv
	Using the Examples in This Manual	xvi
	Merging a Full Example	xvi
	Merging a Snippet	xvii
	Documentation Conventions	xvii
	Documentation Feedback	xix
	Requesting Technical Support	xix
	Self-Help Online Tools and Resources	xix
	Opening a Case with JTAC	xx
Part 1	SONET/SDH Interfaces Configuration Statements Overview	
Chapter 1	SONET/SDH Interfaces Configuration Statements and Hierarchy	3
	[edit chassis] Hierarchy Level	3
	[edit interfaces] Hierarchy Level	4
	[edit logical-systems] Hierarchy Level	21
	SONET/SDH Physical Interfaces Configuration Hierarchy	25
Part 2	Configuring SONET/SDH Interfaces	
Chapter 2	Configuring SONET/SDH Interfaces	29
	SONET/SDH Interfaces Overview	31
	SONET/SDH Physical Interface Properties Overview	32
	Configuring SONET/SDH Physical Interface Properties	32
	Configuring SONET/SDH Physical Interface Options	33
	Configuring SONET/SDH Interface-Specific Options	33
	Configuring MPLS Option for Passive Monitoring	35
	Configuring Automatic Protection Switching Options	35
	Framing Mode Overview	38
	Configuring SONET/SDH Framing Mode	39
	Configuring Virtual Tributary Mapping	40
	Incrementing STM ID Overview	41
	Configuring an Incrementing STM ID	41
	SONET/SDH Interface Speed Overview	42
	Configuring SONET/SDH Interface Speed	44
	SONET/SDH Rate-Selectability Overview	45
	Configuring SONET/SDH Rate-Selectability	47
	SONET/SDH Header Byte Values Overview	48
	Configuring SONET/SDH Header Byte Values	50

Configuring the SONET/SDH Frame Checksum	51
Configuring Channelized IQ and IQE SONET/SDH Loop Timing	52
Configuring SONET/SDH Loopback Capability	53
Configuring SONET/SDH Loopback Capability	53
Displaying SONET/SDH Loopback Capability Configuration	54
Determining Problem Is Internal or External with Loopback Capability	55
SONET/SDH Path Trace Identifier Overview	56
Configuring the SONET/SDH Path Trace Identifier	56
SONET/SDH HDLC Payload Scrambling Overview	57
Configuring SONET/SDH HDLC Payload Scrambling	57
SONET/SDH RFC 2615 Support Overview	58
Configuring SONET/SDH RFC 2615 Support	59
SONET/SDH Defect Triggers to Be Ignored Overview	59
SONET/SDH Defect Hold Times Overview	61
Configuring SONET/SDH Defect Triggers	62
Configuring SONET/SDH Defect Triggers to Be Ignored	63
Configuring SONET/SDH Defect Hold Times	63
Displaying the Configuration for SONET/SDH Defects to Be Ignored	63
Automatic Protection Switching and Multiplex Section Protection Overview	64
Configuring Automatic Protect Switching	66
Basic Automatic Protect Switching Overview	68
Configuring Basic Automatic Protect Switching	68
Example: Configuring Basic APS Support on Routers	69
Container Interfaces for APS on SONET Links Overview	73
Configuring Container Interfaces for APS on SONET Links	74
Configuring Container Interfaces on SONET Links	74
Displaying Container Interface Configuration	76
Displaying the APS Container Interface Configuration	77
APS Using a Container Interface with ATM Encapsulation Overview	77
Configuring APS Using a Container Interface with ATM Encapsulation	78
Displaying APS Using a Container Interface with ATM Encapsulation	78
Displaying APS Using a Container Interface with ATM Encapsulation	78
Displaying the APS Container Interface Configuration	80
Switching Between the Working and Protect Circuits Overview	80
Configuring Annex B Option	82
Configuring Switching Between the Working and Protect Circuits	82
Revertive Mode Overview	84
Configuring Revertive Mode	84
Switching Mode Overview	86
Configuring Switching Mode	87
APS Timers Overview	87
Configuring APS Timers	88
Link PIC Redundancy Overview	89
Configuring Link PIC Redundancy	89
Configuring Link State Replication	89
Displaying Link PIC Redundancy	90
APS Load Sharing Between Circuit Pairs Overview	91
Configuring APS Load Sharing	92
Example: Configuring APS Load Sharing Between Circuit Pairs	92

Configuring SONET Options for 10-Gigabit Ethernet Interfaces	95
Configuring the Media MTU on SONET/SDH Interfaces	96
Enabling Passive Monitoring on SONET/SDH Interfaces	97
Removing MPLS Labels from Incoming Packets	98
Configuring the Clock Source on SONET/SDH Interfaces	99
Receive and Transmit Leaky Bucket Properties Overview	100
Configuring Receive and Transmit Leaky Bucket Properties	101
Damping Interface Transitions	102
Configuring Interface Encapsulation on SONET/SDH Interfaces	102
Configuring the Encapsulation on a Physical SONET/SDH Interface	103
Example: Configuring the Encapsulation on a Physical SONET/SDH Interface	104
Configuring the Encapsulation on a Logical SONET/SDH Interface	105
Example: Configuring SONET/SDH Interfaces	105
Configuring Aggregated SONET/SDH Interfaces	106
Configuring SONET/SDH Link Aggregation	107
Configuring Aggregated SONET/SDH Link Speed	108
Configuring Aggregated SONET/SDH Minimum Links	108
Configuring Filters or Sampling on Aggregated SONET/SDH Links	109
Examples: Configuring Filters or Sampling on Aggregated SONET/SDH Links	109
Example: Configuring Aggregated SONET/SDH Interfaces	110
Configuring Multicast Statistics Collection on Aggregated SONET Interfaces	111
Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode	112

Part 3

Chapter 3

SONET/SDH Interface Configuration Statements

Summary of SONET/SDH Interfaces Configuration Statements	117
advertise-interval	117
aggregate (SONET/SDH)	118
aggregated-sonet-options	118
annex	119
aps	120
atm-options	121
authentication-key	122
bytes	123
clocking	124
container-devices	125
container-list	125
container-options	126
container-type	126
encapsulation	127
encapsulation (Container Interface)	127
encapsulation (Logical Interface)	128
family	132
fast-aps-switch	136
fcs	137
filter	138
force	139

framing (SONET and SDH Interfaces)	140
hold-time	141
hold-time (APS)	141
hold-time (SONET/SDH Defect Triggers)	142
ignore	143
link-speed (Aggregated SONET/SDH)	144
lockout	144
loop-timing	145
loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3)	146
member-interface-speed	147
member-interface-type	148
minimum-links	149
mpls (Interfaces)	150
mtu	151
neighbor (Automatic Protection Switching for SONET/SDH)	153
overflow	154
overflow (Receive Bucket)	154
overflow (Transmit Bucket)	154
paired-group	155
passive-monitor-mode	156
path-trace	157
payload-scrambler	158
pop-all-labels	159
preserve-interface	160
protect-circuit	160
rate	161
receive-bucket	161
receive-options-packets	162
receive-ttl-exceeded	162
request	163
required-depth	164
revert-time (Interfaces)	165
rfc-2615	165
sonet-options	166
speed (SONET/SDH)	168
switching-mode	169
t3-options	170
threshold	171
transmit-bucket	171
trigger	172
vtmapping	173
working-circuit	173
z0-increment	174

Part 4	Troubleshooting	
Chapter 4	Investigating SONET Interfaces	177
	Investigating Interface Steps and Commands	177
	Investigating Interface Steps and Commands Overview	177
	Monitoring Interfaces	177
	Performing a Loopback Test on an Interface	178
	Locating Interface Alarms	180
	Monitoring SONET Interfaces	180
	Checklist for Monitoring SONET Interfaces	181
	Monitoring SONET Interfaces	181
	Displaying the Status of SONET Interfaces	181
	Displaying the Status of a Specific SONET Interface	182
	Displaying Extensive Status Information for a Specific SONET Interface	183
	Monitoring Statistics for a SONET Interface	185
	Verifying the Status of the Logical Interface	187
	Using Loopback Testing for SONET Interfaces	188
	Checklist for Using Loopback Testing for SONET Interfaces	189
	Diagnosing a Suspected Hardware Problem with a SONET Interface	190
	Creating a Loopback	191
	Creating a Physical Loopback	191
	Configuring a Local Loopback	191
	Setting Clocking to Internal	192
	Verifying That the SONET Interface Is Up	192
	Clearing SONET Interface Statistics	194
	Checking That the Received and Transmitted Path Trace Are the Same	194
	Forcing the Link Layer to Stay Up	195
	Configuring Encapsulation to Cisco-HDLC	195
	Configuring No-Keepalives	196
	Pinging the SONET Interface	196
	Checking for SONET Interface Error Statistics	197
	Diagnosing a Suspected Circuit Problem	198
	Creating a Loop from the Router to the Network	198
	Creating a Loop to the Router from Various Points in the Network	199
	Locating SONET Alarms and Errors	200
	List of Common SONET Alarms and Errors	200
	Displaying SONET Alarms and Errors	201
	Locating Most Common SONET Alarms and Errors	204
	Locating Loss of Signal Alarms	205
	Locating Alarm Indication Signal Alarms	206
	Example of a Router Receiving Only an AIS-P Alarm	206
	Example of a Router Receiving Both an AIS-L and AIS-P Alarm	207
	Locating Remote Defect Indication Alarms	207
	Example of a Router Receiving Only an RDI-P Alarm	208
	Example of a Router Receiving Both an RDI-L and RDI-P Alarm	208
	Locating Remote Error Indication Line Errors	209
	Example of Only an REI-P Counter Incrementing	209
	Example of Both REI-L and REI-P Counters Incrementing	210

Locating Bit Error Rate Alarms	211
Locating Payload Label Mismatch Path Alarms	213
Locating Loss of Pointer Path Alarms	215
Locating Unequipped Payload Alarms	216
Locating Phase Lock Loop Alarms	217
Enabling SONET Payload Scrambling	219
Checklist for Enabling SONET Payload Scrambling	219
Understanding SONET Payload Scrambling	220
Checking SONET HDLC Payload Scrambling	221
Configuring SONET HDLC Payload Scrambling	222
Checking the SONET Frame Checksum	223
Checklist for Checking the SONET Frame Checksum	223
Understand the SONET Frame Checksum	224
Checking the SONET Frame Checksum	224
Examining Output for Framing Errors	224
Checking the FCS Configuration	226
Configuring a SONET Frame Checksum	228
Returning to the Default 16-Bit Checksum	228
Configuring a 16-Bit Checksum	228
Configuring a 32-Bit Checksum	229

Part 5

Index

Index	233
Index of Statements and Commands	241

List of Figures

Part 2	Configuring SONET/SDH Interfaces	
Chapter 2	Configuring SONET/SDH Interfaces	29
	Figure 1: APS/MSP Configuration Topologies	65
	Figure 2: APS/MSP Configuration Topologies	70
	Figure 3: APS Load Sharing Between Circuit Pairs	91
	Figure 4: APS Load Sharing Between Circuit Pairs	93
Part 4	Troubleshooting	
Chapter 4	Investigating SONET Interfaces	177
	Figure 5: Example of a SONET Network	202
	Figure 6: Example of an Upstream or Downstream Failure	204
	Figure 7: Another Example of an Upstream or Downstream Failure	204
	Figure 8: Location of an LOS Alarm in a SONET Network	205
	Figure 9: Example of a Router Receiving Only an AIS-P Alarm	206
	Figure 10: Example of a Router Receiving Both an AIS-L and an AIS-P Alarm	207
	Figure 11: Example of a Router Receiving Only an RDI-P Alarm	208
	Figure 12: Example of a Router Receiving Both an RDI-L and RDI-P Alarm	209
	Figure 13: Example of a Router Receiving Only an REI-P Counter Incrementing	210
	Figure 14: Example of a Router Receiving Both An REI-L and REI-P Counter Incrementing	211

List of Tables

	About This Guide	xv
	Table 1: Notice Icons	xvii
	Table 2: Text and Syntax Conventions	xviii
Part 2	Configuring SONET/SDH Interfaces	
Chapter 2	Configuring SONET/SDH Interfaces	29
	Table 3: Type 1 PIC Mode Combinations	43
	Table 4: Type 2 PIC Mode Combinations	43
	Table 5: Port Speed Restrictions for SONET/SDH OC3/STM1 (Multi-Rate) MICs	45
	Table 6: OC12/STM4 Port Configuration Restrictions on MIC-3D-8CHOC3-4CHOC12	46
	Table 7: OC3/STM1 Port Configuration Restrictions on MIC-3D-8CHOC3-4CHOC12	46
	Table 8: OC12/STM4 Port Configuration Restrictions on MIC-3D-4CHOC3-2CHOC12	46
	Table 9: OC3/STM1 Port Configuration Restrictions on MIC-3D-4CHOC3-2CHOC12	47
	Table 10: SONET/SDH Framing Bytes for Specific Speeds	48
	Table 11: SONET/SDH Default Settings	58
	Table 12: SONET/SDH and ATM Active Alarms and Defects	59
Part 4	Troubleshooting	
Chapter 4	Investigating SONET Interfaces	177
	Table 13: Commands Used to Monitor Interfaces	178
	Table 14: Commands Used to Perform Loopback Testing on Interfaces	179
	Table 15: Checklist for Monitoring SONET Interfaces	181
	Table 16: Status of SONET Interfaces	182
	Table 17: SONET Error Statistics	186
	Table 18: Checklist for Using Loopback Testing for SONET Interfaces	189
	Table 19: Problems and Solutions for a Physical Link That Is Down	194
	Table 20: List of Common SONET Alarms and Errors	200
	Table 21: STS Path Signal Label Assignments	214
	Table 22: Location of the Onboard Clock	219
	Table 23: Checklist for Enabling SONET Payload Scrambling	219
	Table 24: Checklist for Checking the SONET Frame Checksum	223

About This Guide

This preface provides the following guidelines for using the *Junos OS SONET/SDH Interfaces for Routing Devices*:

- [Documentation and Release Notes on page xv](#)
- [Supported Routing Platforms on page xv](#)
- [Using the Examples in This Manual on page xvi](#)
- [Documentation Conventions on page xvii](#)
- [Documentation Feedback on page xix](#)
- [Requesting Technical Support on page xix](#)

Documentation and Release Notes

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

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

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

Supported Routing Platforms

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

- J Series
- M Series
- MX Series
- T Series
- ACX Series
- PTX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
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 the *CLI User Guide*.

Documentation Conventions

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

Table 1: Notice Icons





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

Table 2 on page xviii 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 book 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 System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<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)	Enclose optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify 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, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Find product documentation: <http://www.juniper.net/techpubs/>

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

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

Opening a Case with JTAC

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

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

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

PART 1

SONET/SDH Interfaces Configuration Statements Overview

- [SONET/SDH Interfaces Configuration Statements and Hierarchy on page 3](#)

CHAPTER 1

SONET/SDH Interfaces Configuration Statements and Hierarchy

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

This section contains the following topics:

- [\[edit chassis\] Hierarchy Level on page 3](#)
- [\[edit interfaces\] Hierarchy Level on page 4](#)
- [\[edit logical-systems\] Hierarchy Level on page 21](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)

[\[edit chassis\] Hierarchy Level](#)

```
chassis {
  aggregated-devices {
    ethernet {
      device-count number;
    }
    sonet {
      device-count number;
    }
  }
  maximum-links {
  }
  channel-group number {
    ethernet {
      device-count number;
    }
    fpc slot-number {
      pic pic-number {
        adaptive-services {
          service-package (layer-2 | layer-3);
        }
        aggregate-ports;
        atm-cell-relay-accumulation;
```

```

atm-l2circuit-mode (aal5 | cell | trunk trunk);
cel {
    el link-number {
        channel-group group-number;
        timeslots time-slot-range;
    }
}
channelization;
ctl {
    tl link-number {
        channel-group group-number;
        timeslots time-slot-range;
    }
}
ct3 {
    port port-number {
        tl link-number {
            channel-group group-number;
            timeslots time-slot-range;
        }
    }
    framing sdh;
}
max-queues-per-interface number;
mlfr-uni-nni-bundles num-intf;
no-concatenate;
shdsl {
    pic-mode (1-port-atm | 2-port-atm);
}
vtmapping (klm | itu-t);
}
}
fpc slot-number{
pic pic-number{
    account-layer2-overhead
    egress-policer-overhead bytes;
    ingress-policer-overhead bytes;
}
}
}
}

```

[edit interfaces] Hierarchy Level

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



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


```

interfaces {
  traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable |
      no-world-readable> ;
    flag flag <disable>;
  }
  interface-name {
    account-layer2-overhead (Interface Level) {
      value;
      egress bytes;
      ingress bytes;
    }
    accounting-profile name;
    aggregated-ether-options {
      (flow-control | no-flow-control);
      lacp {
        (active | passive);
        link-protection {
          disable;
          (revertive | non-revertive);
          periodic interval;
          system-priority priority;
        }
      }
      link-protection;
      link-speed speed;
      (loopback | no-loopback);
      mc-ae {
        chassis-id chassis-id;
        mc-ae-id mc-ae-id;
        mode (active-active | active-standby);
        redundancy-group group-id;
        status-control (active | standby);
      }
      minimum-links number;
      source-address-filter {
        mac-address;
      }
      (source-filtering | no-source-filtering);
    }
    shared-scheduler;
    aggregated-sonet-options {
      link-speed speed | mixed;
      minimum-links number;
    }
    atm-options {
      cell-bundle-size cells;
      ilmi;
      linear-red-profiles profile-name {
        high-plp-max-threshold percent;
        low-plp-max-threshold percent;
        queue-depth cells high-plp-threshold percent low-plp-threshold percent;
      }
      mpls {
        pop-all-labels {
          required-depth number;
        }
      }
    }
  }
}

```

```

}
pic-type (atm1 | atm2);
plp-to-clp;
promiscuous-mode {
    vpi vpi-identifier;
}
scheduler-maps map-name {
    forwarding-class class-name {
        epd-threshold cells plp1 cells;
        linear-red-profile profile-name;
        priority (high | low);
        transmit-weight (cells number | percent number);
    }
    vc-cos-mode (alternate | strict);
}
use-null-cw;
vpi vpi-identifier {
    maximum-vcs maximum-vcs;
    oam-liveness {
        down-count cells;
        up-count cells;
    }
    oam-period (seconds | disable);
    shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
        burst length);
        queue-length number;
    }
}
}
}
clocking clock-source;
data-input (system | interface interface-name);
dce;
serial-options {
    clock-rate rate;
    clocking-mode (dce | internal | loop);
    control-polarity (negative | positive);
    cts-polarity (negative | positive);
    dcd-polarity (negative | positive);
    dce-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dtr signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
    dsr-polarity (negative | positive);
    dte-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
    }
}

```

```

    dtr signal-handling-option;
    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}
dtr-circuit (balanced | unbalanced);
dtr-polarity (negative | positive);
encoding (nrz | nrzi);
indication-polarity (negative | positive);
line-protocol protocol;
loopback mode;
rts-polarity (negative | positive);
tm-polarity (negative | positive);
transmit-clock invert;
}
description text;
dialer-options {
    pool pool-name <priority priority>;
}
disable;
ds0-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx56 | nx64);
    fcs (16 | 32);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback payload;
    start-end-flag (filler | shared);
}
e1-options {
    bert-error-rate rate;
    bert-period seconds;
    fcs (16 | 32);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (local | remote);
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
e3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    framing feet;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (16 | 32);
    framing (g.751 | g.832);
    idle-cycle-flag (filler | shared);
    invert-data;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);

```

```
    start-end-flag (filler | shared);
    (unframed | no-unframed);
}
encapsulation type;
es-options {
    backup-interface es-fpc/pic/port;
}
fastether-options {
    802.3ad aex;
    (flow-control | no-flow-control);
    ignore-l3-incompletes;
    ingress-rate-limit rate;
    (loopback | no-loopback);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
}
flexible-vlan-tagging;
gigether-options {
    802.3ad aex;
    (asynchronous-notification | no-asynchronous-notification);
    (auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
        local-interface-offline>;
    auto-reconnect seconds;
    (flow-control | no-flow-control);
    ignore-l3-incompletes;
    (loopback | no-loopback);
    mpls {
        pop-all-labels {
            required-depth number;
        }
    }
    no-auto-mdix;
    source-address-filter {
        mac-address;
    }
    (source-filtering | no-source-filtering);
    ethernet-switch-profile {
        (mac-learn-enable | no-mac-learn-enable);
        tag-protocol-id [ tpids ];
        ethernet-policer-profile {
            input-priority-map {
                ieee802.1p premium [ values ];
            }
            output-priority-map {
                classifier {
                    premium {
                        forwarding-class class-name {
                            loss-priority (high | low);
                        }
                    }
                }
            }
        }
    }
}
```

9

```

    t310 seconds;
    tei-option (first-call | power-up);
}
keepalives <down-count number> <interval seconds> <up-count number>;
link-mode mode;
lmi {
    lmi-type (ansi | itu | c-lmi);
    n391dte number;
    n392dce number;
    n392dte number;
    n393dce number;
    n393dte number;
    t391dte seconds;
    t392dce seconds;
}
lsq-failure-options {
    no-termination-request;
    [ trigger-link-failure interface-name ];
}
mac mac-address;
mlfr-uni-nni-bundle-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    drop-timeout milliseconds;
    fragment-threshold bytes;
    cisco-interoperability send-lip-remove-link-for-link-reject;
    hello-timer milliseconds;
    link-layer-overhead percent;
    lmi-type (ansi | itu | c-lmi);
    minimum-links number;
    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 seconds;
    t392 seconds;
    yellow-differential-delay milliseconds;
}
modem-options {
    dialin (console | routable);
    init-command-string initialization-command-string;
}
mtu bytes;
multi-chassis-protection {
    peer a.b.c.d {
        interface interface-name;
    }
}
multiservice-options {
    (core-dump | no-core-dump);
    (syslog | no-syslog);
}
native-vlan-id number;
no-gratuitous-arp-request;

```

```

no-keepalives;
no-partition {
    interface-type type;
}
no-vpivci-swapping;
optics-options {
    alarm low-light-alarm {
        (link-down | syslog);
    }
    tx-power dbm;
    warning low-light-warning {
        (link-down | syslog);
    }
    wavelength nm;
}
otn-options {
    bytes transmit-payload-type value;
    fec (efec | gfec | gfec-sdfec | none);
    (is-ma | no-is-ma);
    (laser-enable | no-laser-enable);
    (line-loopback | no-line-loopback);
    (local-loopback | no-local-loopback);
    (odu-ttim-action-enable | no-odu-ttim-action-enable);
    (otu-ttim-action-enable | no-otu-ttim-action-enable);
    odu-delay-management {
        (bypass | no-bypass);
        (monitor-end-point | no-monitor-end-point);
        (number-of-frames | no-number-of-frames);
        (start-measurement | no-start-measurement);
    }
    (prbs | no-prbs);
    preemptive-fast-reroute {
        (backward-frr-enable | no-backward-frr-enable);
        (signal-degrade-monitor-enable | no-signal-degrade-monitor-enable);
    }
    rate {
        (fixed-stuff-bytes | no-fixed-stuff-bytes);
        otu4;
        (pass-through | no-pass-through);
    }
    signal-degrade {
        ber-threshold-clear value;
        ber-threshold-signal-degrade value;
        interval value;
    }
    trigger trigger-identifier;
    tti tti-identifier;
}
partition partition-number oc-slice oc-slice-range interface-type type;
timeslots time-slot-range;
passive-monitor-mode;
per-unit-scheduler;
ppp-options {
    chap {
        access-profile name;
        default-chap-secret name;
    }
}

```

```
    local-name name;  
    passive;  
  }  
  compression {  
    acfc;  
    pfc;  
  }  
  dynamic-profile profile-name;  
  no-termination-request;  
  pap {  
    access-profile name;  
    local-name name;  
    local-password password;  
    compression;  
  }  
}  
psn-vcip psn-vci-identifier;  
psn-vpip psn-vpi-identifier;  
receive-bucket {  
  overflow (discard | tag);  
  rate percentage;  
  threshold bytes;  
}  
redundancy-options {  
  priority sp-fpc/pic/port;  
  secondary sp-fpc/pic/port;  
  hot-standby;  
}  
satop-options {  
  payload-size n;  
}  
schedulers number;  
serial-options {  
  clock-rate rate;  
  clocking-mode (dce | internal | loop);  
  control-polarity (negative | positive);  
  cts-polarity (negative | positive);  
  dcd-polarity (negative | positive);  
  dce-options {  
    control-signal (assert | de-assert | normal);  
    cts (ignore | normal | require);  
    dcd (ignore | normal | require);  
    dsr (ignore | normal | require);  
    dtr signal-handling-option;  
    ignore-all;  
    indication (ignore | normal | require);  
    rts (assert | de-assert | normal);  
    tm (ignore | normal | require);  
  }  
  dsr-polarity (negative | positive);  
  dte-options {  
    control-signal (assert | de-assert | normal);  
    cts (ignore | normal | require);  
    dcd (ignore | normal | require);  
    dsr (ignore | normal | require);  
    dtr signal-handling-option;
```



```

    ignore-all;
    indication (ignore | normal | require);
    rts (assert | de-assert | normal);
    tm (ignore | normal | require);
}
dtr-circuit (balanced | unbalanced);
dtr-polarity (negative | positive);
encoding (nrz | nrzi);
indication-polarity (negative | positive);
line-protocol protocol;
loopback mode;
rts-polarity (negative | positive);
tm-polarity (negative | positive);
transmit-clock invert;
}
services-options {
    inactivity-timeout seconds;
    open-timeout seconds;
    session-limit {
        maximum number;
        rate new-sessions-per-second;
    }
    syslog {
        host hostname {
            facility-override facility-name;
            log-prefix prefix-number;
            services priority-level;
        }
    }
}
shdsl-options {
    annex (annex-a | annex-b);
    line-rate line-rate;
    loopback (local | remote);
    snr-margin {
        current margin;
        snext margin;
    }
}
sonet-options {
    aggregate asx;
    aps {
        advertise-interval milliseconds;
        annex-b;
        authentication-key key;
        fast-aps-switch;
        force;
        hold-time milliseconds;
        lockout;
        neighbor address;
        paired-group group-name;
        preserve-interface;
        protect-circuit group-name;
        request;
        revert-time seconds;
        switching-mode (bidirectional | unidirectional);
    }
}

```

```

    working-circuit group-name;
}
bytes {
    c2 value;
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
}
fcs (16 | 32);
loopback (local | remote);
mpls {
    pop-all-labels {
        required-depth number;
    }
}
path-trace trace-string;
(payload-scrambler | no-payload-scrambler);
rfc-2615;
trigger {
    defect ignore;
    hold-time up milliseconds down milliseconds;
}
vtmapping (itu-t | klm);
(z0-increment | no-z0-increment);
}
speed (10m | 100m | 1g | oc3 | oc12 | oc48);
stacked-vlan-tagging;
switch-options {
    switch-port port-number {
        (auto-negotiation | no-auto-negotiation);
        speed (10m | 100m | 1g);
        link-mode (full-duplex | half-duplex);
    }
}
t1-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    buildout value;
    byte-encoding (nx56 | nx64);
    crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);
    crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);
    fcs (16 | 32);
    framing (esf | sf);
    idle-cycle-flag (flags | ones);
    invert-data;
    line-encoding (ami | b8zs);
    loopback (local | payload | remote);
    remote-loopback-respond;
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
t3-options {

```

```

atm-encapsulation (direct | plcp);
bert-algorithm algorithm;
bert-error-rate rate;
bert-period seconds;
buildout feet;
(cbit-parity | no-cbit-parity);
compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate
    value>;
fcs (16 | 32);
(feac-loop-respond | no-feac-loop-respond);
idle-cycle-flag value;
(long-buildout | no-long-buildout);
(loop-timing | no-loop-timing);
loopback (local | payload | remote);
(mac | no-mac);
(payload-scrambler | no-payload-scrambler);
start-end-flag (filler | shared);
}
traceoptions {
    flag flag <flag-modifier> <disable>;
}
transmit-bucket {
    overflow discard;
    rate percentage;
    threshold bytes;
}
(traps | no-traps);
unidirectional;
vlan-tagging;
vlan-vci-tagging;
unit logical-unit-number {
    accept-source-mac {
        mac-address mac-address {
            policer {
                input cos-policer-name;
                output cos-policer-name;
            }
        }
    }
}
account-layer2-overhead {
    value;
    egress bytes;
    ingress bytes;
}
accounting-profile name;
advisory-options {
    downstream-rate rate;
    upstream-rate rate;
}
allow-any-vci;
atm-scheduler-map (map-name | default);
backup-options {
    interface interface-name;
}
bandwidth rate;
cell-bundle-size cells;

```

```

clear-dont-fragment-bit;
compression {
  rtp {
    f-max-period number;
    maximum-contexts number <force>;
    queues [ queue-numbers ];
    port {
      minimum port-number;
      maximum port-number;
    }
  }
}
compression-device interface-name;
copy-tos-to-outer-ip-header;
demux-destination family;
demux-source family;
demux-options {
  underlying-interface interface-name;
}
description text;
interface {
  l2tp-interface-id name;
  (dedicated | shared);
}
dialer-options {
  activation-delay seconds;
  callback;
  callback-wait-period time;
  deactivation-delay seconds;
  dial-string [ dial-string-numbers ];
  idle-timeout seconds;
  incoming-map {
    caller (caller-id | accept-all);
    initial-route-check seconds;
    load-interval seconds;
    load-threshold percent;
    pool pool-name;
    redial-delay time;
    watch-list {
      [ routes ];
    }
  }
}
disable;
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
  activation-priority priority;
  bearer-bandwidth-limit kilobits-per-second;
}
encapsulation type;
epd-threshold cells plp1 cells;
fragment-threshold bytes;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {

```

```

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

```

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

```

group filter-group-number;
input filter-name;
input-list {
    [ filter-names ];
    output filter-name;
}
output-list {
    [ filter-names ];
}
}
ipsec-sa sa-name;
keep-address-and-control;
max-sessions number;
max-sessions-vs-a-ignore;
mtu bytes;
multicast-only;
negotiate-address;
no-redirects;
policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}
primary;
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check {
    fail-filter filter-name;
    mode loose;
}
sampling {
    direction;
}
}
service {
    input {
        service-set service-set-name <service-filter filter-name>;
        post-service-filter filter-name;
    }
    output {
        service-set service-set-names <service-filter filter-name>;
    }
}
}
service-name-table table-name;
short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
maximum-seconds>;
targeted-broadcast {
    forward-and-send-to-re;
    forward-only;
}
}
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-beecn | no-translate-fecn-and-beecn);
translate-plp-control-word-de;
unnumbered-address interface-name <destination address destination-profile
profile-name | preferred-source-address address>;

```

```

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

```

Related Documentation

- [Junos OS Hierarchy and RFC Reference](#)
- [Ethernet Interfaces](#)

- *Junos OS Network Interfaces Library for Routing Devices*

[\[edit logical-systems\] Hierarchy Level](#)

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

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

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

```

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

```

```

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

```

Related Documentation

- *Junos OS Hierarchy and RFC Reference*
- *Ethernet Interfaces*
- *Junos OS Network Interfaces Library for Routing Devices*

```
force;
hold-time milliseconds;
lockout;
neighbor address;
paired-group group-name;
preserve-interface
protect-circuit group-name;
request;
revert-time seconds;
switching-mode (bidirectional | unidirectional);
working-circuit group-name;
}
bytes {
  c2 value;
  e1-quiet value;
  f1 value;
  f2 value;
  s1 value;
  z3 value;
  z4 value;
}
fcs (16 | 32);
loopback (local | remote | payload);
mpls {
  pop-all-labels {
    required-depth number;
  }
}
path-trace trace-string;
(payload-scrambler | no-payload-scrambler);
rfc-2615;
trigger {
  defect ignore;
  defect hold-time up milliseconds down milliseconds;
}
}
vtmapping (itu-t | klm);
(z0-increment | no-z0-increment);
speed (oc3 | oc12 | oc48);
```

**Related
Documentation**

- [SONET/SDH Physical Interface Properties Overview on page 32](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)

PART 2

Configuring SONET/SDH Interfaces

- [Configuring SONET/SDH Interfaces on page 29](#)

CHAPTER 2

Configuring SONET/SDH Interfaces

- [SONET/SDH Interfaces Overview on page 31](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Framing Mode Overview on page 38](#)
- [Configuring SONET/SDH Framing Mode on page 39](#)
- [Configuring Virtual Tributary Mapping on page 40](#)
- [Incrementing STM ID Overview on page 41](#)
- [Configuring an Incrementing STM ID on page 41](#)
- [SONET/SDH Interface Speed Overview on page 42](#)
- [Configuring SONET/SDH Interface Speed on page 44](#)
- [SONET/SDH Rate-Selectability Overview on page 45](#)
- [Configuring SONET/SDH Rate-Selectability on page 47](#)
- [SONET/SDH Header Byte Values Overview on page 48](#)
- [Configuring SONET/SDH Header Byte Values on page 50](#)
- [Configuring the SONET/SDH Frame Checksum on page 51](#)
- [Configuring Channelized IQ and IQE SONET/SDH Loop Timing on page 52](#)
- [Configuring SONET/SDH Loopback Capability on page 53](#)
- [SONET/SDH Path Trace Identifier Overview on page 56](#)
- [Configuring the SONET/SDH Path Trace Identifier on page 56](#)
- [SONET/SDH HDLC Payload Scrambling Overview on page 57](#)
- [Configuring SONET/SDH HDLC Payload Scrambling on page 57](#)
- [SONET/SDH RFC 2615 Support Overview on page 58](#)
- [Configuring SONET/SDH RFC 2615 Support on page 59](#)
- [SONET/SDH Defect Triggers to Be Ignored Overview on page 59](#)
- [SONET/SDH Defect Hold Times Overview on page 61](#)
- [Configuring SONET/SDH Defect Triggers on page 62](#)
- [Automatic Protection Switching and Multiplex Section Protection Overview on page 64](#)
- [Configuring Automatic Protect Switching on page 66](#)

- [Basic Automatic Protect Switching Overview on page 68](#)
- [Configuring Basic Automatic Protect Switching on page 68](#)
- [Example: Configuring Basic APS Support on Routers on page 69](#)
- [Container Interfaces for APS on SONET Links Overview on page 73](#)
- [Configuring Container Interfaces for APS on SONET Links on page 74](#)
- [APS Using a Container Interface with ATM Encapsulation Overview on page 77](#)
- [Configuring APS Using a Container Interface with ATM Encapsulation on page 78](#)
- [Displaying APS Using a Container Interface with ATM Encapsulation on page 78](#)
- [Switching Between the Working and Protect Circuits Overview on page 80](#)
- [Configuring Annex B Option on page 82](#)
- [Configuring Switching Between the Working and Protect Circuits on page 82](#)
- [Revertive Mode Overview on page 84](#)
- [Configuring Revertive Mode on page 84](#)
- [Switching Mode Overview on page 86](#)
- [Configuring Switching Mode on page 87](#)
- [APS Timers Overview on page 87](#)
- [Configuring APS Timers on page 88](#)
- [Link PIC Redundancy Overview on page 89](#)
- [Configuring Link PIC Redundancy on page 89](#)
- [APS Load Sharing Between Circuit Pairs Overview on page 91](#)
- [Configuring APS Load Sharing on page 92](#)
- [Example: Configuring APS Load Sharing Between Circuit Pairs on page 92](#)
- [Configuring SONET Options for 10-Gigabit Ethernet Interfaces on page 95](#)
- [Configuring the Media MTU on SONET/SDH Interfaces on page 96](#)
- [Enabling Passive Monitoring on SONET/SDH Interfaces on page 97](#)
- [Configuring the Clock Source on SONET/SDH Interfaces on page 99](#)
- [Receive and Transmit Leaky Bucket Properties Overview on page 100](#)
- [Configuring Receive and Transmit Leaky Bucket Properties on page 101](#)
- [Damping Interface Transitions on page 102](#)
- [Configuring Interface Encapsulation on SONET/SDH Interfaces on page 102](#)
- [Example: Configuring SONET/SDH Interfaces on page 105](#)
- [Configuring Aggregated SONET/SDH Interfaces on page 106](#)
- [Configuring Multicast Statistics Collection on Aggregated SONET Interfaces on page 111](#)
- [Configuring 4-Port OC192 PIC to Operate in OC768-over-OC192 Mode on page 112](#)

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 for Routing Devices*.



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**

- [SONET/SDH Physical Interface Properties Overview on page 32](#)
- [Example: Configuring SONET/SDH Interfaces on page 105](#)

SONET/SDH Physical Interface Properties 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.

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 Routing Devices*.

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.

**Related
Documentation**

- [Automatic Protection Switching and Multiplex Section Protection Overview on page 64](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Configuring SONET Options for 10-Gigabit Ethernet Interfaces on page 95](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)

Configuring SONET/SDH Physical Interface Properties

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

This topic includes the following tasks:

1. [Configuring SONET/SDH Physical Interface Options on page 33](#)
2. [Configuring SONET/SDH Interface-Specific Options on page 33](#)
3. [Configuring MPLS Option for Passive Monitoring on page 35](#)
4. [Configuring Automatic Protection Switching Options on page 35](#)

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” on page 39](#).

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 40](#).

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” on page 41](#).

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 44](#).

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” on page 50](#).

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 51](#).

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” on page 53](#).

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” on page 56](#).

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” on page 57](#).

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 SONET/SDH RFC 2615 Support” on page 59](#).

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 62.

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 68](#).

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 88](#).

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 Annex B Option” on page 82](#).

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 92](#).

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 89](#).

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 82](#).

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 84](#).

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 87](#).

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 on page 64](#)
- [Configuring SONET Options for 10-Gigabit Ethernet Interfaces on page 95](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Framing Mode Overview

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.

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. However, per-port framing is currently not supported on SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP (MIC-3D-8OC3OC12-4OC48) in MX80 routers.



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

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

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Configuring SONET/SDH Framing Mode on page 39](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring SONET/SDH Framing Mode

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/cstm1* when configuring the framing option as *sonet*. Similarly, replace *so* with *coc12/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 SONET/SDH Physical Interface Properties on page 32](#)
- [Framing Mode Overview on page 38](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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.

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
```

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

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 JO 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 on page 32](#)
- [Configuring an Incrementing STM ID on page 41](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring an Incrementing STM ID

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
```

3. 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
```

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 on page 32](#)
- [Incrementing STM ID Overview on page 41](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)

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

.....

For more information about using the **non-concatenate** statement, see the *Junos OS Administration Library for Routing Devices*.

[Table 3 on page 43](#) shows the mode combinations for the next-generation SONET/SDH Type 1 PICs with SFP.

Table 3: Type 1 PIC Mode Combinations

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

[Table 4 on page 43](#) shows the mode combinations for the next-generation SONET/SDH Type 2 PICs with SFP.

Table 4: Type 2 PIC Mode Combinations

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

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Configuring SONET/SDH Interface Speed on page 44](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 non-concatenate statement, see the *Junos OS Administration Library for Routing Devices*.

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [SONET/SDH Interface Speed Overview on page 42](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

SONET/SDH Rate-Selectability Overview

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

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 5 on page 45 shows the port speed restrictions on the SONET/SDH OC3/STM1 (Multi-Rate) MICs.

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

Mode\MIC Name	8-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP	4-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP
Rate-selectable Mode	<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 6 on page 46](#) and [Table 7 on page 46](#) indicate the port configuration restrictions of the 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP.

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

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

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

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

All ports of the 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP can be configured as channelized OC3/channelized STM1. However, only two ports (ports 0 and 1) can be configured as channelized OC12/channelized STM4. [Table 8 on page 46](#) and [Table 9 on page 47](#) indicate the port configuration restrictions of the 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP.

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

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

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

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

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Configuring SONET/SDH Rate-Selectability on page 47](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [SONET/SDH Rate-Selectability Overview on page 45](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

SONET/SDH Header Byte Values Overview

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 48](#) 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

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

Overhead Bytes	STM4	STM16	STM64	OC12	OC48	OC192
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 on page 32](#)
- [Configuring SONET/SDH Header Byte Values on page 50](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring SONET/SDH Header Byte Values

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 on page 32](#)
- [SONET/SDH Header Byte Values Overview on page 48](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [loop-timing on page 145](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring SONET/SDH Loopback Capability

- [Configuring SONET/SDH Loopback Capability on page 53](#)
- [Displaying SONET/SDH Loopback Capability Configuration on page 54](#)
- [Determining Problem Is Internal or External with Loopback Capability on page 55](#)

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 *Interface Diagnostics*. For more information about using operational mode commands to test interfaces, see the *Junos OS Operational Mode Commands*.

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 Problem Is Internal or External with Loopback Capability

Problem 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 on page 32](#)
 - [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
 - [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [Configuring the SONET/SDH Path Trace Identifier on page 56](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring the SONET/SDH Path Trace Identifier

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 on page 32](#)
- [SONET/SDH Path Trace Identifier Overview on page 56](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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”](#) on page 101.

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 on page 32](#)
- [Configuring SONET/SDH HDLC Payload Scrambling on page 57](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring SONET/SDH HDLC Payload Scrambling

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
```

You 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 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 on page 32](#)
- [SONET/SDH HDLC Payload Scrambling Overview on page 57](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

SONET/SDH RFC 2615 Support Overview

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

[Table 11 on page 58](#) shows the older (RFC 1619) and newer (RFC 2615) values, together with the Juniper Networks default values.

Table 11: SONET/SDH Default Settings

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

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Configuring SONET/SDH RFC 2615 Support on page 59](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring SONET/SDH RFC 2615 Support

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

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 on page 32](#)
- [SONET/SDH RFC 2615 Support Overview on page 58](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

SONET/SDH Defect Triggers to Be Ignored 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 12 on page 59](#) lists the defects you can configure.

Table 12: 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	

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

Alarm	Description
ais-l	Alarm indication signal—line
rfi-l	Remote failure indication—line
ber-sd	Bit error rate defect-signal degrade
ber-sf	Bit error rate fault-signal fail
Path	
ais-p	Alarm indication signal—path
locd (ATM only)	Loss of cell delineation
lop-p	Loss of pointer—path
plm-p	Payload (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 on page 32](#)
- [Configuring SONET/SDH Defect Triggers on page 62](#)

- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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

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

- You can configure an up hold time, a down hold time, or both.
- Each interface on a SONET/SDH PIC controls certain aspects of the SONET/SDH overhead. For example, when you configure an OC48 PIC to be nonconcatenated, four interfaces are created. Each interface has its own path overhead. However, all four path interfaces share the same physical, section, and line overhead. This means the following:
 - Each interface's path trigger configuration is honored.
 - The physical, section, and line trigger configuration for the primary interface (**so-fpc/pic/slot:0**) is applied to all four interfaces.

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

- The hold timers on the SONET/SDH defects are applied in addition to any other hold timers you configure on the interface. For example, if an interface is up and you configure a SONET/SDH trigger down hold time of 100 milliseconds and an interface down hold time of 250 milliseconds, when the SONET/SDH defect occurs, the SONET/SDH trigger timer starts. After 100 milliseconds, assuming the defect is still present, the SONET/SDH defect starts the 250 millisecond down timer. After this has expired and again assuming the defect is still outstanding, the interface will be marked down. For more information about interface hold timers, see [“Damping Interface Transitions” on page 102](#).
- 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 on page 32](#)
- [Configuring SONET/SDH Defect Triggers on page 62](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring SONET/SDH Defect Triggers

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 on page 63](#)
- [Configuring SONET/SDH Defect Hold Times on page 63](#)
- [Displaying the Configuration for SONET/SDH Defects to Be Ignored on page 63](#)

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 for SONET/SDH Defects to Be Ignored

Purpose To display the configuration for SONET/SDH defects to be ignored.

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-1 ignore;  
lof ignore;  
los ignore;  
pll ignore;  
rfi-1 ignore;  
rfi-p ignore;
```

**Related
Documentation**

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [SONET/SDH Defect Hold Times Overview on page 61](#)
- [SONET/SDH Defect Triggers to Be Ignored Overview on page 59](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Automatic Protection Switching and Multiplex Section Protection Overview

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



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

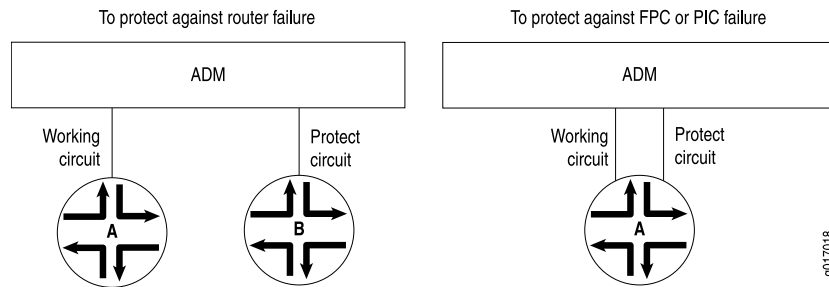
The Junos OS supports APS 1+1 switching, either revertive or nonrevertive mode, and bidirectional mode only (although you can configure interoperation with line-terminating equipment [LTE] provisioned for unidirectional mode). The Junos OS does not transmit identical data on the working and protect circuits,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

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

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

To configure APS or MSP, you configure a working and a protect circuit, as shown in [Figure 1 on page 65](#). 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 on page 32](#)
- [Configuring Basic Automatic Protect Switching on page 68](#)
- [Basic Automatic Protect Switching Overview on page 68](#)
- [Example: Configuring Basic APS Support on Routers on page 69](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 64](#)
- [Basic Automatic Protect Switching Overview on page 68](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Example: Configuring Basic APS Support on Routers on page 69](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 64](#)
- [Configuring Basic Automatic Protect Switching on page 68](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Example: Configuring Basic APS Support on Routers on page 69](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)

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 on page 64](#)
- [Basic Automatic Protect Switching Overview on page 68](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Example: Configuring Basic APS Support on Routers on page 69](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Example: Configuring Basic APS Support on Routers

- [Requirements for a Basic APS Support on page 70](#)
- [Basic APS Overview on page 70](#)
- [Configuring Basic APS Support on Routers on page 70](#)

Requirements for a Basic APS Support

This example uses the following hardware and software components:

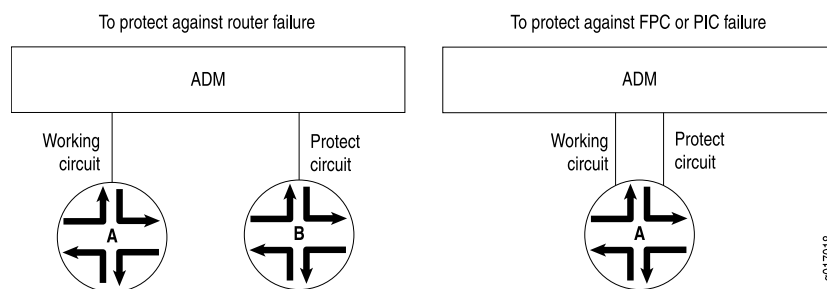
- Two MX Series, M Series, or T Series routers.
- Junos OS Release 7.4 or later

Basic APS Overview

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

To configure APS or MSP, you configure a working and a protect circuit, as shown in [Figure 2 on page 70](#). 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

To configure Router A to be the working router and Router B to be the protect router as shown in [Figure 2 on page 70](#).

- [On Router A \(the Working Router\) on page 71](#)
- [On Router B \(the Protect Circuit\) on page 71](#)
- [On a Single Platform, One Interface as the Working Circuit and Another Interface as the Protect Circuit on page 71](#)
- [Results on page 72](#)

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 “\$9\$B2612345”


```
[edit]
user@host# set authentication-key “$9$B2612345”
```

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 on page 64](#)
 - [Basic Automatic Protect Switching Overview on page 68](#)
 - [Configuring Basic Automatic Protect Switching on page 68](#)
 - [Configuring SONET/SDH Physical Interface Properties on page 32](#)
 - [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
 - [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 *Container Interfaces Overview* for more information.

Container interfaces support the following features:

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

To configure a container interface, you must first create the number of container devices that you require. You can create up to a maximum of 128 container interfaces per router using the **device-count** statement at the **[edit chassis container-devices]** hierarchy level.

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 on page 32](#)
 - [Configuring Container Interfaces for APS on SONET Links on page 74](#)
 - [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
 - [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring Container Interfaces for APS on SONET Links

- [Configuring Container Interfaces on SONET Links on page 74](#)
- [Displaying Container Interface Configuration on page 76](#)
- [Displaying the APS Container Interface Configuration on page 77](#)

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 interfaces cin 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 interfaces cin 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 interfaces cin 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 ci0:

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

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

```
[edit interfaces so-0/0/1]
```

```
user@host# set container-options container-list ci0 standby
allow-configuration-override
```

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-1/0/2 interface as primary and the so-1/0/3 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** operational mode command.

```
[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** operational mode command.

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

6. The following output is displayed.

```
so-1/0/2 {
  container-options {
    container-list ci0;
    primary;
  }
}
so-1/0/3 {
  container-options {
    container-list ci0;
    standby;
  }
}
ci0 {
  encapsulation cisco-hdlc;
  container-options {
    container-type aps {
      member-interface-type sonet {
        member-interface-speed mixed;
      }
    }
  }
}
```



```

unit 0 {
  family inet {
    address 192.168.11.1/24;
  }
}
}

```

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 on page 32](#)
 - [Container Interfaces for APS on SONET Links Overview on page 73](#)
 - [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
 - [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 *Container Interfaces Overview*.

Container ATM APS does not support interchassis APS.

MLPPP over ATM CI is not supported.

- Related Documentation**
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
 - [Displaying APS Using a Container Interface with ATM Encapsulation on page 78](#)
 - [Configuring APS Using a Container Interface with ATM Encapsulation on page 78](#)
 - [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
 - [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [APS Using a Container Interface with ATM Encapsulation Overview on page 77](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)
- [Displaying APS Using a Container Interface with ATM Encapsulation on page 78](#)

Displaying APS Using a Container Interface with ATM Encapsulation

- [Displaying APS Using a Container Interface with ATM Encapsulation on page 78](#)
- [Displaying the APS Container Interface Configuration on page 80](#)

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 1.0.0.1/30;
  }
}
unit 1 {
  vci 200;
  oam-period 3;
  family inet {
    address 2.0.0.1/30;
  }
}
```

```
}  
}
```

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 *Junos OS Operational Mode Commands*.

- Related Documentation**
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
 - [APS Using a Container Interface with ATM Encapsulation Overview on page 77](#)
 - [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
 - [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 82](#)
- [Configuring Annex B Option on page 82](#)
- [Configuring Switching Between the Working and Protect Circuits on page 82](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)

Configuring Annex B Option

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.

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

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Switching Between the Working and Protect Circuits Overview on page 80](#)
- [Configuring Switching Between the Working and Protect Circuits on page 82](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [Switching Between the Working and Protect Circuits Overview on page 80](#)
- [Configuring Annex B Option on page 82](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [Switching Between the Working and Protect Circuits Overview on page 80](#)

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 on page 32](#)
- [Configuring Revertive Mode on page 84](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [Revertive Mode Overview on page 84](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [Configuring Switching Mode on page 87](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [Switching Mode Overview on page 86](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [Configuring APS Timers on page 88](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [APS Timers Overview on page 87](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 on page 32](#)
- [Configuring Link PIC Redundancy on page 89](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Configuring Link PIC Redundancy

- [Configuring Link State Replication on page 89](#)
- [Displaying Link PIC Redundancy on page 90](#)

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 on page 32](#)
- [Link PIC Redundancy Overview on page 89](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

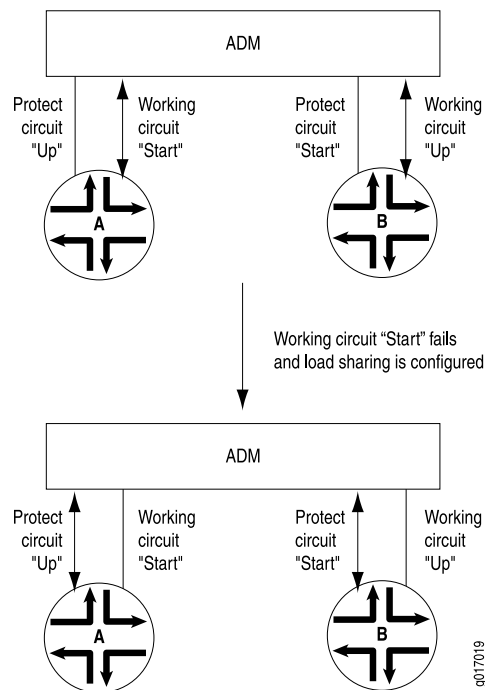
APS Load Sharing Between Circuit Pairs Overview

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 91 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 on page 32](#)
- [Configuring APS Load Sharing on page 92](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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

```
[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 on page 32](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

Example: Configuring APS Load Sharing Between Circuit Pairs

- [Requirements for APS Load Sharing Between Circuit Pairs on page 92](#)
- [APS Load Sharing Between Circuit Pairs Overview on page 92](#)
- [Configuring APS Load Sharing Between Circuit Pairs on page 93](#)

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

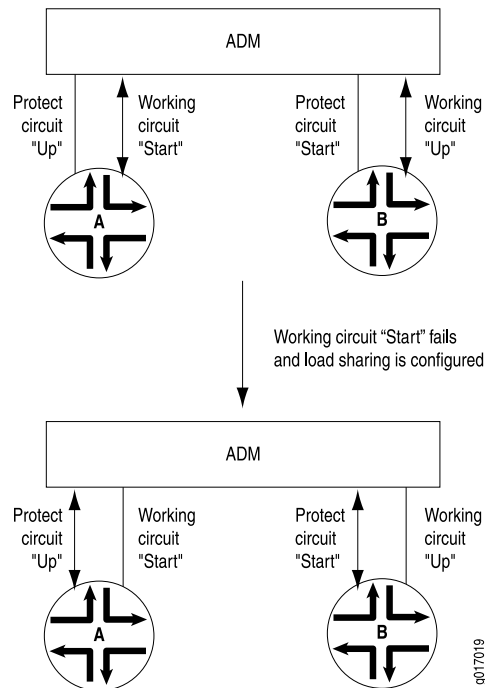
APS Load Sharing Between Circuit Pairs Overview

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 4 on page 93](#) 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 4: APS Load Sharing Between Circuit Pairs



Configuring APS Load Sharing Between Circuit Pairs

To configure APS load sharing to match the configuration shown in [Figure 4 on page 93](#), perform the following tasks:

- [Configuring APS Load Sharing on Router A on page 93](#)
- [Configuring APS Load Sharing on Router B on page 94](#)

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 on page 64](#)
- [Basic Automatic Protect Switching Overview on page 68](#)
- [Configuring Basic Automatic Protect Switching on page 68](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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 [“Removing MPLS Labels from Incoming Packets”](#) on page 98.

Related Documentation

- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [SONET/SDH Physical Interfaces Configuration Hierarchy on page 25](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)

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](#).

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 on page 102](#)
- [mtu on page 151](#)
- [Setting the Protocol MTU](#)

Enabling Passive Monitoring on SONET/SDH Interfaces

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

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

`passive-monitor-mode;`

You can include this statement at the following hierarchy levels:

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

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

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

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

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

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

For the monitoring services interface, you can configure multiservice physical interface properties. For more information, see *Configuring Multiservice Physical Interface Properties* and the *Junos OS Services Interfaces 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 by including the **pop-all-labels** statement at the **[edit interfaces *interface-name* sonet-options mpls]** hierarchy level.

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

By default, the **pop-all-labels** statement takes effect for incoming packets with one or two labels. You can specify the number of MPLS labels an incoming packet must have for the **pop-all-labels** statement to take effect by including the **required-depth** statement at the **[edit interfaces *interface-name* atm-options mpls pop-all-labels]** hierarchy level.

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

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

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

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

Configuring the Clock Source on SONET/SDH Interfaces

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

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

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

Related Documentation

- [Clock Sources on Channelized Interfaces](#)
- [clocking on page 124](#)

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 Policy Feature Guide for Routing Devices*.

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” on page 57](#).

Related Documentation

- [Configuring Receive and Transmit Leaky Bucket Properties on page 101](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)
- [receive-bucket on page 161](#)
- [transmit-bucket on page 171](#)

Configuring Receive and Transmit Leaky Bucket Properties

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 on page 100](#)
- [SONET/SDH Physical Interface Properties Overview on page 32](#)
- [receive-bucket on page 161](#)
- [transmit-bucket on page 171](#)

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

To damp interface transitions:

1. In the 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 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 1-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 Overview on page 61](#)
- [Configuring SONET/SDH Defect Triggers on page 62](#)
- *hold-time*

Configuring Interface Encapsulation on SONET/SDH Interfaces

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

an encapsulation on a logical interface, which is the encapsulation used within certain packet types.

Configuring the Encapsulation on a Physical SONET/SDH Interface

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

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

- Extended TCC version (**extended-frame-relay-ether-type-tcc**)—This encapsulation allows you to dedicate Cisco-compatible Frame Relay TCC for DLCIs 1 through 1022. This encapsulation is used for circuits with different media on either side of the connection. All ether type TCC encapsulation is supported on the same PICs as non-ether type Frame Relay TCC encapsulation.



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

To configure the encapsulation on a physical interface, include the **encapsulation** statement at the **[edit interfaces *interface-name*]** hierarchy level, where you can set the encapsulation to `cisco-hdlc`, `cisco-hdlc-ccc`, `cisco-hdlc-tcc`, `frame-relay`, `frame-relay-ccc`, `frame-relay-tcc`, `frame-relay-tcc`, `ppp`, `ppp-ccc`, or `ppp-tcc`.

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

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

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

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

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

```
[edit interfaces]  
so-7/0/0 {  
  encapsulation ppp;  
  unit 0 {  
    point-to-point;  
    family inet {  
      address 192.168.1.113/32 {  
        destination 192.168.1.114;  
      }  
    }  
    family iso;  
    family mpls;  
  }  
}
```

Configuring the Encapsulation on a Logical SONET/SDH Interface

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

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

You can include this statement at the following hierarchy levels:

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

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

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

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

Example: Configuring SONET/SDH Interfaces

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

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

Related Documentation

- [Configuring SONET/SDH Defect Triggers on page 62](#)
- [Configuring SONET/SDH Framing Mode on page 39](#)
- [Configuring SONET/SDH Physical Interface Properties on page 32](#)
- [Configuring SONET/SDH Interface Speed on page 44](#)

Configuring 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 for Routing Devices*.

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

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

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

Starting with Junos OS Release 13.2, a maximum of 64 aggregated interfaces are supported for link aggregation of SONET/SDH interfaces. In releases before Junos OS Release 13.2, a maximum of 16 aggregated interfaces are 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*.



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

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

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

The following example shows an aggregated SONET/SDH configuration.

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

```

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

```

You also need to specify the constituent physical interfaces by including the **aggregate** statement at the **[edit interfaces *interface-name* sonet-options]** hierarchy level; for more information, see [“Configuring SONET/SDH Link Aggregation” on page 107](#). You can optionally specify other physical properties that apply specifically to the aggregated SONET/SDH interfaces; for details, see [“SONET/SDH Physical Interface Properties Overview” on page 32](#). For a sample configuration, see [“Example: Configuring Aggregated SONET/SDH Interfaces” on page 110](#).

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

```

[edit]
user@host# delete interfaces asx

```

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

You can configure the following aggregated SONET/SDH properties:

- [Configuring SONET/SDH Link Aggregation on page 107](#)
- [Configuring Aggregated SONET/SDH Link Speed on page 108](#)
- [Configuring Aggregated SONET/SDH Minimum Links on page 108](#)
- [Configuring Filters or Sampling on Aggregated SONET/SDH Links on page 109](#)
- [Example: Configuring Aggregated SONET/SDH Interfaces on page 110](#)

Configuring SONET/SDH Link Aggregation

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

```

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

```

x is the interface instance number and can be from 0 through 63, for a total of 64 aggregated interfaces. You should not mix SONET and SDH mode on the same aggregated interface. You must also include a statement configuring **asx** at the **[edit interfaces]** hierarchy level. For a sample configuration, see [“Example: Configuring Aggregated SONET/SDH Interfaces” on page 110](#).

Configuring Aggregated SONET/SDH Link Speed

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



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

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

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

The link speed can be one of the following values:

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

Configuring Aggregated SONET/SDH Minimum Links

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

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

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

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

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

Configuring Filters or Sampling on Aggregated SONET/SDH Links

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

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

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

You can include this statement at the following hierarchy levels:

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

You must also configure separate statements that define the properties of the filter. For more information, see the *Routing Policy Feature Guide for Routing Devices* and “[Examples: Configuring Filters or Sampling on Aggregated SONET/SDH Links](#)” on page 109.

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

Configure filtering on aggregated SONET/SDH interfaces:

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

Defining the Filter

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

**Configuring Sampling
on an Aggregated
SONET/SDH Interface**

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

**Defining the Sampling
Filter and the
Forwarding Action**

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

[edit forwarding-options]
sampling {
  input {
    family inet {
      rate 10000;
      run-length 1;
    }
  }
}
```

Example: Configuring Aggregated SONET/SDH Interfaces

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

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

[edit chassis]
aggregated-devices {
  sonet {
    device-count 15;
  }
}

[edit interfaces]
```

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

Configuring Multicast Statistics Collection on Aggregated SONET Interfaces

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

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

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

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

To configure multicast statistics:

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

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

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

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

Related Documentation

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

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 • *aggregate-ports*
Documentation

PART 3

SONET/SDH Interface Configuration Statements

- [Summary of SONET/SDH Interfaces Configuration Statements on page 117](#)

CHAPTER 3

Summary of SONET/SDH Interfaces Configuration Statements

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

advertise-interval

Syntax	<code>advertise-interval <i>milliseconds</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<i>milliseconds</i> —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	<ul style="list-style-type: none">• Configuring APS Timers on page 88

aggregate (SONET/SDH)

Syntax	aggregate <i>asx</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring Aggregated SONET/SDH Interfaces on page 106

aggregated-sonet-options

Syntax	aggregated-sonet-options { link-speed <i>speed</i> ; minimum-links <i>number</i> ; }
Hierarchy Level	[edit interfaces <i>asx</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure aggregated SONET/SDH-specific interface properties. The statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Aggregated SONET/SDH Interfaces on page 106

annex

Syntax	<code>annex (annex-a annex-b);</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> shdsl-options], [edit interfaces <i>interface-name</i> sonet-options aps], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> shdsl-options]
Release Information	Statement introduced in Junos OS Release 7.4.
Description	For J Series Services Routers only, configure the type of SHDSL annex. For M320 and M120 routers only, for Multiplex Section Protection (MSP) switching on SDH interfaces, set annex-b . You must also configure the working protection circuit under the [edit interfaces <i>so-fpc/pic/port</i> sonet-options aps] hierarchy level.
Default	annex-b
Options	annex-a —Use for North American SHDSL network implementations. annex-b —Use for European SHDSL network implementations.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>ATM-over-SHDSL Overview</i>

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 statements are explained separately.

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

Related Documentation • [Automatic Protection Switching and Multiplex Section Protection Overview on page 64](#)

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 Access Routers.

Description Configure ATM-specific physical interface properties.

The statements are explained separately.



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

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

authentication-key

Syntax authentication-key *key*;

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

Release Information Statement introduced before Junos OS Release 7.4.

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

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

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

Related Documentation

- [Configuring Basic Automatic Protect Switching on page 68](#)
- For information about the **authentication-key** statement at the [edit interfaces *interface-name* unit *unit-number* family inet address *address* (vrrp-group | vrrp-inet6-group) *group-number*] or [edit logical-systems *logical-system-name* interfaces *interface-name* unit *unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-number*] hierarchy level, see the *Junos OS High Availability Library for Routing Devices*.

bytes

Syntax	<pre>bytes { c2 <i>value</i>; e1-quiet <i>value</i>; f1 <i>value</i>; f2 <i>value</i>; s1 <i>value</i>; z3 <i>value</i>; z4 <i>value</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Set values in some SONET/SDH header bytes.
Options	<p>c2 <i>value</i>—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.</p> <p>Range: 0 through 255</p> <p>Default: 0xCF</p> <p>e1-quiet <i>value</i>—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.</p> <p>Range: 0 through 255</p> <p>Default: 0x7F</p> <p>f1 <i>value</i>, f2 <i>value</i>, z3 <i>value</i>, z4 <i>value</i>—SONET/SDH overhead bytes.</p> <p>Range: 0 through 255</p> <p>Default: 0x00</p> <p>s1 <i>value</i>—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.</p> <p>Range: 0 through 255</p> <p>Default: 0xCC</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring SONET/SDH Header Byte Values on page 50 • <i>no-concatenate</i>

clocking

Syntax	clocking (external [interface <i>interface-name</i>] internal);
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>interface option added in Junos OS Release 8.2.</p> <p>Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers.</p>
Description	For interfaces that can use various clock sources, configure the source of the transmit clock on each interface.
Options	<p>external—The clock source is provided by the data communication equipment (DCE).</p> <p>interface <i>interface-name</i>—For interfaces operating on T1/E1 PIMs for J Series Services Routers only, configure clocking for the drop-and insert feature. When configuring this feature, both ports must use the same clock source: either the router's internal clock or an external clock on one of the interfaces. If an external clock source is required, one interface must specify clocking external and the other must specify the same clock.</p> <p>internal—Use the internal stratum 3 clock as the reference clock.</p> <p>Default: internal</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Clock Source</i>• Configuring the Clock Source on SONET/SDH Interfaces on page 99• <i>Clock Sources on Channelized Interfaces</i>• <i>Configuring a Channelized T1/E1 Interface to Drop and Insert Time Slots</i>• loop-timing on page 145

container-devices

Syntax	container-devices { device-count <i>number</i> ; }
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	<ul style="list-style-type: none"> • Displaying APS Using a Container Interface with ATM Encapsulation on page 78 • Configuring Container Interfaces for APS on SONET Links on page 74

container-list

Syntax	container-list [<i>container-interface-names</i>];
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	<ul style="list-style-type: none"> • Displaying APS Using a Container Interface with ATM Encapsulation on page 78 • Configuring Container Interfaces for APS on SONET Links on page 74 • container-options on page 126

container-options

Syntax	<pre>container-options { container-list [<i>container-interface-names</i>]; container-type aps; member-interface-type sonet { member-interface-speed [<i>speed</i>]; } }</pre>
Hierarchy Level	[edit interfaces]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Specify the container interface options.
Options	<p>interface-name—Name of the SONET or the container interface.</p> <p>aps—Specify the member link interface type of the container as APS.</p> <p>sonet—Protocol type of the container interface.</p> <p>speed—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Displaying APS Using a Container Interface with ATM Encapsulation on page 78• Configuring Container Interfaces for APS on SONET Links on page 74

container-type

Syntax	<pre>container-type aps;</pre>
Hierarchy Level	[edit interfaces container-options]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Specify the container-options interface type.
Options	<p>aps—Configure the interface type to be Automatic Protection Switching (APS).</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Displaying APS Using a Container Interface with ATM Encapsulation on page 78• Configuring Container Interfaces for APS on SONET Links on page 74

encapsulation

See the following sections:

- [encapsulation \(Container Interface\) on page 127](#)
- [encapsulation \(Logical Interface\) on page 128](#)

encapsulation (Container Interface)

Syntax	<code>encapsulation (cisco-hdlc ppp);</code>
Hierarchy Level	<code>[edit interfaces cin]</code>
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	<ul style="list-style-type: none">• Displaying APS Using a Container Interface with ATM Encapsulation on page 78• Configuring Container Interfaces for APS on SONET Links on page 74

encapsulation (Logical Interface)

Syntax	<code>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);</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</code> <code>[edit interfaces <i>rlsq number</i> unit <i>logical-unit-number</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers (vlan-ccc and vlan-tcc options only). Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers. Only the atm-ccc-cell-relay and atm-ccc-vc-mux options are supported on ACX Series routers.
Description	Configure a logical link-layer encapsulation type.
Options	<p>atm-ccc-cell-relay—Use ATM cell-relay encapsulation.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the inet family only.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.</p>

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 device over a time-division multiplexing (TDM) link. This encapsulation type enables the PE device 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. J Series routers do not support frame-relay-ppp encapsulation.

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

ppp-over-ether-over-atm-llc—(J Series routers and 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.

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

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 MPLS LSP Tunnel Cross-Connects Using CCC*
- *Circuit and Translational Cross-Connects Overview*
- *Identifying the Access Concentrator*
- *Configuring ATM Interface Encapsulation*
- *Configuring VLAN Encapsulation*
- *Configuring Extended VLAN Encapsulation*
- *Configuring ISDN Logical Interface Properties*
- *Configuring ATM-to-Ethernet Interworking*
- *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*
- *Junos OS Services Interfaces Library for Routing Devices*
- *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 ...
        }
        bridge-domain-type (bvlan | svlan);
        bundle interface-name;
        core-facing;
        demux-destination {
            destination-prefix;
        }
        demux-source {
            source-prefix;
        }
        duplicate-protection;
        dynamic-profile profile-name;
        filter {
            group filter-group-number;
            input filter-name;
            input-list [ filter-names ];
            output filter-name;
            output-list [ filter-names ];
        }
        interface-mode (access | trunk);
        ipsec-sa sa-name;
        isid-list all-service-groups;
        keep-address-and-control;
        mac-validate (loose | strict);
        max-sessions number;
        max-sessions-vsa-ignore;
        mtu bytes;
        multicast-only;
        negotiate-address;
        no-redirects;
        policer {
            arp policer-template-name;
            input policer-template-name;
            output policer-template-name;
        }
        primary;
        protocols [inet iso mpls];
        proxy inet-address address;
        receive-options-packets;
        receive-ttl-exceeded;
        remote (inet-address address | mac-address address);

```



```

rpf-check {
    fail-filter filter-name
    mode loose;
}
sampling {
    input;
    output;
}
service {
    input {
        post-service-filter filter-name;
        service-set service-set-name <service-filter filter-name>;
    }
    output {
        service-set service-set-name <service-filter filter-name>;
    }
}
service-name-table table-name
short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
    maximum-seconds>;
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    master-only;
    multipoint-destination address dlci dlci-identifier;
    multipoint-destination address {
        epd-threshold cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period (disable | seconds);
        shaping {
            (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
                sustained rate);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
}
preferred;
primary;
vrrp-group 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 <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
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.



NOTE: Not all subordinate stanzas 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.

- **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
- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite
- **iso**—International Organization for Standardization Open Systems Interconnection (ISO OSI) protocol suite
- **mlfr-end-to-end**—Multilink Frame Relay FRF.15
- **mlfr-uni-nni**—Multilink Frame Relay FRF.16
- **multilink-ppp**—Multilink Point-to-Point Protocol
- **mpls**—Multiprotocol Label Switching (MPLS)
- **pppoe**—Point-to-Point Protocol over Ethernet
- **tcc**—Translational cross-connect protocol suite
- **tnp**—Trivial Network Protocol
- **vpls**—(M Series and T Series routers only) Virtual private LAN service


The remaining statements are explained separately.

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


Related Documentation

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

fast-aps-switch

Syntax	fast-aps-switch;
Hierarchy Level	[edit interfaces <i>interface-name</i> 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 and EX Series switches) Reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits.
	<div> NOTE:<ul style="list-style-type: none">• 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.</div>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Reducing APS Switchover Time in Layer 2 Circuits</i>

fcs

Syntax	fcs (16 32);
Hierarchy Level	[edit interfaces e1- <i>fpc/pic/port</i>], [edit interfaces t1- <i>fpc/pic/port</i>], [edit interfaces <i>interface-name</i> ds0-options], [edit interfaces <i>interface-name</i> e1-options], [edit interfaces <i>interface-name</i> e3-options], [edit interfaces <i>interface-name</i> sonet-options], [edit interfaces <i>interface-name</i> t1-options], [edit interfaces <i>interface-name</i> 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 Access Routers.
Description	<p>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.</p> <p>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.</p>
	<div>  <p>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-<i>fpc/pic/port</i>] or [edit interfaces t1-<i>fpc/pic/port</i>] hierarchy level as appropriate.</p> </div>
Options	<p>16—Use a 16-bit frame checksum on the interface.</p> <p>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.</p> <p>Default: 16</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the E1 Frame Checksum</i> • <i>Configuring the E3 Frame Checksum</i> • <i>Configuring the SONET/SDH Frame Checksum on page 51</i> • <i>Configuring the T1 Frame Checksum</i> • <i>Configuring the T3 Frame Checksum</i>

filter

Syntax	<pre>filter { group <i>filter-group-number</i>; input <i>filter-name</i>; input-list [<i>filter-names</i>]; output <i>filter-name</i>; output-list [<i>filter-names</i>]; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Apply a filter to an interface. You can also use filters for encrypted traffic. When you configure filters, you can configure them under the family ethernet-switching , inet , inet6 , mpls , or vpls only.
Options	<p>group <i>filter-group-number</i>—Define an interface to be part of a filter group. Range: 1 through 255</p> <p>input <i>filter-name</i>—Name of one filter to evaluate when packets are received on the interface.</p> <p>output <i>filter-name</i>—Name of one filter to evaluate when packets are transmitted on the interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Applying a Filter to an Interface</i>• <i>Junos OS Services Interfaces Library for Routing Devices</i>• <i>Routing Policy Feature Guide for Routing Devices</i>• <i>Junos OS Administration Library for Routing Devices</i>• <i>Configuring Gigabit Ethernet Interfaces (CLI Procedure)</i>• <i>Configuring Gigabit Ethernet Interfaces (CLI Procedure)</i>• <i>Configuring Firewall Filters (CLI Procedure)</i>• <i>Configuring Firewall Filters and Policers for VPLS</i>• <i>family</i>• <i>family</i>

force

Syntax	<code>force (protect working);</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring Switching Between the Working and Protect Circuits on page 82• request on page 163

framing (SONET and SDH Interfaces)

Syntax	framing (sdh sonet);
Hierarchy Level	[edit interfaces <i>so-fpc/pic/port</i>]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	<p>This functionality allows you to mix SONET and SDH modes on interfaces on the same PIC.</p> <ul style="list-style-type: none">• 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.
Default	Default framing mode is SONET .
Options	<p>sdh—SDH framing.</p> <p>sonet—SONET framing.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring SONET/SDH Framing Mode on page 39

hold-time

See the following sections:

- [hold-time \(APS\) on page 141](#)
- [hold-time \(SONET/SDH Defect Triggers\) on page 142](#)



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

hold-time (APS)

Syntax	hold-time <i>milliseconds</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<i>milliseconds</i> —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	<ul style="list-style-type: none"> • Configuring APS Timers on page 88 • advertise-interval on page 117

hold-time (SONET/SDH Defect Triggers)

Syntax	hold-time up <i>milliseconds</i> down <i>milliseconds</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring SONET/SDH Defect Triggers on page 62• <i>hold-time (Physical Interface)</i>

ignore

Syntax	ignore;
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring SONET/SDH Defect Triggers on page 62• <i>hold-time (Physical Interface)</i>


link-speed (Aggregated SONET/SDH)

Syntax	link-speed (<i>speed</i> 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	<p>speed—Aggregated SONET/SDH links can have one of the following speed values.</p> <ul style="list-style-type: none">• 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. <p>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.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Aggregated Ethernet Link Speed</i>• Configuring Aggregated SONET/SDH Link Speed on page 108

lockout

Syntax	lockout;
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring Switching Between the Working and Protect Circuits on page 82

loop-timing

Syntax	(loop-timing no-loop-timing);
Hierarchy Level	[edit interfaces ct3- <i>fpc/pic/port</i> t3-options], [edit interfaces e1- <i>fpc/pic/port:0</i> sonet-options], [edit interfaces stm1- <i>fpc/pic/port</i> 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.
	<div>  <p>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.</p> </div>
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	<ul style="list-style-type: none"> • Configuring Channelized IQ and IQE SONET/SDH Loop Timing on page 52 • Configuring the Channelized T3 Loop Timing • clocking on page 124

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

Syntax	<code>loopback (local payload remote);</code>
Hierarchy Level	<code>[edit interfaces ce1-<i>fpc/pic/port</i>],</code> <code>[edit interfaces ct1-<i>fpc/pic/port</i>],</code> <code>[edit interfaces t1-<i>fpc/pic/port</i>],</code> <code>[edit interfaces <i>interface-name</i> ds0-options],</code> <code>[edit interfaces <i>interface-name</i> dsl-options],</code> <code>[edit interfaces <i>interface-name</i> e1-options],</code> <code>[edit interfaces <i>interface-name</i> e3-options],</code> <code>[edit interfaces <i>interface-name</i> shdsl-options],</code> <code>[edit interfaces <i>interface-name</i> sonet-options],</code> <code>[edit interfaces <i>interface-name</i> t1-options],</code> <code>[edit interfaces <i>interface-name</i> t3-options]</code>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers.</p>
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 NxDSO 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. NxDSO 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	<ul style="list-style-type: none"> • <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 on page 53 • <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 <i>speed</i> ;
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	<ul style="list-style-type: none"> • Displaying APS Using a Container Interface with ATM Encapsulation on page 78 • Configuring Container Interfaces for APS on SONET Links on page 74 • container-options on page 126

member-interface-type

Syntax	<code>member-interface-type sonet { member-interface-speed [<i>speed</i>]; }</code>
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	<ul style="list-style-type: none">• Displaying APS Using a Container Interface with ATM Encapsulation on page 78• Configuring Container Interfaces for APS on SONET Links on page 74• container-options on page 126

minimum-links

Syntax	<code>minimum-links <i>number</i>;</code>
Hierarchy Level	<p>[edit interfaces aex aggregated-ether-options], [edit interfaces aex aggregated-sonet-options], [edit interfaces <i>interface-name</i> mlfr-uni-nni-bundle-options], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit interfaces interface-range <i>range</i> aggregated-ether-options], [edit interfaces interface-range <i>range</i> aggregated-sonet-options], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
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	<p><i>number</i>—Number of links.</p> <p>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.</p> <p>Default: 1</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Aggregated Ethernet Minimum Links</i> • Configuring Aggregated SONET/SDH Minimum Links on page 108 • <i>Configuring Aggregated Ethernet Links (CLI Procedure)</i> • <i>Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch</i> • <i>Junos OS Services Interfaces Library for Routing Devices</i>

mpls (Interfaces)

Syntax	<pre>mpls { pop-all-labels { required-depth <i>number</i>; } }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> atm-options], [edit interfaces <i>interface-name</i> sonet-options], [edit interfaces <i>interface-name</i> fastether-options], [edit interfaces <i>interface-name</i> gige-ether-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>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.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Removing MPLS Labels from Incoming Packets</i>• Removing MPLS Labels from Incoming Packets on page 98• <i>Junos OS Services Interfaces Library for Routing Devices</i>

mtu

Syntax	<code>mtu bytes;</code>
Hierarchy Level	<p>[edit interfaces <i>interface-name</i>],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>],</p> <p>[edit interfaces interface-range <i>name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit local-switching interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls],</p> <p>[edit protocols l2circuit local-switching interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i>],</p> <p>[edit protocols l2circuit neighbor <i>address</i> interface <i>interface-name</i> backup-neighbor <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols l2vpn interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols vpls]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for Layer 2 VPNs and VPLS introduced in Junos OS Release 10.4.</p> <p>Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.</p> <p>Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.</p> <p>Support at the [set interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>ccc</i>] hierarchy level introduced in Junos OS Release 12.3R3 for MX Series routers.</p>
Description	<p>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.</p> <p>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 and also on the IRB interface or RVI itself (the irb or vlan interface, respectively).</p>



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: 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.



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

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

Options *bytes*—MTU size.

Range: 256 through 9192 bytes, 256 through 9500 bytes (Junos OS 12.1X48R2 for PTX Series routers)

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 Gigabit Ethernet Interfaces (CLI Procedure)*
- *Configuring Gigabit Ethernet Interfaces (CLI Procedure)*
- *Configuring Routed VLAN Interfaces (CLI Procedure)*
- *Configuring Integrated Routing and Bridging Interfaces (CLI Procedure)*
- *Configuring the Media MTU*
- *Configuring the MTU for Layer 2 Interfaces*
- *Setting the Protocol MTU*

neighbor (Automatic Protection Switching for SONET/SDH)

Syntax	<code>neighbor <i>address</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options aps]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>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.</p> <p>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.</p>
Options	<i>address</i> —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	<ul style="list-style-type: none">• Configuring Basic Automatic Protect Switching on page 68

overflow

See the following sections:

- [overflow \(Receive Bucket\) on page 154](#)
- [overflow \(Transmit Bucket\) on page 154](#)

overflow (Receive Bucket)

Syntax	overflow (discard tag);
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring Receive and Transmit Leaky Bucket Properties on page 101

overflow (Transmit Bucket)

Syntax	overflow discard;
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring Receive and Transmit Leaky Bucket Properties on page 101

paired-group

Syntax	<code>paired-group <i>group-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options aps]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure load sharing between two working protect circuit pairs.
Options	<i>group-name</i> —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	<ul style="list-style-type: none">• Configuring APS Load Sharing on page 92• working-circuit on page 173


passive-monitor-mode

Syntax	<code>passive-monitor-mode;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>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.</p> <p>This statement is supported on ATM, Ethernet, and SONET/SDH interfaces. For more information, see <i>ATM Interfaces Feature Guide for Routing Devices</i>.</p> <p>For ATM and Ethernet interfaces, you can include this statement on the physical interface only.</p> <p>For SONET/SDH interfaces, you can include this statement on the logical interface only.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Enabling Passive Monitoring on ATM Interfaces</i>• <i>Passive Monitoring on Ethernet Interfaces Overview</i>• Enabling Passive Monitoring on SONET/SDH Interfaces on page 97• <i>multiservice-options</i>• <i>Junos OS Services Interfaces Library for Routing Devices</i>

path-trace

Syntax	<code>path-trace <i>trace-string</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>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.</p> <p>On SONET/SDH OC48 interfaces that are configured for channelized (multiplexed) mode (by including the no-concatenate statement at the [edit chassis fpc <i>slot-number</i> pic <i>pic-number</i>] 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.</p> <p>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.</p>
Options	<p>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.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the SONET/SDH Path Trace Identifier on page 56 • sonet-options on page 166

payload-scrambler

Syntax	(payload-scrambler no-payload-scrambler);
Hierarchy Level	[edit interfaces <i>interface-name</i> e3-options], [edit interfaces <i>interface-name</i> sonet-options], [edit interfaces <i>interface-name</i> t3-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>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.</p> <p>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.</p> <p>Disable payload scrambling on an E3 interface if Digital Link compatibility mode is used.</p> <p>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.</p>
	<div> NOTE: The payload-scrambler statement at the [edit interfaces <i>interface-name</i> e3-options] hierarchy level is not valid for IQE PICs.</div>
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	<ul style="list-style-type: none">• <i>Configuring E3 and T3 Parameters on ATM Interfaces</i>• <i>Configuring E3 HDLC Payload Scrambling</i>• Configuring SONET/SDH HDLC Payload Scrambling on page 57• <i>Configuring T3 HDLC Payload Scrambling</i>• <i>Examples: Configuring T3 Interfaces</i>• <i>compatibility-mode</i>

pop-all-labels

Syntax	pop-all-labels { required-depth <i>number</i> ; }
Hierarchy Level	[edit interfaces <i>interface-name</i> atm-options mpls], [edit interfaces <i>interface-name</i> sonet-options mpls], [edit interfaces <i>interface-name</i> fastether-options mpls], [edit interfaces <i>interface-name</i> gether-options mpls]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Description	<p>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.</p> <p>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.</p> <p>The remaining statement is explained separately.</p>
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	<ul style="list-style-type: none"> • <i>Removing MPLS Labels from Incoming Packets</i> • Removing MPLS Labels from Incoming Packets on page 98 • <i>Junos OS Services Interfaces Library for Routing Devices</i>

preserve-interface

Syntax	<code>preserve-interface;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options aps]
Release Information	Statement introduced in Junos OS Release 7.6.
Description	<p>Provide link PIC replication, providing MLPPP link redundancy at the port level. This feature is supported with SONET APS and the following link PICs:</p> <ul style="list-style-type: none">• Channelized OC3 IQ PIC• Channelized OC12 IQ PIC• Channelized STM1 IQ PIC <p>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.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Link PIC Redundancy on page 89• <i>Junos OS Services Interfaces Library for Routing Devices</i>

protect-circuit

Syntax	<code>protect-circuit <i>group-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<i>group-name</i> —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	<ul style="list-style-type: none">• Configuring Basic Automatic Protect Switching on page 68• working-circuit on page 173

rate

Syntax	<code>rate percentage;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> <code>receive-bucket</code>], [edit interfaces <i>interface-name</i> <code>transmit-bucket</code>]
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	<ul style="list-style-type: none"> • Configuring Receive and Transmit Leaky Bucket Properties on page 101

receive-bucket

Syntax	<pre>receive-bucket { overflow (discard tag); rate percentage; threshold bytes; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Set parameters for the receive leaky bucket, which specifies what percentage of the interface's total capacity can be used to receive packets.</p> <p>For each DS3 channel on a channelized OC12 interface, you can configure a unique receive bucket.</p> <p>The statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Receive and Transmit Leaky Bucket Properties on page 101 • transmit-bucket on page 171

receive-options-packets

Syntax	receive-options-packets;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> 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	<ul style="list-style-type: none">• Enabling Passive Monitoring on ATM Interfaces• Enabling Passive Monitoring on SONET/SDH Interfaces on page 97

receive-ttl-exceeded

Syntax	receive-ttl-exceeded;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> 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	<ul style="list-style-type: none">• Enabling Passive Monitoring on ATM Interfaces• Enabling Passive Monitoring on SONET/SDH Interfaces on page 97

request

Syntax	<code>request (protect working);</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring Switching Between the Working and Protect Circuits on page 82• force on page 139

required-depth

Syntax	<code>required-depth <i>number</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> atm-options mpls pop-all-labels], [edit interfaces <i>interface-name</i> sonet-options mpls pop-all-labels], [edit interfaces <i>interface-name</i> fastether-options mpls pop-all-labels], [edit interfaces <i>interface-name</i> gigether-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 Access Routers.
Description	<p>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.</p> <p>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.</p>
Options	<p>number—Number of MPLS labels on incoming IP packets.</p> <p>Range: 1 or 2 labels</p> <p>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.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Removing MPLS Labels from Incoming Packets</i>• Removing MPLS Labels from Incoming Packets on page 98• <i>Junos OS Services Interfaces Library for Routing Devices</i>

revert-time (Interfaces)

Syntax	<code>revert-time seconds;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<p>seconds—Amount of time to wait after the working circuit has again become functional before making the working circuit active again.</p> <p>Range: 1 through 65,535 seconds</p> <p>Default: None (APS operates in nonrevertive mode)</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Revertive Mode on page 84

rfc-2615

Syntax	<code>rfc-2615;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Include this statement to enable features described in RFC 2615, <i>PPP over SONET/SDH</i> .
Default	Settings required by RFC 1619, <i>PPP over SONET/SDH</i> .
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring SONET/SDH RFC 2615 Support on page 59

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 statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring SONET/SDH Parameters on ATM Interfaces</i> • <i>Channelized OC12/STM4 IQ and IQE Interfaces Overview</i> • <i>Channelized STM1 Interfaces Overview</i> • SONET/SDH Physical Interface Properties Overview on page 32 • <i>no-concatenate</i>

speed (SONET/SDH)

Syntax	<code>speed (oc3 oc12 oc48);</code>
Hierarchy Level	[edit interfaces <i>so-fpc/pic/port</i>], [edit interfaces <i>so-fpc/pic/port:channel</i>]
Release Information	Statement introduced in Junos OS Release 8.3.
Description	Configure the interface speed. This statement applies to SONET/SDH interfaces on next-generation SONET/SDH Type 1 and Type 2 PICs with SFP. Available speeds depend on whether the PIC is in concatenated mode or nonconcatenated mode. Include the channel in the interface name when configuring nonconcatenated interfaces.
Options	<p>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.</p> <p>You can configure port 0 of a 4-port OC12 PIC to have a speed of oc12.</p> <p>oc3 oc12—Speed when the PIC is in nonconcatenated mode.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring SONET/SDH Interface Speed on page 44

switching-mode

Syntax	switching-mode (bidirectional unidirectional);
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<ul style="list-style-type: none">• Configuring Switching Mode on page 87

t3-options

Syntax t3-options {
 atm-encapsulation (direct | plcp);
 bert-algorithm *algorithm*;
 bert-error-rate *rate*;
 bert-period *seconds*;
 (cbit-parity | no-cbit-parity);
 compatibility-mode (digital-link | kentrox | larscom) <subrate *value*>;
 fcs (16 | 32);
 (feac-loop-respond | no-feac-loop-respond);
 idle-cycle-flag *value*;
 (long-buildout | no-long-buildout);
 (**loop-timing** | no-**loop-timing**);
 loopback (local | payload | remote);
 start-end-flag *value*;
 }

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

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

On T3 interfaces, the default encapsulation is PPP.

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

The statements are explained separately.

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

Related Documentation • *T3 Interfaces Overview*

threshold

Syntax	<code>threshold bytes;</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i>]</code>
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	<p>bytes—Maximum size, in bytes, for traffic bursts. For ease of entry, you can enter <i>number</i> 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.</p> <p>Range: 0 through 65,535 bytes</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Receive and Transmit Leaky Bucket Properties on page 101

transmit-bucket

Syntax	<pre>transmit-bucket { overflow discard; rate percentage; threshold bytes; }</pre>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Set parameters for the transmit leaky bucket, which specifies what percentage of the interface's total capacity can be used to transmit packets.</p> <p>For each DS3 channel in a channelized OC12 interface, you can configure a unique transmit bucket.</p> <p>The statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Receive and Transmit Leaky Bucket Properties on page 101 • receive-bucket on page 161

trigger

Syntax	<pre>trigger { defect ignore; defect hold-time up <i>milliseconds</i> down <i>milliseconds</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> 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	<p>defect—Defect to ignore or hold. It can be one of the following:</p> <ul style="list-style-type: none">• 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• rfi-l—Line remote failure indication• rfi-p—Path remote failure indication• uneq-p—Path unequipped <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring SONET/SDH Defect Triggers on page 62

vtmapping

Syntax	vtmapping (itu-t klm);
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options]; [edit chassis fpc <i>number</i> pic <i>number</i>]
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 <i>number</i> pic <i>number</i>] hierarchy level.
Options	itu-t—International Telephony Union standard. klm—KLM standard. Default: klm
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Virtual Tributary Mapping of Channelized STM1 Interfaces</i> • <i>Configuring the Junos OS to Support Channelized STM1 Interface Virtual Tributary Mapping</i>

working-circuit

Syntax	working-circuit <i>group-name</i> ;
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options aps]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the working router in an APS circuit pair.
Options	<i>group-name</i> —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	<ul style="list-style-type: none"> • Configuring Basic Automatic Protect Switching on page 68 • protect-circuit on page 160

z0-increment

Syntax	(z0-increment no-z0-increment);
Hierarchy Level	[edit interfaces <i>interface-name</i> sonet-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure an incremental STM ID rather than a static one.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an Incrementing STM ID on page 41• sonet-options on page 166

PART 4

Troubleshooting

- [Investigating SONET Interfaces on page 177](#)

CHAPTER 4

Investigating SONET Interfaces

- [Investigating Interface Steps and Commands on page 177](#)
- [Monitoring SONET Interfaces on page 180](#)
- [Using Loopback Testing for SONET Interfaces on page 188](#)
- [Locating SONET Alarms and Errors on page 200](#)
- [Enabling SONET Payload Scrambling on page 219](#)
- [Checking the SONET Frame Checksum on page 223](#)

Investigating Interface Steps and Commands

This section includes the following information to assist you when troubleshooting ATM interfaces:

- [Investigating Interface Steps and Commands Overview on page 177](#)
- [Monitoring Interfaces on page 177](#)
- [Performing a Loopback Test on an Interface on page 178](#)
- [Locating Interface Alarms on page 180](#)

Investigating Interface Steps and Commands Overview

The “[Monitoring Interfaces](#)” on [page 177](#) section helps you determine the nature of the interface problem. The “[Performing a Loopback Test on an Interface](#)” on [page 178](#) section provides information to help you isolate the source of the problem. The “[Locating Interface Alarms](#)” on [page 180](#) section explains some of the alarms and errors for the media.

Monitoring Interfaces

Problem The following steps are a general outline of how you monitor interfaces to determine the nature of interface problems. For more detailed information on a specific interface, see the corresponding monitor interfaces section.

Solution To monitor interfaces, follow these steps:

1. Display the status of an interface.
2. Display the status of a specific interface.

3. Display extensive status information for a specific interface.
4. Monitor statistics for an interface.

The [Table 13 on page 178](#) lists and describes the operational mode commands you use to monitor interfaces.

Table 13: Commands Used to Monitor Interfaces

CLI Command	Description
show interfaces terse <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.

Performing a Loopback Test on an Interface

Problem The following steps are a general outline of how you use loopback testing to isolate the source of the interface problem. For more detailed information on a specific interface, see the corresponding loopback section.

Solution To use loopback testing for interfaces, follow these steps:

1. 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 14 on page 179](#) lists and describes the operational and configuration mode commands you use to perform loopback testing on interfaces (the commands are shown in the order in which you perform them).

Table 14: Commands Used to Perform Loopback Testing on Interfaces

CLI Statement or Command	Interface Type	Description
[edit interfaces <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.
[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.

Table 14: Commands Used to Perform Loopback Testing on Interfaces (*continued*)

CLI Statement or Command	Interface Type	Description
<code>[edit interfaces <i>interface-name</i>] set encapsulation cisco-hdlc</code>	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.
<code>[edit interfaces <i>interface-name</i>] set no-keepalives</code>	T1, T3, SONET, and Multichannel DS3 interfaces	The no-keepalives statement at this level disables the sending of keepalives on the physical interface.
<code>show interfaces <i>interface-name</i> terse</code>	T1, T3, and SONET interfaces	Display summary information about interfaces. (Use to display the status of the logical interfaces for these interfaces.)
<code>ping interface t1-x/y/z <i>local-ip-address</i> bypass-routing count 1000 rapid</code>	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>
<code>show interfaces <i>interface-name</i> extensive</code>	All interfaces	Display very detailed interface information about a specific interface.

Locating Interface Alarms

Problem Locating alarms and errors for the media can be a simple process.

Solution To locate interface alarms and errors, use the **show interfaces *interface-name* extensive** command and examine the output for active alarms and defects.

Monitoring SONET Interfaces

This section includes the following information to assist you when troubleshooting SONET interfaces:

- [Checklist for Monitoring SONET Interfaces on page 181](#)
- [Monitoring SONET Interfaces on page 181](#)
- [Verifying the Status of the Logical Interface on page 187](#)

Checklist for Monitoring SONET Interfaces

Purpose To monitor SONET interfaces and begin the process of isolating SONET interface problems when they occur.

Action [Table 15 on page 181](#) provides the links and commands for monitoring SONET interfaces.

Table 15: Checklist for Monitoring SONET Interfaces

Tasks	Command or Action
“Monitoring SONET Interfaces” on page 181	
1. Displaying the Status of SONET Interfaces on page 181	<code>show interfaces terse so*</code>
2. Displaying the Status of a Specific SONET Interface on page 182	<code>show interfaces so-fpc/pic/port</code>
3. Displaying Extensive Status Information for a Specific SONET Interface on page 183	<code>show interfaces so-fpc/pic/port extensive</code>
4. Monitoring Statistics for a SONET Interface on page 185	<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 on page 181](#)
2. [Displaying the Status of a Specific SONET Interface on page 182](#)
3. [Displaying Extensive Status Information for a Specific SONET Interface on page 183](#)
4. [Monitoring Statistics for a SONET Interface on page 185](#)

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 16 on page 182](#).

Table 16: Status of SONET Interfaces

Physical Interface	Logical Interface	Status Description
so-1/0/0	so-1/0/0.0	This interface has both the physical and logical links up and running.
Admin Up	Admin Up	
Link Up	Link Up	
so-1/1/1	so-1/1/1.0	This interface is administratively disabled. The physical link is healthy (Link Up), but the logical link is not established end to end (Link Down).
Admin Down	Admin Up	
Link Up	Link Down	
so-3/0/1	so-3/0/1.0	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).
Admin Up	Admin Up	
Link Up	Link Down	
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	

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 183](#) 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 185](#) 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 200](#) 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 17 on page 186](#) lists and describes the SONET error statistics in the output for the `monitor interface` command. The output fields are listed in the order in which they appear in the output.

Table 17: SONET Error Statistics

Output Field	Output Field Description
Input errors	Sum of the incoming frame aborts and FCS errors.
Input drops	Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's random early detection (RED) mechanism.
Input framing errors	The number of packets that have FCS errors.
Policed discards	Frames that the incoming packet match code discarded because they were not recognized or of interest. Usually, this field reports protocols that the Junos OS does not handle.
L3 incompletes	Increments when the incoming packet fails Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header would be discarded and this counter would increment.
L2 channel errors	Increments when the software cannot find a valid logical interface for an incoming frame.
L2 mismatch timeouts	Count of malformed or short packets that cause the incoming packet handler to discard the frame as unreadable.

Table 17: SONET Error Statistics (*continued*)

Output Field	Output Field Description
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.

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.

- Related Documentation**
- [Monitoring Interfaces on page 177](#)
 - [Performing a Loopback Test on an Interface on page 178](#)

Using Loopback Testing for SONET Interfaces

This section includes the following information to assist you when troubleshooting SONET interfaces:

- [Checklist for Using Loopback Testing for SONET Interfaces on page 189](#)
- [Diagnosing a Suspected Hardware Problem with a SONET Interface on page 190](#)
- [Creating a Loopback on page 191](#)

- [Setting Clocking to Internal on page 192](#)
- [Verifying That the SONET Interface Is Up on page 192](#)
- [Clearing SONET Interface Statistics on page 194](#)
- [Checking That the Received and Transmitted Path Trace Are the Same on page 194](#)
- [Forcing the Link Layer to Stay Up on page 195](#)
- [Pinging the SONET Interface on page 196](#)
- [Checking for SONET Interface Error Statistics on page 197](#)
- [Diagnosing a Suspected Circuit Problem on page 198](#)

Checklist for Using Loopback Testing for SONET Interfaces

Purpose To use loopback testing to isolate SONET interface problems.

Action [Table 18 on page 189](#) provides the links and commands for using loopback testing for SONET interfaces.

Table 18: Checklist for Using Loopback Testing for SONET Interfaces

Tasks	Command or Action
“Diagnosing a Suspected Hardware Problem with a SONET Interface” on page 190	
1. Creating a Loopback on page 191	Create a loopback.
a. Creating a Physical Loopback on page 191	Connect the transmit port to the receive port.
b. Configuring a Local Loopback on page 191	<code>[edit interfaces <i>interface-names</i>sonet-options] set loopback local show commit</code>
2. Setting Clocking to Internal on page 192	<code>[edit interfaces <i>interface-name</i>] set clocking internal show commit</code>
3. Verifying That the SONET Interface Is Up on page 192	<code>show interfaces so-<i>fpc/pic/port</i></code>
4. Clearing SONET Interface Statistics on page 194	<code>clear interfaces statistics so-<i>fpc/pic/port</i></code>
5. Checking That the Received and Transmitted Path Trace Are the Same on page 194	<code>show interfaces so-<i>fpc/pic/port</i> extensive</code>
6. Forcing the Link Layer to Stay Up on page 195	
a. Configuring Encapsulation to Cisco-HDLC on page 195	<code>[edit interfaces <i>interface-name</i>] set encapsulation cisco-hdlc show commit</code>

Table 18: Checklist for Using Loopback Testing for SONET Interfaces (*continued*)

Tasks	Command or Action
b. Configuring No-Keepalives on page 196	<code>[edit interfaces <i>interface-name</i>] set no-keepalives show commit</code>
7. Verifying the Status of the Logical Interface on page 187	<code>show interfaces so-<i>fpc/pic/port</i> show interfaces so-<i>fpc/pic/port</i> terse</code>
8. Pinging the SONET Interface on page 196	<code>ping interface so-<i>fpc/pic/port</i> local-IP-address bypass-routing count 1000 rapid</code>
9. Checking for SONET Interface Error Statistics on page 197	<code>show interfaces so-<i>fpc/pic/port</i> extensive</code>
“Diagnosing a Suspected Circuit Problem” on page 198	
1. Creating a Loop from the Router to the Network on page 198	<code>[edit interfaces <i>interface-name</i> sonet-options] set loopback remote show commit</code>
2. Creating a Loop to the Router from Various Points in the Network on page 199	Perform Steps 2 through 8 from “ Diagnosing a Suspected Hardware Problem with a SONET Interface ” on page 190.

Diagnosing a Suspected Hardware Problem with a SONET Interface

Problem When you suspect a hardware problem, take the following steps to verify if there is a problem.

Solution To diagnose a suspected hardware problem with the SONET interface, follow these steps:

- [Creating a Loopback on page 191](#)
- [Setting Clocking to Internal on page 192](#)
- [Verifying That the SONET Interface Is Up on page 192](#)
- [Clearing SONET Interface Statistics on page 194](#)
- [Checking That the Received and Transmitted Path Trace Are the Same on page 194](#)
- [Forcing the Link Layer to Stay Up on page 195](#)
- [Verifying the Status of the Logical Interface on page 187](#)
- [Pinging the SONET Interface on page 196](#)
- [Checking for SONET Interface Error Statistics on page 197](#)

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 on page 191](#)
2. [Configuring a Local Loopback on page 191](#)

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.

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.

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.

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 194.

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 19 on page 194](#) lists problem situations and actions for a physical link that is down.

Table 19: Problems and Solutions for a Physical Link That Is Down

Problem	Action
Cable mismatch	Verify that the fiber connection is correct.
Damaged and/or dirty cable	Verify that the fiber can successfully loop a known good port of the same type.
Too much or too little optical attenuation	Verify that the attenuation is correct per the PIC optical specifications.
The transmit port is not transmitting within the dBm optical range per the specifications	Verify that the Tx power of the optics is within range of the PIC optical specification.

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.

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 195](#).

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.

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 on page 195](#)
2. [Configuring No-Keepalives on page 196](#)

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.

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.

Pinging the SONET Interface

Purpose To ping the local interface and verify the loopback connection, use the following Junos OS CLI operational mode command:

Action `user@host> ping interface so-fpc/pic/port local-IP-address bypass-routing count 1000 rapid`

Sample Output

```
user@host# ping interface so-2/2/0 10.0.2.1 bypass-routing count 1000 rapid
```



```

PING 10.0.2.1 (10.0.2.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
--- 10.0.2.1 ping statistics ---
1000 packets transmitted, 1000 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.374/0.446/9.744/0.754 ms

```

Meaning This command sends 1000 ping packets out of the interface to the local IP address. The ping should complete successfully with no packet loss. If there is any persistent packet loss, open a case with the Juniper Networks Technical Assistance Center (JTAC) at support@juniper.net or at 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

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).

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 on page 198](#)
2. [Creating a Loop to the Router from Various Points in the Network on page 199](#)

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.

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 190](#). Keep in mind that any problems encountered in the test indicate a problem with the connection from the router to the loopback in the network.

By performing tests to loopbacks at various points in the network, you can isolate the source of the problem.

Related Documentation

- [Investigating Interface Steps and Commands on page 177](#)
- [Monitoring SONET Interfaces on page 180](#)
- [Locating SONET Alarms and Errors on page 200](#)
- [Enabling SONET Payload Scrambling on page 219](#)
- [Checking the SONET Frame Checksum on page 223](#)

Locating SONET Alarms and Errors

This section includes the following information to assist you when troubleshooting SONET interfaces:

- [List of Common SONET Alarms and Errors on page 200](#)
- [Displaying SONET Alarms and Errors on page 201](#)
- [Locating Most Common SONET Alarms and Errors on page 204](#)
- [Locating Loss of Signal Alarms on page 205](#)
- [Locating Alarm Indication Signal Alarms on page 206](#)
- [Locating Remote Defect Indication Alarms on page 207](#)
- [Locating Remote Error Indication Line Errors on page 209](#)
- [Locating Bit Error Rate Alarms on page 211](#)
- [Locating Payload Label Mismatch Path Alarms on page 213](#)
- [Locating Loss of Pointer Path Alarms on page 215](#)
- [Locating Unequipped Payload Alarms on page 216](#)
- [Locating Phase Lock Loop Alarms on page 217](#)

List of Common SONET Alarms and Errors

Purpose To check for the most common SONET alarms and errors you can encounter when investigating line problems on a Juniper Networks router.

Action [Table 20 on page 200](#) provides links and commands for checking SONET alarms and errors.

Table 20: List of Common SONET Alarms and Errors

Tasks	Command or Action
“Displaying SONET Alarms and Errors” on page 201	<code>show interfaces so-fpc/pic/port extensive</code>
“Locating Most Common SONET Alarms and Errors” on page 204	
1. Locating Loss of Signal Alarms on page 205	Check the connection between the router port and the first SONET network element.
2. Locating Alarm Indication Signal Alarms on page 206	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 207	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 209	Upstream from the router, check the line-terminating equipment and path-terminating equipment for an error in the B2 or B3 byte.

Table 20: List of Common SONET Alarms and Errors (*continued*)

Tasks	Command or Action
5. Locating Bit Error Rate Alarms on page 211	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 213	Check the received and transmitted C2 byte.
7. Locating Loss of Pointer Path Alarms on page 215	Check that both sides of the connection are configured for concatenate mode or nonconcatenate mode.
8. Locating Unequipped Payload Alarms on page 216	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 217	Investigate the timing source, and configure the clocking to external or internal depending on the situation.

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:
    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...]

```

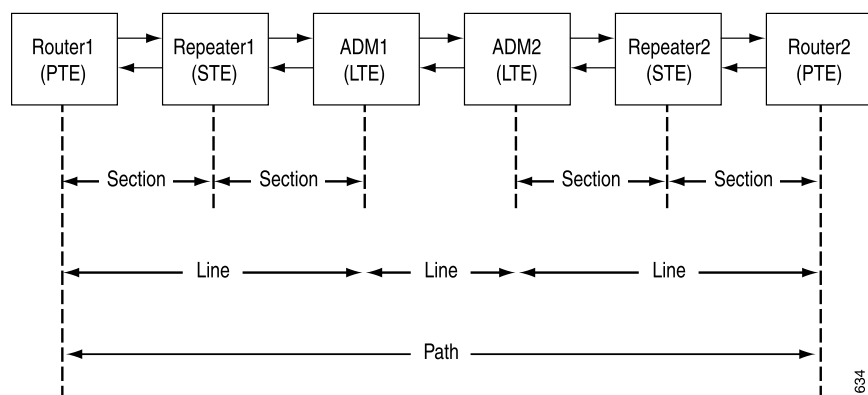
Meaning

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 202](#) shows an example of a SONET network with the section, line, and path areas delimited. [Figure 5 on page 202](#) 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

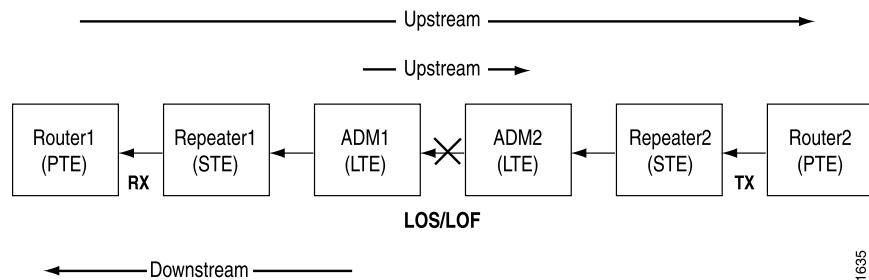
The SONET system hierarchy is comprised of PTEs, LTEs, and STEs. The characteristics of each are as follows:

- 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 204](#).)

Upstream and Downstream

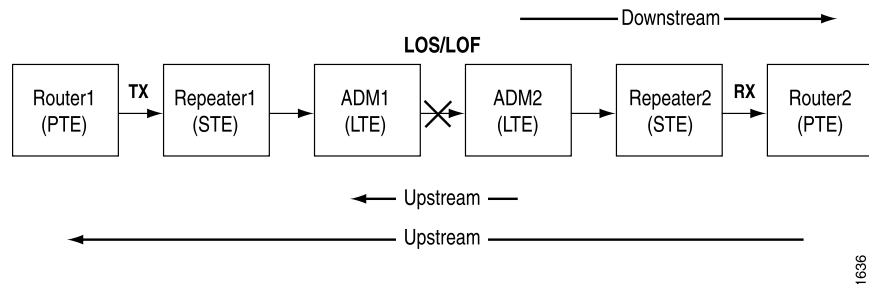
The terms *upstream* and *downstream* are used in defining SONET alarms and errors. The terms are meaningful when viewed from the point of view of the failure in the circuit.

For example, in [Figure 6 on page 204](#) 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 204](#), 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.

Locating Most Common SONET Alarms and Errors

Problem This information describes the most common SONET alarms and errors you can encounter when investigating line problems on a Juniper Networks router.

Solution The following alarms and errors are described in this section:

- [Locating Loss of Signal Alarms on page 205](#)
- [Locating Alarm Indication Signal Alarms on page 206](#)
- [Locating Remote Defect Indication Alarms on page 207](#)

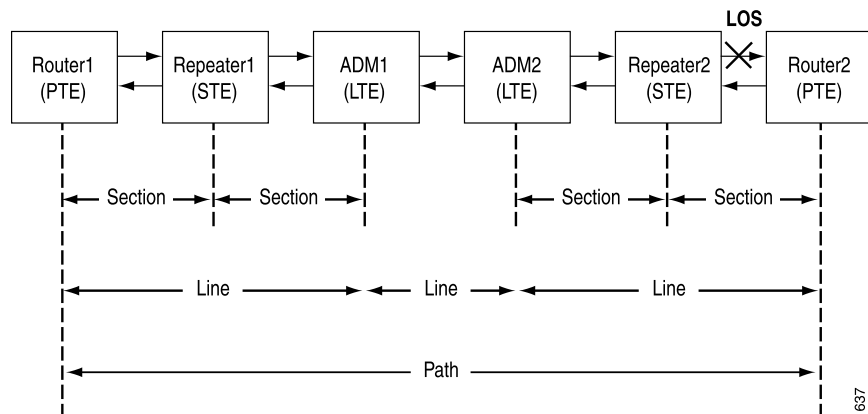
- [Locating Remote Error Indication Line Errors on page 209](#)
- [Locating Bit Error Rate Alarms on page 211](#)
- [Locating Payload Label Mismatch Path Alarms on page 213](#)
- [Locating Loss of Pointer Path Alarms on page 215](#)
- [Locating Unequipped Payload Alarms on page 216](#)
- [Locating Phase Lock Loop Alarms on page 217](#)

Locating Loss of Signal Alarms

Problem A loss of signal (LOS) alarm indicates that there is a physical link problem with the connection to the router receive port from the neighboring SONET equipment transmit port.

Solution To locate the LOS alarm, check the connection between the router port and the first SONET network element. In the example network in [Figure 8 on page 205](#), 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:
  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.

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 an upstream SONET section.
- Alarm indication signal line (AIS-L) is sent by an STE to a downstream LTE when an LOS or LOF is detected on an incoming SONET section.

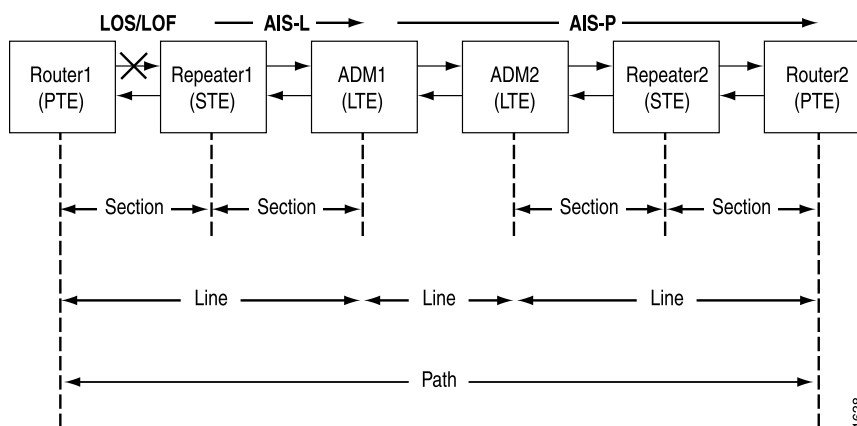
1. [Example of a Router Receiving Only an AIS-P Alarm on page 206](#)
2. [Example of a Router Receiving Both an AIS-L and AIS-P Alarm on page 207](#)

Example of a Router Receiving Only an AIS-P Alarm

Problem Figure 9 on page 206 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 206, the progression of events occurring after the failure is as follows:

1. Repeater 1 detects an LOS or LOF on an incoming SONET section.
2. Repeater 1 sends an AIS-L downstream to ADM1 (LTE).

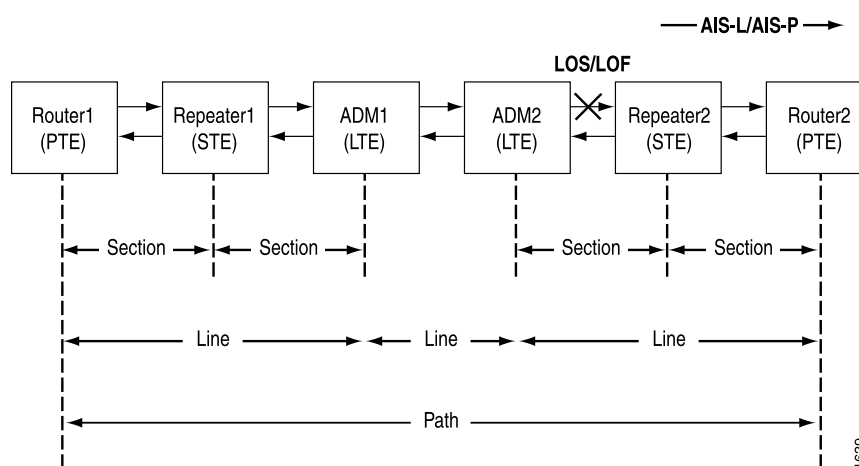
3. ADM 1 sends an AIS-P to Router 2 (PTE).
4. The only alarm that Router 2 receives is the AIS-P alarm from ADM 1.

Example of a Router Receiving Both an AIS-L and AIS-P Alarm

Problem Figure 10 on page 207 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 207, 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.

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.

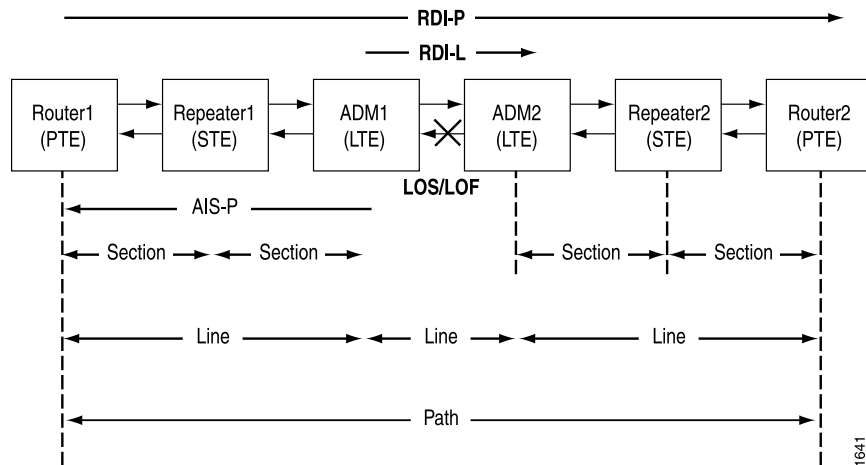
1. [Example of a Router Receiving Only an RDI-P Alarm on page 208](#)
2. [Example of a Router Receiving Both an RDI-L and RDI-P Alarm on page 208](#)

Example of a Router Receiving Only an RDI-P Alarm

Problem Figure 11 on page 208 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 208, the progression of events occurring after the failure is as follows:

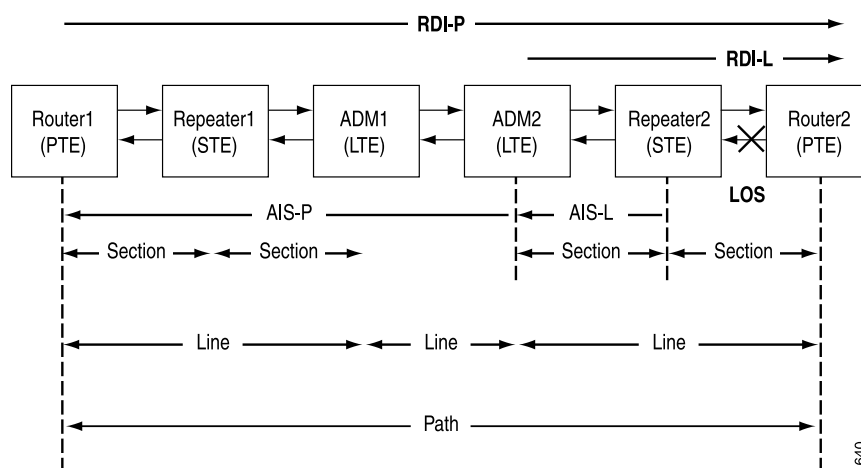
1. ADM 1 detects an LOS or LOF on an incoming SONET section.
2. ADM 1 sends an RDI-L to ADM 2.
3. ADM 1 sends an AIS-P downstream to Router 1.
4. Router 1 sends an RDI-P upstream to Router 2.
5. Router 2 only receives an RDI-P alarm.

Example of a Router Receiving Both an RDI-L and RDI-P Alarm

Problem Figure 12 on page 209 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 209](#), 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.

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.

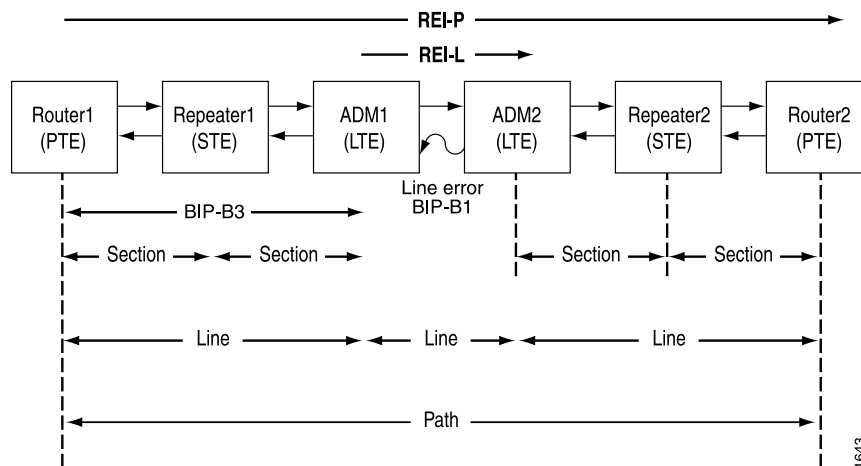
1. [Example of Only an REI-P Counter Incrementing on page 209](#)
2. [Example of Both REI-L and REI-P Counters Incrementing on page 210](#)

Example of Only an REI-P Counter Incrementing

Problem [Figure 13 on page 210](#) 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 210](#), the progression of events occurring after the failure is as follows:

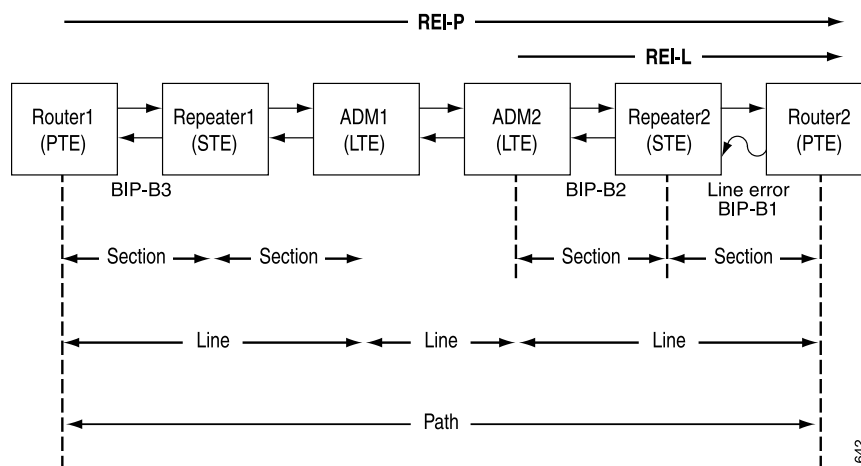
1. ADM 1 detects parity errors in the B1 byte.
2. ADM 1 sends an REI-L upstream to ADM 2.
3. Router 1 detects parity errors in the B3 byte.
4. Router 1 sends an REI-P upstream to Router 2.
5. Router 2 only sees an REI-P incrementing counter.

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

Problem [Figure 14 on page 211](#) 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 211](#), 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.

Locating Bit Error Rate Alarms

Problem Bit error rate (BER) alarms are declared when the number of BIP-B2 errors hits a certain threshold. Depending on the threshold, there are two types of BER alarms. In both cases the interface is taken down.

- Bit error rate-signal degrade (BERR-SD) is declared when a bit error rate of 10^{-6} is reached.
- Bit error rate-signal failure (BERR-SF) is declared when a bit error rate of 10^{-3} is reached.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

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

Sample Output

The following sample output displays a BERR-SD error:

```
user@router2> show interfaces so-1/1/1 extensive
```

```
[... Output truncated...]
Active alarms : BERR-SD
Active defects : BERR-SD
SONET PHY:
Seconds      Count  State
  PLL Lock      0      0 OK
  PHY Light      0      0 OK
SONET section:
  BIP-B1      22     101
  SEF          0      0 OK
  LOS          0      0 OK
  LOF          0      0 OK
  ES-S        22
  SES-S        0
  SEFS-S       0
SONET line:
  BIP-B2      22     103
  REI-L        0      0
  RDI-L        0      0 OK
  AIS-L        0      0 OK
  BERR-SF      0      0 OK
  BERR-SD     11     53 Defect Active
  ES-L        22
  SES-L        4
  UAS-L        2
  ES-LFE       0
  SES-LFE      0
  UAS-LFE      0
SONET path:
  BIP-B3      22     166
  REI-P        0      0
  LOP-P        0      0 OK
  AIS-P        0      0 OK
  RDI-P        0      0 OK
  UNEQ-P       0      0 OK
  PLM-P        0      0 OK
  ES-P        22
  SES-P        3
  UAS-P        1
  ES-PFE       0
  SES-PFE      0
  UAS-PFE      0
```

Meaning

Bit error rates can be caused by any of the following situations:

- Degrading optical fiber
- Optical transmitter or receiver problems
- Dirty fiber-optic connector
- Clocking issues
- Too much attenuation in the optical signal
- BIP-B1 and BIP-B3 are not used in the BER alarm calculations

Locating Payload Label Mismatch Path Alarms

Problem 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 21 on page 214](#) shows the synchronous transport signal (STS) path signal label assignments as described in Issue 3 (Sept. 2000) of the GR-253 CORE.

Table 21: STS Path Signal Label Assignments

Code (Hex)	Content of the STS SPE
00	Unequipped
01	Equipped - Nonspecific Payload
02	VT-Structured STS1 SPE a
03	Locked VT Mode a
04	Asynchronous Mapping for DS3
12	Asynchronous Mapping for DS4NA
13	Mapping for ATM
14	Mapping for DQDB
15	Asynchronous Mapping for FDDI
16	HDLC-over-SONET Mapping
FE	O.181 Test Signal (TSS1 to TSS3) Mapping b

On POS interfaces, Juniper Networks routers by default accept a C2 value of either **0xcf** or **0x16**. Any other values raise a PLM-P alarm. An important thing to remember is that the C2 byte value of **0x16** is a standardized value (per RFC 2615, G.707, and GR-253) used for POS interfaces. **0xcf** is used by default since much SONET equipment still uses this value. If you need to change this byte, use the **rfc-2615** option as follows:

```
user@host# set interface so-fpc/pic/port sonet-options rfc-2615
```

This option changes the following values:

```
C2 byte 22 (0x16)
FCS 32
payload-scrambling (this was already the default)
```

Locating Loss of Pointer Path Alarms

Problem A loss of pointer path (LOP-P) alarm indicates a possible provisioning problem and occurs when the Juniper Networks router cannot determine a valid payload pointer. The Juniper Networks router monitors the H1/H2 bytes, located in the line overhead area. This alarm is usually discovered upon initial provisioning of SONET circuits, and is not generally seen after the router has been deployed in the network for some time.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

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

Sample Output

```
user@host> show interfaces so-1/1/1 extensive
[...Output truncated...]
SONET alarms : LOP
SONET defects : LOP
SONET PHY:
  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.

Locating Unequipped Payload Alarms

Problem An unequipped payload (UNEQ-P) alarm indicates a possible provisioning problem and occurs when the Juniper Networks router detects a value of 0x00 in the C2 byte.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

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

Sample Output

```

user@host> show interfaces so-1/1/1 extensive
[...Output truncated...]
SONET alarms : UNEQ-P
SONET defects : UNEQ-P
SONET PHY:
  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.

Locating Phase Lock Loop Alarms

Problem The phase lock loop (PLL) alarm occurs when the PLL cannot lock on to a timing device, and indicates a possible hardware or network timing problem.

Solution To display SONET alarms and errors, use the following Junos OS CLI operational mode command:

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

Sample Output

```

user@host> show interfaces so-1/1/1 extensive
[...Output truncated...]
Active alarms : PLL
Active defects : PLL
SONET PHY:
PLL Lock      26      0 PLL Lock Error
PHY Light      0      0 OK
SONET section:
BIP-B1        0      0
SEF           0      0 OK
LOS           0      0 OK
LOF           0      0 OK
ES-S          0
SES-S         0

```

```

SEFS-S                                0
SONET line:
BIP-B2                                0          0
REI-L                                 0          0
RDI-L                                 3          3 OK
AIS-L                                 0          0 OK
BERR-SF                               0          0 OK
BERR-SD                               0          0 OK
ES-L                                  0
SES-L                                  0
UAS-L                                  0
ES-LFE                                0
SES-LFE                                0
UAS-LFE                                0
SONET path:
BIP-B3                                0          0
REI-P                                 0          0
LOP-P                                 0          0 OK
AIS-P                                 0          0 OK
RDI-P                                 0          0 OK
UNEQ-P                                0          0 OK
PLM-P                                 0          0 OK
ES-P                                  0
SES-P                                  0
UAS-P                                  0
ES-PFE                                0
SES-PFE                                0
UAS-PFE                                0
[...Output truncated...]

```

Meaning

The sample output shows a PLL alarm lasting for 26 seconds. You must investigate the timing source to diagnose the problem. The timing source is derived from an incoming SONET circuit (when **clock external** is configured), or from the onboard Stratum 3 clock (when **clock internal** is configured). Internal clocking is the default for Juniper Networks routers.

The cause of the problem differs depending on the type of system board on the router. (See [Table 22 on page 219](#).) For example:

- On the M20 and M40 Internet router OC48-SM-IR PIC and the M160 Internet router OC192 board, the problem might be caused by the following:
 - An out-of-tolerance clock coming from the far end, if clocking external is configured.
 - An out-of-tolerance clock coming from the far end or a problem with the board being unable to lock on to its internal clock to derive the transmit clock, if clocking internal is configured.
 - On OC3 and OC12 PICs, the PIC not establishing a lock to the onboard clock to derive the outgoing clock.
- To further diagnose the problem, try the following:
 - Configure clocking to external. If the alarm disappears, the board might not have locked to the internal clock used to derive the outgoing clock.

- Configure clocking to internal and make sure that a loopback fiber is plugged in. If the PLL alarm persists, it is most likely a hardware problem. However, you may not be able to determine if the direction is on the inbound or outbound side of the board.

Table 22 on page 219 shows the location of the onboard clock on the various system boards of Juniper Networks routers.

Table 22: Location of the Onboard Clock

Router	System Board
M5, M10, M20, and M40 routers	System Control Board (SCB), System and Switch Board (SSB), Switching and Forwarding Module (SFM), and Single Board Router (SBR)
OC48-SM-IR PIC used on the M20 and M40 routers	Flexible PIC Concentrator (FPC)
M40e and M160 routers	Miscellaneous Control Subsystem (MCS)
T-series routing platforms	SONET Clock Generator (SCG)

Related Documentation

- [Investigating Interface Steps and Commands on page 177](#)
- [Monitoring SONET Interfaces on page 180](#)
- [Using Loopback Testing for SONET Interfaces on page 188](#)
- [Enabling SONET Payload Scrambling on page 219](#)
- [Checking the SONET Frame Checksum on page 223](#)

Enabling SONET Payload Scrambling

This section includes the following information to assist you when troubleshooting SONET interfaces:

- [Checklist for Enabling SONET Payload Scrambling on page 219](#)
- [Understanding SONET Payload Scrambling on page 220](#)

Checklist for Enabling SONET Payload Scrambling

Table 23 on page 219 provides links and commands for SONET payload scrambling and how to check and configure it.

Table 23: Checklist for Enabling SONET Payload Scrambling

Tasks	Command or Action
“Understanding SONET Payload Scrambling” on page 220	
1. Checking SONET HDLC Payload Scrambling on page 221	<code>show configuration interfaces interface-name</code> <code>show interfaces interface-name</code>

Table 23: Checklist for Enabling SONET Payload Scrambling (*continued*)

Tasks	Command or Action
2. Configuring SONET HDLC Payload Scrambling on page 222	<pre>[edit] edit interfaces so-fpc/pic/port sonet-options set payload-scrambler show commit</pre>

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 on page 221](#)
2. [Configuring SONET HDLC Payload Scrambling on page 222](#)

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 9.0.0.2/32 {
            destination 9.0.0.1;
        }
    }
    family mpls;
}
```

Sample Output 2

```
user@host> show configuration interfaces so-0/0/0
encapsulation cisco-hdlc;
sonet-options {
    no-payload-scrambler;
}
unit 0 {
    family inet {
        address 9.0.0.2/32 {
            destination 9.0.0.1;
        }
    }
    family mpls;
}
```

Sample Output 3

```
user@host> show interfaces so-0/0/1
Physical interface: so-0/0/1, Enabled, Physical link is Up
  Interface index: 48, SNMP ifIndex: 114
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
  Loopback: None, FCS: 32,
  Payload scrambler: Disabled
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 70627 (00:00:07 ago), Output: 70791 (00:00:08 ago)
  LCP state: Opened
```

```
NCP state: inet: Opened, inet6: Not-configured, iso: Opened, mpls: Not-configured

Input rate      : 78056456 bps (6504 pps)
Output rate     : 78044840 bps (6503 pps)
SONET alarms    : None
SONET defects   : None
Logical interface so-0/0/1.0 (Index 61) (SNMP ifIndex 118)
  Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
  Protocol inet, MTU: 4470, Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 192.168.50.0/30, Local: 192.168.50.1
    Protocol iso, MTU: 4470, Flags: None
```

Meaning Sample output 1 shows that the SONET interface payload scrambling has been enabled.

Sample output 2 shows that HDLC payload scrambling has been disabled. If you use the **show configuration** or **show configuration interfaces** command, you must scroll to the particular interface for payload scrambling status.

Sample output 3 shows that payload scrambling has been disabled. To explicitly configure payload scrambling, see [“Configuring SONET HDLC Payload Scrambling” on page 222](#).

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
```

Related Documentation

- [Investigating Interface Steps and Commands on page 177](#)
- [Monitoring SONET Interfaces on page 180](#)
- [Using Loopback Testing for SONET Interfaces on page 188](#)
- [Locating SONET Alarms and Errors on page 200](#)
- [Checking the SONET Frame Checksum on page 223](#)

Checking the SONET Frame Checksum

This section includes the following information to assist you when troubleshooting SONET interfaces:

- [Checklist for Checking the SONET Frame Checksum on page 223](#)
- [Understand the SONET Frame Checksum on page 224](#)
- [Checking the SONET Frame Checksum on page 224](#)
- [Configuring a SONET Frame Checksum on page 228](#)

Checklist for Checking the SONET Frame Checksum

Purpose To check and configure SONET frame checksum.

Action [Table 24 on page 223](#) provides the links and commands for SONET frame checksum.

Table 24: Checklist for Checking the SONET Frame Checksum

Tasks	Command or Action
“Understand the SONET Frame Checksum” on page 224	
“Checking the SONET Frame Checksum” on page 224	
1. Examining Output for Framing Errors on page 224	<code>show interfaces <i>interface-name</i> extensive</code>
2. Checking the FCS Configuration on page 226	<code>show configuration interfaces <i>interface-name</i></code> <code>show interfaces <i>interface-name</i></code>
“Configuring a SONET Frame Checksum” on page 228	
1. Returning to the Default 16-Bit Checksum on page 228	<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 228	<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>

Table 24: Checklist for Checking the SONET Frame Checksum (*continued*)

Tasks	Command or Action
3. Configuring a 32-Bit Checksum on page 229	<pre>[edit] edit interfaces so-fpc/pic/port sonet-options set (fcs 32 rfc-2615) show commit</pre>

Understand the SONET Frame Checksum

Problem 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 This chapter describes the following tasks:

- [Checking the SONET Frame Checksum on page 224](#)
- [Configuring a SONET Frame Checksum on page 228](#)

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 on page 224](#)
2. [Checking the FCS Configuration on page 226](#)

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:
  PLL Lock          0          0 OK
  PHY Light         0          0 OK
SONET section:
  BIP-B1            0          0
  SEF               0          0 OK
  LOS               0          0 OK
  LOF               0          0 OK
  ES-S              0
  SES-S             0
  SEFS-S            0
SONET line:
  BIP-B2            0          0
  REI-L             0          0
  RDI-L             0          0 OK
  AIS-L             0          0 OK
  BERR-SF           0          0 OK
  BERR-SD           0          0 OK
  ES-L              0
  SES-L             0
  UAS-L             0
  ES-LFE            0
  SES-LFE           0
  UAS-LFE           0
SONET path:
  BIP-B3            0          0
  REI-P             0          0
  LOP-P             0          0 OK
  AIS-P             0          0 OK
  RDI-P             0          0 OK
  UNEQ-P            0          0 OK
  PLM-P             0          0 OK

```

```

ES-P                                0
SES-P                               0
UAS-P                               0
ES-PFE                             0
SES-PFE                            0
UAS-PFE                            0
Received SONET overhead:
F1      : 0x00, J0      : 0x00, K1      : 0x00, K2      : 0x00
S1      : 0x00, C2      : 0xcf, C2(cmp) : 0xcf, F2      : 0x00
Z3      : 0x00, Z4      : 0x00, S1(cmp) : 0x00, V5      : 0x00
V5(cmp) : 0x00
Transmitted SONET overhead:
F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00
S1      : 0x00, C2      : 0xcf, F2      : 0x00, Z3      : 0x00
Z4      : 0x00, V5      : 0x00
Received path trace: router2 so-1/3/1
73 6c 69 70 70 65 72 79 20 73 6f 2d 31 2f 33 2f  router2 so-1/3/1
31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 0a .....
Transmitted path trace: router1 so-1/0/0
68 61 69 72 79 20 73 6f 2d 31 2f 30 2f 30 00 00  router1 so-1/0/0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
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.

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 9.0.0.2/32 {
      destination 9.0.0.1;
    }
  }
  family mpls;
}
```

Sample Output 2

```
user@host> show interfaces so-0/0/1
Physical interface: so-0/0/1, Enabled, Physical link is Up
  Interface index: 48, SNMP ifIndex: 114
  Link-level type: PPP, MTU: 4474, Clocking: Internal, SONET mode, Speed: OC3,
  Loopback: None, FCS: 32,
    Payload scrambler: Disabled
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link flags     : Keepalives
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 70627 (00:00:07 ago), Output: 70791 (00:00:08 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Opened, mpls: Not-configured

  Input rate      : 78056456 bps (6504 pps)
  Output rate     : 78044840 bps (6503 pps)
  SONET alarms    : None
  SONET defects   : None
  Logical interface so-0/0/1.0 (Index 61) (SNMP ifIndex 118)
    Flags: Point-To-Point SNMP-Traps Encapsulation: PPP
    Protocol inet, MTU: 4470, Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 192.168.50.0/30, Local: 192.168.50.1
    Protocol iso, MTU: 4470, Flags: None
```

Meaning

Sample output 1 shows that FCS 32 is configured. If you use the **show configuration** or **show configuration interfaces** command, you must scroll to the particular interface for the FCS configuration status.

Meaning Sample output 2 shows that FCS 32 is configured. To change the FCS configuration, see [“Returning to the Default 16-Bit Checksum” on page 228](#), [“Configuring a 16-Bit Checksum” on page 228](#), or [“Configuring a 32-Bit Checksum” on page 229](#).

Configuring a SONET Frame Checksum

After you have checked the FCS and determined that a problem exists, you might need to do one of the following, depending on the situation:



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

- [Returning to the Default 16-Bit Checksum on page 228](#)
- [Configuring a 16-Bit Checksum on page 228](#)
- [Configuring a 32-Bit Checksum on page 229](#)

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
```

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
```

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.

- Related Documentation**
- [Investigating Interface Steps and Commands on page 177](#)
 - [Monitoring SONET Interfaces on page 180](#)
 - [Using Loopback Testing for SONET Interfaces on page 188](#)
 - [Locating SONET Alarms and Errors on page 200](#)
 - [Enabling SONET Payload Scrambling on page 219](#)

PART 5

Index

- [Index on page 233](#)
- [Index of Statements and Commands on page 241](#)

Index

Symbols

#, comments in configuration statements.....	xviii
(), in syntax descriptions.....	xviii
10-Gigabit Ethernet interfaces	
SONET.....	95
< >, in syntax descriptions.....	xviii
[], in configuration statements.....	xviii
{ }, in configuration statements.....	xviii
(pipe), in syntax descriptions.....	xviii

A

add/drop multiplexer See ADM	
ADM.....	202
advertise-interval statement.....	117
aggregate statement	
usage guidelines.....	107
aggregated SONET interfaces.....	107
configuring.....	106
example configuration.....	110
firewall filters.....	109
example configuration.....	109
link speed.....	108
minimum links.....	108
multicast statistics.....	111
aggregated-sonet-options statement.....	118
usage guidelines.....	106
AIS-P alarms	
figure.....	206
alarm triggers, SONET interfaces	
hold timers.....	63
alarms	
AIS, locating.....	206
AIS-L, locating	207
AIS-P, locating	206
LOS, locating	205
SONET interfaces, checklist.....	200
SONET network, figure.....	204
annex statement.....	119

APS

link PIC redundancy	
example configuration.....	90
overview.....	64
aps statement.....	120
annex-b.....	119
ATM cells.....	220
atm-options statement.....	121
authentication-key statement.....	122

B

braces, in configuration statements.....	xviii
brackets	
angle, in syntax descriptions.....	xviii
square, in configuration statements.....	xviii
bytes statement.....	123

C

c2 SONET header byte.....	48, 50
cables	
damaged or dirty.....	194
mismatch.....	194
single-mode fiber.....	191
cell-payload scrambling.....	220
channelized OC48 interfaces	
SONET header bytes.....	48, 50
checklist for alarms	
SONET interfaces.....	200
checklist for monitoring	
SONET interfaces	181
checklist for payload scrambling, SONET	219
checklist for SONET frame checksum	223
checksum, SONET frame.....	223
circuit problems	
SONET interfaces	198
Cisco-HDLC, configuring encapsulation	
SONET interfaces.....	195
clear interfaces statistics command	
SONET interfaces.....	186, 194
clock	
location of onboard, table	219
clock sources.....	124
clocking	
SONET interfaces	192
clocking statement.....	124
commands for router management,	
interfaces.....	178, 179
comments, in configuration statements.....	xviii

container interfaces	
configuration example.....	74
container-devices statement.....	125
device-count.....	125
container-list statement.....	125
container-options statement.....	126
container-type statement.....	126
conventions	
text and syntax.....	xvii
cumulative statistics	
SONET interfaces.....	186
curly braces, in configuration statements.....	xviii
customer support.....	xix
contacting JTAC.....	xix

D

damping	
interface transitions.....	102
data integrity.....	220
defect triggers, SONET interfaces.....	59, 63
configuration example.....	63
hold timers.....	63
delete fcs 32 command	228
dense wavelength-division multiplexing <i>See</i> DWDM	
documentation	
comments on.....	xix
downstream, SONET alarms and errors,	
defining.....	203
DWDM.....	29

E

edit interfaces command.....	179
SONET interfaces	192, 195, 196, 228
edit interfaces sonet-options command	
SONET interfaces.....	191, 199, 222
encapsulation	
example configuration.....	104
on logical interfaces.....	105
on physical interfaces.....	103
SONET interfaces	195
encapsulation statement.....	127
container interface.....	127
logical interfaces.....	128
usage guidelines.....	105
physical interfaces	
usage guidelines.....	103
error statistics	
SONET interfaces	197

errors	
SONET interfaces.....	185
external clock sources.....	124

F

f1 SONET header byte.....	48, 50
f2 SONET header byte.....	48, 50
family statement.....	132
fast-aps-switch statement.....	136
fcs statement.....	137
filter statement.....	138
filters.....	109
on aggregated links.....	109
example configuration.....	109
<i>See also</i> firewall filters	
Flexible PIC Concentrator FPC <i>See</i> FPC	
font conventions.....	xvii
force statement.....	139
Forwarding Module SFM <i>See</i> SFM	
FPC	219
frame checksum, SONET interfaces	223
frame error control, SONET interfaces overview	
.....	224
Frame Relay encapsulation	
logical interfaces.....	105
physical interfaces.....	103
Frame Relay Ether Type encapsulation	
physical interfaces.....	103
frames, SONET	202
framing errors	
SONET interfaces.....	186
framing statement	
SONET and SDH interfaces.....	140

H

HDLC	
configuring encapsulation	
SONET interfaces	195
payload scrambling	
SONET interfaces, checking	221
header byte values.....	48, 50
hierarchy	
SONET	203
hold-time statement.....	141
APS.....	141
damping interface transitions	
usage guidelines.....	102

- SONET defect triggers
 - usage guidelines.....63
 - SONET/SDH Defect Triggers.....142
- I**
- icons defined, notice.....xvii
 - ignore statement.....143
 - input keepalives, SONET interfaces.....186
 - interface transitions
 - damping.....102
 - interfaces
 - aggregated SONET.....106
 - alarms180
 - clock sources.....124
 - configuration statements.....4, 117
 - investigation process180
 - locating alarms.....180
 - loopback test commands, table.....179
 - monitoring commands, table.....178
 - monitoring, general steps.....177
 - overview.....29
 - troubleshooting overview, (monitoring, loopback testing, and locating alarms).....177
 - internal clock sources.....124
 - investigation process
 - interfaces.....180
- K**
- keepalives, disabling196
- L**
- LAN PHY.....95
 - leaky bucket properties.....100, 101
 - line overhead bytes203
 - line-terminating equipment See LTE
 - lines, SONET203
 - link aggregation
 - SONET interfaces.....107
 - link layer, forcing up
 - SONET interfaces.....195
 - link speed
 - SONET aggregation.....108
 - link stability.....222
 - link-speed statement
 - usage guidelines.....108
 - lockout statement.....144
 - logical interfaces
 - SONET interfaces, status.....187, 188
 - logical systems
 - configuration statements.....21
 - loop-timing statement.....145
 - loopback capability
 - SONET interfaces
 - example configuration.....54
 - loopback statement
 - ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3.....146
 - LOS alarms
 - SONET interfaces.....205
 - LTE.....202
- M**
- manuals
 - comments on.....xix
 - MCS219
 - member-interface-speed statement.....147
 - member-interface-type statement.....148
 - minimum links for aggregation
 - SONET links.....108
 - minimum-links statement.....149
 - usage guidelines.....108
 - Miscellaneous Control Subsystem See MCS
 - monitor interface command
 - SONET interfaces.....185
 - mpls statement.....150
 - SONET/SDH interfaces
 - usage guidelines.....98
 - MSP
 - overview.....64
 - mtu statement.....151
 - multicast-statistics statement
 - usage guidelines
 - aggregated SONET.....111
- N**
- neighbor statement.....153
 - network.....198
 - no-keepalives, configuring
 - SONET interfaces196
 - no-loop-timing statement.....145
 - no-payload-scrambler statement.....158
 - no-z0-increment statement.....174
 - notice icons defined.....xvii
- O**
- OC3 interfaces
 - example configuration.....105

OC48 interfaces	
SONET header bytes.....	48, 50
onboard clock.....	219
optical attenuation.....	194
output keepalives, SONET interfaces.....	186
overflow statement.....	154
configuring.....	101
receive bucket.....	154
transmit bucket.....	154
P	
paired-group statement.....	155
parentheses, in syntax descriptions.....	xviii
passive monitoring flow	
SONET/SDH interfaces.....	97
passive-monitor-mode statement.....	156
usage guidelines.....	97
path area, SONET interfaces.....	203
path overhead bytes	203
path-terminating equipment See PTE	
path-trace statement.....	157
payload	
scrambling	
checking	221
configuring	222
SONET interfaces	219
status.....	222
SONET interfaces.....	203
payload-scrambler statement.....	158
physical interfaces	
clock sources.....	124
header byte values.....	48, 50
leaky bucket properties.....	100, 101
SONET defect triggers.....	59, 63
configuration example.....	63
hold timers.....	63
SONET link aggregation.....	107
transitions, damping.....	102
physical link down	
SONET interfaces.....	193
table.....	194
physical link up	
SONET interfaces	193
physical loopback	
SONET interfaces	191
ping interface command	
SONET interfaces	196
Point-to-Point Protocol encapsulation	
on physical interfaces.....	103
pop-all-labels statement.....	159
usage guidelines.....	98
preserve-interface statement.....	160
protect-circuit statement.....	160
PTE.....	202
R	
rate statement.....	161
configuring.....	101
receive-bucket statement.....	161
configuring.....	101
receive-options-packets statement.....	162
usage guidelines.....	97
receive-ttl-exceeded statement.....	162
usage guidelines.....	97
repeaters.....	202
request statement.....	163
required-depth statement.....	164
usage guidelines.....	98
revert-time statement.....	165
rfc-2615 statement.....	165
routers, path-terminating equipment.....	202
S	
sl SONET header byte.....	48, 50
sampling on aggregated links.....	109
example configuration.....	109
SBR	219
SCB	219
SCG	219
scrambling, SONET payload.....	219
SDH APS	
configuration.....	66
SDH APS Load Sharing	
configuration.....	92
overview.....	91
SDH APS Timers	
configuration.....	88
overview.....	87
SDH Basic APS	
configuration.....	68
example.....	69, 92
overview.....	68
SDH Container Interfaces on ATM Encapsulation	
configuration.....	78
displaying.....	78
overview.....	77

SDH Container Interfaces on SONET Links		SDH Switching Mode	
configuration.....	74	configuration.....	87
overview.....	73	overview.....	86
SDH Defect Triggers		SDH Virtual Tributary Mapping	
configuration.....	62	configuration.....	40
overview.....	61	section overhead	
SDH Frame Checksum		bytes.....	202, 203
configuration.....	51	section-terminating equipment See STE	
SDH Framing Mode		set cli terminal command	
configuration.....	39	SONET interfaces	186
overview.....	38	set clocking internal command	
SDH HDLC Payload Scrambling		SONET interfaces	192
configuration.....	57	set encapsulation command	
overview.....	57	SONET interfaces	195
SDH Incrementing STM ID		set fcs 16 command.....	229
configuration.....	41	set fcs 32 command	229
overview.....	41	set loopback local command	
SDH Interface Speed		SONET interfaces.....	191
configuration.....	44	set loopback remote command	
overview.....	42	SONET interfaces	199
SDH interfaces.....	29	set no-keepalives command	
configuration.....	50	SONET interfaces	196
overview.....	29, 48	set payload-scrambler command	222, 229
See also SONET interfaces		set rfc-2615 command	229
SDH Link PIC Redundancy		SFM	219
configuration.....	89	show configuration command	221
overview.....	89	show configuration interfaces command	
SDH Loop Timing		SONET interfaces	221
configuration.....	52	show interfaces command.....	221
SDH Loopback Capability		SONET interfaces.....	182, 187, 192, 221
configuration.....	53	show interfaces extensive command.....	195
SDH Path Trace Identifier		SONET interfaces.....	183, 197, 201, 205
configuration.....	56	show interfaces terse command	
overview.....	56	SONET interfaces.....	181, 187
SDH Physical Interface Properties		signal transmission.....	204
configuration.....	32	Single Board Router See SBR	
overview.....	32	single-mode fiber cable.....	191
SDH Rate Selectability		SONET APS	
configuration.....	47	configuration.....	66
overview.....	45	SONET APS Load Sharing	
SDH Revertive Mode		configuration.....	92
configuration.....	84	overview.....	91
overview.....	84	SONET APS Timers	
SDH RFC2615		configuration.....	88
configuration.....	59	overview.....	87
overview.....	58	SONET Basic APS	
SDH Switching Between Circuits		configuration.....	68
configuration.....	82	example.....	69, 92
overview.....	80	overview.....	68

SONET clock generator	See SCG
SONET Container Interfaces on ATM Encapsulation	
configuration	78
displaying	78
overview	77
SONET Container Interfaces on SONET Links	
configuration	74
overview	73
SONET Defect Triggers	
configuration	62
overview	61
SONET Frame Checksum	
configuration	51
SONET frames	202
line overhead bytes	203
path overhead bytes	203
section overhead bytes	202
SONET Framing Mode	
configuration	39
overview	38
SONET HDLC Payload Scrambling	
configuration	57
overview	57
SONET Incrementing STM ID	
configuration	41
overview	41
SONET Interface Speed	
configuration	44
overview	42
SONET interfaces	29, 229
alarms and errors	
AIS-P alarms	206
displaying	201
LOS alarms	205
path signal label assignments, table	214
PLM-P alarms	213
RDI-L alarms	209
RDI-P alarms	208
REI-L alarms	210
REI-P alarms	209
signal label mismatch	213
alarms and errors checklist	200
APS	29
circuit problems	198
clear interfaces statistics command	194
clocking	
setting	192
damping interface transitions	102
defect triggers	59, 63
configuration example	63
hold timers	63
delete fcs 32 command	228
displaying for specific	182
edit interfaces command	192, 195, 196, 228
edit interfaces sonet-options	
command	191, 199, 222
encapsulation	103
encapsulation, configuring	195
error statistics	197
example configuration	105
frame	202
checksum checklist	223
error control	224
further investigation	182
HDLC payload scrambling	221
header byte values	48, 50
leaky bucket properties	100, 101
line area	203
link aggregation	107
link layer, forcing up	195
logical interface, status	187
loopback	
configuring local	191
creating physical	191
monitor checklist	181
no keepalives	
configuring	196
setting	196
overview	29
path area	203
payload scrambling	
checklist	219
configuring	222
conflicts	220
described	220
levels	220
status	222
physical link down, table	194
ping interface command	196
section area	203
set cli terminal command	186
set clocking internal command	192
set encapsulation command	195
set fcs 16 command	229
set fcs 32 command	229
set loopback local command	191
set loopback remote command	199

-
- set no keepalives command196
 - set payload-scrambler command.....222
 - show configuration interfaces command221
 - show interfaces
 - command.....182, 183, 185, 192, 221
 - show interfaces extensive
 - command.....183, 201, 213
 - show interfaces terse command.....181, 187
 - statistics
 - checking errors.....197
 - monitoring.....185
 - resetting.....194
 - status
 - description table.....182
 - displaying.....181
 - extensive.....183
 - verifying.....193
 - transmitted path trace, checking.....194
 - See also* SDH interfaces
 - SONET Link PIC Redundancy
 - configuration.....89
 - overview.....89
 - SONET Loop Timing
 - configuration.....52
 - SONET Loopback Capability
 - configuration.....53
 - SONET network.....202
 - line area.....203
 - network, figure.....202
 - section area.....202
 - span.....202
 - system hierarchy.....203
 - SONET Path Trace Identifier
 - configuration.....56
 - overview.....56
 - SONET Physical Interface Properties
 - configuration.....32
 - overview.....32
 - SONET Rate Selectability
 - configuration.....47
 - overview.....45
 - SONET Revertive Mode
 - configuration.....84
 - overview.....84
 - SONET RFC 2615
 - configuration.....59
 - overview.....58
 - SONET Switching Between Circuits
 - configuration.....82
 - overview.....80
 - SONET Switching Mode
 - configuration.....87
 - overview.....86
 - SONET Virtual Tributary Mapping
 - configuration.....40
 - sonet-options statement.....166, 191, 222, 228, 229
 - SONET/SDH interfaces
 - passive monitoring.....97
 - span and SONET line.....202
 - span, and SONET line.....203
 - speed statement
 - SONET/SDH.....168
 - SSB219
 - statistics
 - cumulative for SONET interfaces.....186
 - errors
 - SONET interfaces.....197
 - SONET interfaces, resetting.....194
 - status
 - SONET interfaces.....181, 192
 - status description, table
 - SONET interfaces.....182
 - status extensive
 - SONET interfaces183
 - status for specific interface
 - SONET182
 - STE.....202
 - STS
 - path signal label assignments, figure.....214
 - path signal label assignments, table214
 - support, technical *See* technical support
 - switching-mode statement.....169
 - Synchronous Digital Hierarchy *See* SDH interfaces
 - Synchronous Optical Network *See* SONET
 - interfacesxvii
 - syntax conventions.....xvii
 - System and Switch Board *See* SSB
 - system board, location of, table219
 - System Control Board *See* SCB
 - system hierarchy, SONET interfaces.....203
- T**
- t3-options statement.....170
 - technical support
 - contacting JTAC.....xix

threshold statement.....	171
configuring.....	101
transitions	
damping.....	102
transmit-bucket statement.....	171
configuring.....	101
trigger statement.....	172
configuration.....	63

U

upstream or downstream failure, figure	204
upstream, SONET alarms and errors, defining.....	203

V

vtmapping statement.....	173
--------------------------	-----

W

WAN PHY.....	95
wavelength-division multiplexing See WDM	
WDM.....	29
working-circuit statement.....	173

Z

z0-increment statement.....	174
z3 SONET header byte.....	48, 50
z4 SONET header byte.....	48, 50

Index of Statements and Commands

A

advertise-interval statement.....	117
aggregated-sonet-options statement.....	118
annex statement.....	119
aps statement.....	120
annex-b.....	119
atm-options statement.....	121
authentication-key statement.....	122

B

bytes statement.....	123
----------------------	-----

C

clocking statement.....	124
container-devices statement.....	125
device-count.....	125
container-list statement.....	125
container-options statement.....	126
container-type statement.....	126

E

encapsulation statement.....	127
container interface.....	127
logical interfaces.....	128

F

family statement.....	132
fast-aps-switch statement.....	136
fcs statement.....	137
filter statement.....	138
force statement.....	139
framing statement	
SONET and SDH interfaces.....	140

H

hold-time statement.....	141
APS.....	141
SONET/SDH Defect Triggers.....	142

I

ignore statement.....	143
-----------------------	-----

L

lockout statement.....	144
loop-timing statement.....	145
loopback statement	
ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3.....	146

M

member-interface-speed statement.....	147
member-interface-type statement.....	148
minimum-links statement.....	149
mpls statement.....	150
mtu statement.....	151

N

neighbor statement.....	153
no-loop-timing statement.....	145
no-payload-scrambler statement.....	158
no-z0-increment statement.....	174

O

overflow statement.....	154
receive bucket.....	154
transmit bucket.....	154

P

paired-group statement.....	155
passive-monitor-mode statement.....	156
path-trace statement.....	157
payload-scrambler statement.....	158
pop-all-labels statement.....	159
preserve-interface statement.....	160
protect-circuit statement.....	160

R

rate statement.....	161
receive-bucket statement.....	161
receive-options-packets statement.....	162
receive-ttl-exceeded statement.....	162
request statement.....	163
required-depth statement.....	164

revert-time statement.....	165
rfc-2615 statement.....	165

S

sonet-options statement.....	166, 191, 222, 228, 229
speed statement	
SONET/SDH.....	168
switching-mode statement.....	169

T

t3-options statement.....	170
threshold statement.....	171
transmit-bucket statement.....	171
trigger statement.....	172

V

vtmapping statement.....	173
--------------------------	-----

W

working-circuit statement.....	173
--------------------------------	-----

Z

z0-increment statement.....	174
-----------------------------	-----