



Junos[®] OS

SONET/SDH Interfaces Configuration Guide

Release
11.2



Published: 2011-05-20

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 Configuration Guide

Release 11.2

Copyright © 2011, Juniper Networks, Inc.

All rights reserved.

Revision History

May 2011—R1 Junos® OS 11.2

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

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The 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

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Abbreviated Table of Contents

	About This Guide	xvii
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	27
Part 3	SONET/SDH Interface Configuration Statements	
Chapter 3	Summary of SONET/SDH Interfaces Configuration Statements	75
Part 4	Index	
	Index	131
	Index of Statements and Commands	137

Table of Contents

	About This Guide	xvii
	JUNOS Documentation and Release Notes	xvii
	Objectives	xviii
	Audience	xviii
	Supported Routing Platforms	xviii
	Using the Indexes	xix
	Using the Examples in This Manual	xix
	Merging a Full Example	xix
	Merging a Snippet	xx
	Documentation Conventions	xx
	Documentation Feedback	xxii
	Requesting Technical Support	xxii
	Self-Help Online Tools and Resources	xxiii
	Opening a Case with JTAC	xxiii
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	20
Part 2	Configuring SONET/SDH Interfaces	
Chapter 2	Configuring SONET/SDH Interfaces	27
	SONET/SDH Interfaces Overview	27
	Configuring SONET/SDH Physical Interface Properties	28
	Configuring SONET/SDH Framing	30
	Configuring SONET/SDH Interface Speed	31
	Configuring SONET/SDH Rate-Selectability	33
	Configuring SONET/SDH Header Byte Values	34
	Configuring an Incrementing STM ID	35
	Configuring the SONET/SDH Frame Checksum	36
	Configuring Channelized IQ and IQE SONET/SDH Loop Timing	36
	Configuring SONET/SDH Loopback Capability	37
	Example: Configuring SONET/SDH Loopback Capability	38
	Configuring the SONET/SDH Path Trace Identifier	38
	Configuring SONET/SDH HDLC Payload Scrambling	39
	Configuring SONET/SDH RFC 2615 Support	39
	Configuring SONET/SDH Defect Triggers to Be Ignored	40

Configuring SONET/SDH Defect Hold Times	41
Example: Configuring SONET/SDH Defects to Be Ignored	43
Configuring Virtual Tributary Mapping	43
Configuring APS and MSP	44
Configuring Basic APS Support	46
Configuring Container Interfaces	47
Configuring APS Using a Container Interface with ATM Encapsulation	50
Configuring Switching Between the Working and Protect Circuits	52
Configuring Revertive Mode	54
Configuring Unidirectional Switching Mode Support	54
Configuring APS Timers	55
Configuring Link PIC Redundancy	56
Example: Configuring Link PIC Redundancy	56
Configuring APS Load Sharing Between Circuit Pairs	57
Example: Configuring APS Load Sharing Between Circuit Pairs	58
Configuring SONET Options for 10-Gigabit Ethernet Interfaces	58
Configuring the Media MTU on SONET/SDH Interfaces	59
Enabling Passive Monitoring on SONET/SDH Interfaces	59
Removing MPLS Labels from Incoming Packets	60
Configuring the Clock Source on SONET/SDH Interfaces	61
Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces	62
Damping Interface Transitions on SONET/SDH Interfaces	63
Configuring Interface Encapsulation on SONET/SDH Interfaces	64
Configuring the Encapsulation on a Physical SONET/SDH Interface	64
Example: Configuring the Encapsulation on a Physical SONET/SDH Interface	65
Configuring the Encapsulation on a Logical SONET/SDH Interface	66
Example: Configuring SONET/SDH Interfaces	66
Configuring Aggregated SONET/SDH Interfaces	67
Configuring SONET/SDH Link Aggregation	68
Configuring Aggregated SONET/SDH Link Speed	69
Configuring Aggregated SONET/SDH Minimum Links	69
Configuring Filters or Sampling on Aggregated SONET/SDH Links	70
Examples: Configuring Filters or Sampling on Aggregated SONET/SDH Links	70
Example: Configuring Aggregated SONET/SDH Interfaces	71
Configuring Multicast Statistics Collection on Aggregated SONET Interfaces	72

Part 3

Chapter 3

SONET/SDH Interface Configuration Statements

Summary of SONET/SDH Interfaces Configuration Statements	75
advertise-interval	75
aggregate (SONET/SDH)	76
aggregated-sonet-options	76
annex	77
aps	78
atm-options	79

authentication-key	80
bytes	81
clocking	82
container-devices	83
container-list	83
container-options	84
container-type	84
encapsulation	85
encapsulation (Container Interface)	85
encapsulation (Logical Interface)	86
family	89
fcs	93
filter	94
force	95
framing (SONET and SDH Interfaces)	95
hold-time	96
hold-time (APS)	96
hold-time (SONET/SDH Defect Triggers)	97
ignore	98
link-speed (Aggregated SONET/SDH)	99
lockout	99
loop-timing	100
loopback (ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and T1/T3)	101
member-interface-speed	102
member-interface-type	103
minimum-links	104
mpls	105
mtu	106
neighbor	107
overflow	108
overflow (Receive Bucket)	108
overflow (Transmit Bucket)	108
paired-group	109
passive-monitor-mode	109
path-trace	110
payload-scrambler	111
pop-all-labels	112
preserve-interface	113
protect-circuit	113
rate	114
receive-bucket	114
receive-options-packets	115
receive-ttl-exceeded	115
request	116
required-depth	117
revert-time	118
rfc-2615	118
sonet-options	119
speed (SONET/SDH)	121

switching-mode	122
t3-options	123
threshold	124
transmit-bucket	125
trigger	126
vtmapping	127
working-circuit	127
z0-increment	128

Part 4

Index

Index	131
Index of Statements and Commands	137

List of Figures

Part 2	Configuring SONET/SDH Interfaces	
Chapter 2	Configuring SONET/SDH Interfaces	27
	Figure 1: APS/MSP Configuration Topologies	44
	Figure 2: APS Load Sharing Between Circuit Pairs	57

List of Tables

	About This Guide	xvii
	Table 1: Notice Icons	xxi
	Table 2: Text and Syntax Conventions	xxi
Part 2	Configuring SONET/SDH Interfaces	
Chapter 2	Configuring SONET/SDH Interfaces	27
	Table 3: Type 1 PIC Mode Combinations	31
	Table 4: Type 2 PIC Mode Combinations	32
	Table 5: Port Speed Restrictions for SONET/SDH OC3/STM1 (Multi-Rate) MICs	33
	Table 6: SONET/SDH Framing Bytes for Specific Speeds	34
	Table 7: SONET/SDH Default Settings	40
	Table 8: SONET/SDH and ATM Active Alarms and Defects	40

About This Guide

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

- JUNOS Documentation and Release Notes on page xvii
- Objectives on page xviii
- Audience on page xviii
- Supported Routing Platforms on page xviii
- Using the Indexes on page xix
- Using the Examples in This Manual on page xix
- Documentation Conventions on page xx
- Documentation Feedback on page xxii
- Requesting Technical Support on page xxii

JUNOS Documentation and Release Notes

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

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

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

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

Objectives

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



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

Audience

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

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

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

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

Supported Routing Platforms

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

- J Series
- M Series

- MX Series
- T Series

Using the Indexes

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

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

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

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. 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 [Junos OS CLI User Guide](#).

Documentation Conventions

Table 1 on page xxi 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 xxi 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: <code>user@host> configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces 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; interface names; 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.	<code>stub <default-metric metric>;</code>

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

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<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 J-Web selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

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

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

SONET/SDH Interfaces Configuration Statements Overview

- 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 20

[edit chassis] Hierarchy Level

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

```

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

```

[edit interfaces] Hierarchy Level

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



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

```

interfaces {
    traceoptions {
        file filename <files number> <match regular-expression> <size size> <world-readable |
        no-world-readable> ;
    }
}

```

```

    flag flag <disable>;
}
interface-name {
    accounting-profile name;
    aggregated-ether-options {
        (flow-control | no-flow-control);
        lacp {
            (active | passive);
            link-protection {
                disable;
                (revertive | non-revertive);
                periodic interval;
                system-priority priority;
            }
        }
        link-protection;
        link-speed speed;
        (loopback | no-loopback);
        mc-ae {
            chassis-id chassis-id;
            mc-ae-id mc-ae-id;
            mode (active-active | active-standby);
            redundancy-group group-id;
            status-control (active | standby);
        }
        minimum-links number;
        source-address-filter {
            mac-address;
        }
        (source-filtering | no-source-filtering);
    }
    aggregated-sonet-options {
        link-speed speed | mixed;
        minimum-links number;
    }
    atm-options {
        cell-bundle-size cells;
        ilmi;
        linear-red-profiles profile-name {
            high-plp-max-threshold percent;
            low-plp-max-threshold percent;
            queue-depth cells high-plp-threshold percent low-plp-threshold percent;
        }
        mpls {
            pop-all-labels {
                required-depth number;
            }
        }
        pic-type (atm1 | atm2);
        plp-to-clp;
        promiscuous-mode {
            vpi vpi-identifier;
        }
        scheduler-maps map-name {
            forwarding-class class-name {
                epd-threshold cells plp1 cells;
                linear-red-profile profile-name;
            }
        }
    }
}

```

```
        priority (high | low);
        transmit-weight (cells number | percent number);
    }
    vc-cos-mode (alternate | strict);
}
use-null-cw;
vpi vpi-identifier {
    maximum-vcs maximum-vcs;
    oam-liveness {
        down-count cells;
        up-count cells;
    }
    oam-period (seconds | disable);
    shaping {
        (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate
        burst length);
        queue-length number;
    }
}
}
clocking clock-source;
data-input (system | interface interface-name);
dce;
serial-options {
    clock-rate rate;
    clocking-mode (dce | internal | loop);
    control-polarity (negative | positive);
    cts-polarity (negative | positive);
    dcd-polarity (negative | positive);
    dce-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dtr signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
    dsr-polarity (negative | positive);
    dte-options {
        control-signal (assert | de-assert | normal);
        cts (ignore | normal | require);
        dcd (ignore | normal | require);
        dsr (ignore | normal | require);
        dtr signal-handling-option;
        ignore-all;
        indication (ignore | normal | require);
        rts (assert | de-assert | normal);
        tm (ignore | normal | require);
    }
}
dtr-circuit (balanced | unbalanced);
dtr-polarity (negative | positive);
encoding (nrz | nrzi);
indication-polarity (negative | positive);
```

```

line-protocol protocol;
loopback mode;
rts-polarity (negative | positive);
tm-polarity (negative | positive);
transmit-clock invert;
}
description text;
dialer-options {
    pool pool-name <priority priority>;
}
disable;
ds0-options {
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    byte-encoding (nx56 | nx64);
    fcs (16 | 32);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback payload;
    start-end-flag (filler | shared);
}
e1-options {
    bert-error-rate rate;
    bert-period seconds;
    fcs (16 | 32);
    framing (g704 | g704-no-crc4 | unframed);
    idle-cycle-flag (flags | ones);
    invert-data;
    loopback (local | remote);
    start-end-flag (filler | shared);
    timeslots time-slot-range;
}
e3-options {
    atm-encapsulation (direct | plcp);
    bert-algorithm algorithm;
    bert-error-rate rate;
    bert-period seconds;
    framing feet;
    compatibility-mode (digital-link | kentrox | larscom) <subrate value>;
    fcs (16 | 32);
    framing (g.751 | g.832);
    idle-cycle-flag (filler | shared);
    invert-data;
    loopback (local | remote);
    (payload-scrambler | no-payload-scrambler);
    start-end-flag (filler | shared);
    (unframed | no-unframed);
}
encapsulation type;
es-options {
    backup-interface es-fpc/pic/port;
}
fastether-options {
    802.3ad aex;
    (flow-control | no-flow-control);
}

```

```
ignore-l3-incompletes;
ingress-rate-limit rate;
(loopback | no-loopback);
mpls {
  pop-all-labels {
    required-depth number;
  }
}
source-address-filter {
  mac-address;
}
(source-filtering | no-source-filtering);
}
flexible-vlan-tagging;
gigether-options {
  802.3ad aex;
  (asynchronous-notification | no-asynchronous-notification);
  (auto-negotiation | no-auto-negotiation) remote-fault <local-interface-online |
    local-interface-offline>;
  auto-reconnect seconds;
  (flow-control | no-flow-control);
  ignore-l3-incompletes;
  (loopback | no-loopback);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
}
no-auto-mdix;
source-address-filter {
  mac-address;
}
(source-filtering | no-source-filtering);
ethernet-switch-profile {
  (mac-learn-enable | no-mac-learn-enable);
  tag-protocol-id [ tpids ];
  ethernet-policer-profile {
    input-priority-map {
      ieee802.1p premium [ values ];
    }
    output-priority-map {
      classifier {
        premium {
          forwarding-class class-name {
            loss-priority (high | low);
          }
        }
      }
    }
  }
}
policer cos-policer-name {
  aggregate {
    bandwidth-limit bps;
    burst-size-limit bytes;
  }
  premium {
    bandwidth-limit bps;
  }
}
```


9

```
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);  
  minimum-links number;  
  mrru bytes;  
  n391 number;  
  n392 number;  
  n393 number;  
  red-differential-delay milliseconds;  
  t391 seconds;  
  t392 seconds;  
  yellow-differential-delay milliseconds;  
}  
modem-options {  
  dialin (console | routable);  
  init-command-string initialization-command-string;  
}  
mtu bytes;  
multiservice-options {  
  (core-dump | no-core-dump);  
  (syslog | no-syslog);  
}  
native-vlan-id number;  
no-gratuitous-arp-request;  
no-keepalives;  
no-partition {  
  interface-type type;  
}  
otn-options {  
  fec (efec | gfec | none);  
  (laser-enable | no-laser-enable);  
  (line-loopback | no-line-loopback);  
  pass-thru;  
  rate (fixed-stuff-bytes | no-fixed-stuff-bytes | pass-thru);  
  transmit-payload-type number;  
  trigger (oc-lof | oc-lom | oc-los | oc-wavelength-lock | odu-ais | odu-bbe-th | odu-bdi  
    | odu-es-th | odu-lck | odu-oci | odu-sd | odu-ses-th | odu-ttim | odu-uas-th |  
    opu-ptm | otu-ais | otu-bbe-th | otu-bdi | otu-es-th | otu-fec-deg | otu-fec-exe |  
    otu-iae | otu-sd | otu-ses-th | otu-ttim | otu-uas-th);
```

```

    tti;
}
optics-options {
    wavelength nm;
    alarm alarm-name {
        (syslog | link-down);
    }
    warning warning-name {
        (syslog | link-down);
    }
}
partition partition-number oc-slice oc-slice-range interface-type type;
timeslots time-slot-range;
passive-monitor-mode;
per-unit-scheduler;
ppp-options {
    chap {
        access-profile name;
        default-chap-secret name;
        local-name name;
        passive;
    }
    compression {
        acfc;
        pfc;
    }
    dynamic-profile profile-name;
    no-termination-request;
    pap {
        access-profile name;
        local-name name;
        local-password password;
        compression;
    }
}
receive-bucket {
    overflow (discard | tag);
    rate percentage;
    threshold bytes;
}
redundancy-options {
    priority sp-fpc/pic/port;
    secondary sp-fpc/pic/port;
    hot-standby;
}
satop-options {
    payload-size n;
}
schedulers number;
serial-options {
    clock-rate rate;
    clocking-mode (dce | internal | loop);
    control-polarity (negative | positive);
    cts-polarity (negative | positive);
    dcd-polarity (negative | positive);
    dce-options {

```

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

```

sonet-options {
  aggregate asx;
  aps {
    advertise-interval milliseconds;
    annex-b;
    authentication-key key;
    force;
    hold-time milliseconds;
    lockout;
    neighbor address;
    paired-group group-name;
    preserve-interface;
    protect-circuit group-name;
    request;
    revert-time seconds;
    switching-mode (bidirectional | unidirectional);
    working-circuit group-name;
  }
  bytes {
    c2 value;
    e1-quiet value;
    f1 value;
    f2 value;
    s1 value;
    z3 value;
    z4 value;
  }
  fcs (16 | 32);
  loopback (local | remote);
  mpls {
    pop-all-labels {
      required-depth number;
    }
  }
  path-trace trace-string;
  (payload-scrambler | no-payload-scrambler);
  rfc-2615;
  trigger {
    defect ignore;
    hold-time up milliseconds down milliseconds;
  }
  vtmapping (itu-t | klm);
  (z0-increment | no-z0-increment);
}
speed (10m | 100m | 1g | oc3 | oc12 | oc48);
stacked-vlan-tagging;
switch-options {
  switch-port port-number {
    (auto-negotiation | no-auto-negotiation);
    speed (10m | 100m | 1g);
    link-mode (full-duplex | half-duplex);
  }
}
t1-options {
  bert-algorithm algorithm;
  bert-error-rate rate;
}

```

```
bert-period seconds;  
buildout value;  
byte-encoding (nx56 | nx64);  
crc-major-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5);  
crc-minor-alarm-threshold (1e-3 | 5e-4 | 1e-4 | 5e-5 | 1e-5 | 5e-6 | 1e-6);  
fcs (16 | 32);  
framing (esf | sf);  
idle-cycle-flag (flags | ones);  
invert-data;  
line-encoding (ami | b8zs);  
loopback (local | payload | remote);  
remote-loopback-respond;  
start-end-flag (filler | shared);  
timeslots time-slot-range;  
}  
t3-options {  
  atm-encapsulation (direct | plcp);  
  bert-algorithm algorithm;  
  bert-error-rate rate;  
  bert-period seconds;  
  buildout feet;  
  (cbit-parity | no-cbit-parity);  
  compatibility-mode (adtran | digital-link | kentrox | larscom | verilink) <subrate  
    value>;  
  fcs (16 | 32);  
  (feac-loop-respond | no-feac-loop-respond);  
  idle-cycle-flag value;  
  (long-buildout | no-long-buildout);  
  (loop-timing | no-loop-timing);  
  loopback (local | payload | remote);  
  (mac | no-mac);  
  (payload-scrambler | no-payload-scrambler);  
  start-end-flag (filler | shared);  
}  
traceoptions {  
  flag flag <flag-modifier> <disable>;  
}  
transmit-bucket {  
  overflow discard;  
  rate percentage;  
  threshold bytes;  
}  
(traps | no-traps);  
unidirectional;  
vlan-tagging;  
vlan-vci-tagging;  
unit logical-unit-number {  
  accept-source-mac {  
    mac-address mac-address {  
      policer {  
        input cos-policer-name;  
        output cos-policer-name;  
      }  
    }  
  }  
}  
}  
accounting-profile name;
```

```

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;
dial-options {
    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;
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
targeted-broadcast {
  forward-and-send-to-re;
  forward-only;
}
(translate-discard-eligible | no-translate-discard-eligible);
```

```

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

```

[edit logical-systems] Hierarchy Level

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

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

```

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

```

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

```

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

```

```
    }
    vci vpi-identifier.vci-identifier;
  }
  preferred;
  primary;
  (vrrp-group | vrrp-inet6-group) group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-type authentication;
    authentication-key key;
    fast-interval milliseconds;
    (preempt | no-preempt) {
      hold-time seconds;
    }
  }
  priority-number number;
  track {
    priority-cost seconds;
    priority-hold-time interface-name {
      interface priority;
      bandwidth-threshold bits-per-second {
        priority;
      }
    }
  }
  route ip-address/mask routing-instance instance-name priority-cost cost;
}
virtual-address [ addresses ];
}
}
}
```


PART 2

Configuring SONET/SDH Interfaces

- [Configuring SONET/SDH Interfaces on page 27](#)

CHAPTER 2

Configuring SONET/SDH Interfaces

- SONET/SDH Interfaces Overview on page 27
- Configuring SONET/SDH Physical Interface Properties on page 28
- Configuring the Media MTU on SONET/SDH Interfaces on page 59
- Enabling Passive Monitoring on SONET/SDH Interfaces on page 59
- Configuring the Clock Source on SONET/SDH Interfaces on page 61
- Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 62
- Damping Interface Transitions on SONET/SDH Interfaces on page 63
- Configuring Interface Encapsulation on SONET/SDH Interfaces on page 64
- Example: Configuring SONET/SDH Interfaces on page 66
- Configuring Aggregated SONET/SDH Interfaces on page 67
- Configuring Multicast Statistics Collection on Aggregated SONET Interfaces on page 72

SONET/SDH Interfaces Overview

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

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

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

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

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

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

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



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

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

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

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

For information about taking a PIC offline or online, see the `request chassis pic offline` command and the `request chassis pic online` command in the [Junos OS System Basics and Services Command Reference](#).

Configuring SONET/SDH Physical Interface Properties

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

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

```

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

```

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

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

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

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

- Configuring SONET/SDH Framing on page 30
- Configuring SONET/SDH Interface Speed on page 31
- Configuring SONET/SDH Rate-Selectability on page 33
- Configuring SONET/SDH Header Byte Values on page 34
- Configuring an Incrementing STM ID on page 35
- Configuring the SONET/SDH Frame Checksum on page 36
- Configuring Channelized IQ and IQE SONET/SDH Loop Timing on page 36
- Configuring SONET/SDH Loopback Capability on page 37
- Configuring the SONET/SDH Path Trace Identifier on page 38
- Configuring SONET/SDH HDLC Payload Scrambling on page 39
- Configuring SONET/SDH RFC 2615 Support on page 39
- Configuring SONET/SDH Defect Triggers to Be Ignored on page 40
- Configuring SONET/SDH Defect Hold Times on page 41
- Configuring Virtual Tributary Mapping on page 43
- Configuring APS and MSP on page 44
- Configuring SONET Options for 10-Gigabit Ethernet Interfaces on page 58

Configuring SONET/SDH Framing

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

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

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

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



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



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

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

Configuring SONET/SDH Interface Speed

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

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

Table 3: Type 1 PIC Mode Combinations

PIC	Mode	Speed Configuration	Default Mode
2-port OC3	2xOC3 concatenated	<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 32 shows the mode combinations for the next-generation SONET/SDH Type 2 PICs with SFP.

Table 4: Type 2 PIC Mode Combinations

PIC	Mode	Speed Configuration	Default Mode
1-port OC48	1xOC48 concatenated	<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

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

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

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

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

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

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



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

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

Configuring SONET/SDH Rate-Selectability

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

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

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

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



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

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

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

Mode\MIC Name	8-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP	4-port SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP
Rate-selectable Mode	<ul style="list-style-type: none"> Only the first two ports (0–1) can be configured for <code>oc48-stm16</code> speed. All eight ports can be configured for <code>oc3-stm1</code> or <code>oc12-stm4</code> speed. Total available bandwidth is 8.75 Gbps. 	<ul style="list-style-type: none"> Only the first port (0) can be configured for <code>oc48-stm16</code> speed. All four ports can be configured for <code>oc3-stm1</code> or <code>oc12-stm4</code> 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 <code>oc48-stm16</code> speed. Total available bandwidth is 10 Gbps. 	This mode is not available on this MIC.

Configuring SONET/SDH Header Byte Values

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

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

You can configure the following SONET/SDH header bytes:

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

Table 6 on page 34 displays Junos OS framing bytes for several specific speeds.

Table 6: SONET/SDH Framing Bytes for Specific Speeds

Overhead Bytes	STM4	STM16	STM64	OC12	OC48	OC192
A1	F6	F6	F6	F6	F6	F6
A2	28	28	28	28	28	28
C1	—	—	—	1..12	1..48	1..192
H1/H2	6A0A	6A0A	6A0A	620A	620A	620A
Z0	01/CC	01/CC	01/CC	—	—	—
Concatenated mode	93FF	93FF	93FF	93FF	93FF	93FF

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

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

F1—Section user channel byte

F2—Path user channel byte

Z3, Z4—SONET/SDH overhead bytes

E1—quiet default idle byte

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

Z0, F1—Section user channel bytes

K1, K2, S1— Line user channel bytes

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

Configuring an Incrementing STM ID

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

Current SDH standards specify a set of $3*n$ overhead bytes in an STM n that includes the J0 section trace byte. The rest are essentially unused (spare Z0) and contain hexadecimal values (0x01, 0xCC, 0xCC ... 0xCC). The older version of the standard specified that the same set of bytes should contain an incrementing sequence: 1, 2, 3, ..., $3*n$. Their use was

still unspecified although they might have been used to assist in frame alignment. You can configure an incrementing STM ID to enable your Juniper Networks router to interoperate with older equipment that relies on these bytes for frame alignment.

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

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

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

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

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

Configuring the SONET/SDH Frame Checksum

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

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

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

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

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

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

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

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

Configuring Channelized IQ and IQE SONET/SDH Loop Timing

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

```
loop-timing;
```

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

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

You can include these statements at the following hierarchy levels:

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

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

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

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

Configuring SONET/SDH Loopback Capability

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

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

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

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

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

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

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

For example, for DS3 channels on a channelized OC12 interface, the **sonet-options loopback** statement is supported only for channel 0; it is ignored if included in the configuration for channels 1 through 11. The SONET/SDH loopback configured for channel

0 applies to all 12 channels equally. To configure loopbacks on the individual DS3 channels, you must include the **t3-options loopback** statement in the configuration for each channel. This allows each DS3 channel can be put in loopback mode independently.

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

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

Example: Configuring SONET/SDH Loopback Capability

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

```
[edit interfaces]
so-1/0/0 {
  no-keepalives;
  encapsulation cisco-hdlc;
  sonet-options {
    loopback local;
  }
  unit 0 {
    family inet {
      address 10.100.100.1/24;
    }
  }
}
```

Configuring the SONET/SDH Path Trace Identifier

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

By default, the Junos OS uses the router and interface names for the path trace identifier. Depending on the router and interface names, the default path trace identifier might be longer 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.

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

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

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

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

Configuring SONET/SDH HDLC Payload Scrambling

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



NOTE: HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling, because the Junos OS rejects configurations that have both features enabled. For more information, see “Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces” on page 62.

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

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

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

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

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

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

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

Configuring SONET/SDH RFC 2615 Support

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

Table 7 on page 40 shows the older (RFC 1619) and newer (RFC 2615) values, together with the Juniper Networks default values.

Table 7: SONET/SDH Default Settings

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

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

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

Configuring SONET/SDH Defect Triggers to Be Ignored

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

Table 8 on page 40 lists the defects you can configure.

Table 8: SONET/SDH and ATM Active Alarms and Defects

Alarm	Description
Physical	
pll	Phase-locked loop out of lock
lol	Loss of light
Section	
lof	Loss of frame
los	Loss of signal
Line	
ais-l	Alarm indication signal—line
rfl-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

Table 8: SONET/SDH and ATM Active Alarms and Defects (*continued*)

Alarm	Description
locd (ATM only)	Loss of cell delineation
lop-p	Loss of pointer—path
plm-p	Payload label mismatch
rfi-p	Remote failure indication—path
uneq-p	Path unequipped

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

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

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

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

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

Configuring SONET/SDH Defect Hold Times

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

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



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

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

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

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

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

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

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

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

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

- The hold timers on the SONET/SDH defects are applied in addition to any other hold timers you configure on the interface. For example, if an interface is up and you configure a SONET/SDH trigger down hold time of 100 milliseconds and an interface down hold time of 250 milliseconds, when the SONET/SDH defect occurs, the SONET/SDH trigger timer starts. After 100 milliseconds, assuming the defect is still present, the SONET/SDH defect starts the 250 millisecond down timer. After this has expired and again assuming the defect is still outstanding, the interface will be marked down. For more information about interface hold timers, see Damping Interface Transitions.
- Some defects are reported through a periodic poll (once every second). For these defects, there could be up to one second lost before the defect is detected and the hold timer is started. The hold timer expires in precisely the amount of time configured. At that point, the existence of the defect is checked again and the interface is marked up or down accordingly. These defects are as follows:

- lol
- pll
- ber-sf
- ber-sd
- We recommend the following settings:
 - Configure SONET/SDH defect timers on no more than 64 interfaces per FPC.
 - Configure a combined up hold time and down hold time for a SONET/SDH defect to be at least 100 milliseconds.

Example: Configuring SONET/SDH Defects to Be Ignored

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

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

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

Configuring Virtual Tributary Mapping

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

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

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

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

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

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

Configuring APS and MSP

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



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

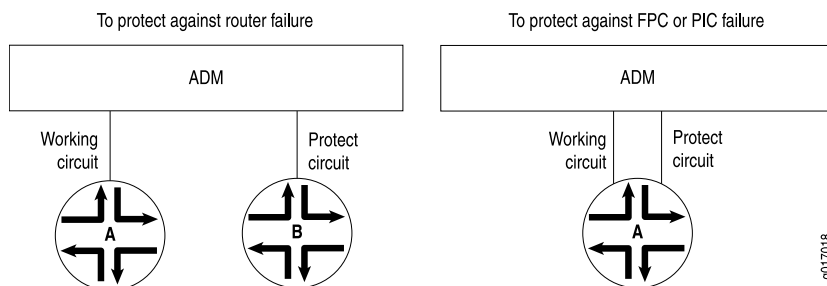
The Junos OS supports APS 1+1 switching, either revertive or nonrevertive mode, and bidirectional mode only (although you can configure interoperation with line-terminating equipment [LTE] provisioned for unidirectional mode). The Junos OS does not transmit identical data on the working and protect circuits,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

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

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

To configure APS or MSP, you configure a working and a protect circuit, as shown in Figure 1 on page 44. To protect against a router failure, you connect two routers to the ADM, configuring one of them as the working router and the second as the protect router. To protect against a PIC or FPC failure, you connect one router to the ADM through both the working and protect circuits, configuring one of the PICs or FPCs as the working circuit and the second as the protect circuit.

Figure 1: APS/MSP Configuration Topologies



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

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

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

This section includes the following topics:

- [Configuring Basic APS Support on page 46](#)
- [Configuring Container Interfaces on page 47](#)
- [Configuring APS Using a Container Interface with ATM Encapsulation on page 50](#)
- [Configuring Switching Between the Working and Protect Circuits on page 52](#)
- [Configuring Revertive Mode on page 54](#)
- [Configuring Unidirectional Switching Mode Support on page 54](#)
- [Configuring APS Timers on page 55](#)
- [Configuring Link PIC Redundancy on page 56](#)
- [Example: Configuring Link PIC Redundancy on page 56](#)
- [Configuring APS Load Sharing Between Circuit Pairs on page 57](#)
- [Example: Configuring APS Load Sharing Between Circuit Pairs on page 58](#)



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

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

For more information and a configuration example, see the [Junos OS VPNs Configuration Guide](#).

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

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

Configuring Basic APS Support

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

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

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

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

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

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

On the Working Circuit	<pre>[edit interfaces so-fpc/pic/port sonet-options] aps { working-circuit group-name; authentication-key key; neighbor address; # Include if protect circuit is on a different router }</pre>
On the Protect Circuit	<pre>aps { protect-circuit group-name; authentication-key key; neighbor address; # Include if working circuit is on a different router }</pre>

Example: Configuring Basic APS Support

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

On Router A (the Working Router)	<pre>[edit interfaces so-6/1/1 sonet-options] aps { working-circuit San-Jose; authentication-key "\$9\$B2612345"; }</pre>
On Router B (the Protect Circuit)	<pre>[edit interfaces so-0/0/0 sonet-options] aps { protect-circuit San-Jose; authentication-key "\$9\$B2612345"; neighbor 192.168.1.2; # Address of Router A on the link between A and B }</pre>
On a Single Platform, One Interface as the Working Circuit and Another Interface as the Protect Circuit	<pre>[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; }</pre>

Configuring Container Interfaces

The Junos OS supports container interfaces for APS on SONETlinks. Physical interfaces and logical interfaces remain up on switchover, and their APS parameters are auto-copied from the container interface to the member links. See Container Interfaces Overview for more information.

Container interfaces support the following features:

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

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

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.

The following configuration steps are required:

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

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

2. Configure the container interface parameters for a specified container **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
```

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

- a. Specify the SONET interfaces and their container options; including the **container-list**, identified by its *cin*.
- b. Specify the **container-type** as **primary** (corresponding to an APS working-circuit) or **standby** (corresponding to an APS protect-circuit).

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

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

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

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

Example Container Interface Configuration

The following is a sample container interface configuration:

```
[edit chassis]
container-devices {
  device-count 1;
}
[edit interfaces]
so-1/0/2 {
  container-options {
    container-list ci0;
```

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

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

```
user@host> show aps
```

Interface	Group	Circuit	Intf state
ci0	CONTAINER_ci0	Container	enabled, up
so-1/2/2	MEMBER_OF_ci0	Working	enabled, up
so-1/2/3	MEMBER_OF_ci0	Protect	disabled, up

Configuring APS Using a Container Interface with ATM Encapsulation

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

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

Configuring APS Using a Container Interface with ATM Encapsulation

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

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

Container ATM APS does not support interchassis APS.

MLPPP over ATM CI is not supported.

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

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

Viewing the APS Container Interface Configuration

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

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

See the [Junos OS Interfaces Command Reference](#).

Configuring Switching Between the Working and Protect Circuits

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

The lockout feature is supported as follows:

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

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

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

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

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

Configuring Revertive Mode

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

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

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

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

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

Configuring Unidirectional Switching Mode Support

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

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

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

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

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

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

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

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

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



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

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

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

Configuring APS Timers

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

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

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

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

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

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

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

Configuring Link PIC Redundancy

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

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

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

```
preserve-interface;
```

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

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

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

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

Example: Configuring Link PIC Redundancy

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

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



```

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

```

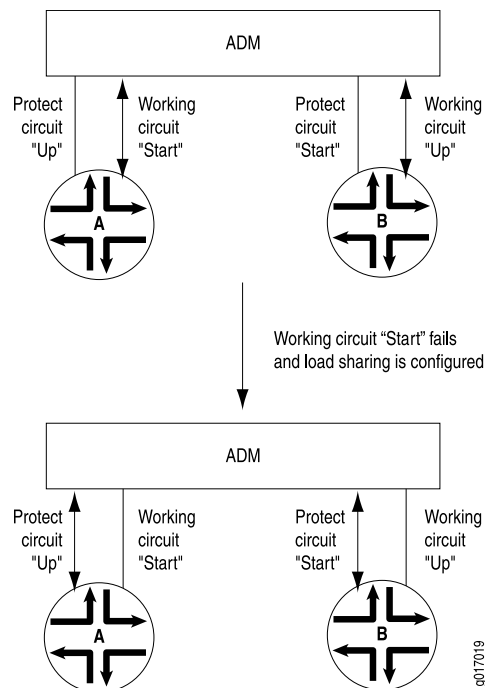
Configuring APS Load Sharing Between Circuit Pairs

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

Figure 2 on page 57 illustrates load sharing between circuits on two routers. Router A has a working circuit "Start" and a protect circuit "Up," and Router B has a working circuit "Up" and a protect circuit "Start." Under normal circumstances, Router A carries the "Start" circuit traffic and Router B carries the "Up" circuit traffic. If the working circuit "Start" were to fail, Router B would end up carrying all the traffic for both the "Start" and "Up" circuits.

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

Figure 2: APS Load Sharing Between Circuit Pairs



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

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

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

Example: Configuring APS Load Sharing Between Circuit Pairs

Configure APS load sharing to match the configuration shown in Figure 2 on page 57:

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

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

Configuring SONET Options for 10-Gigabit Ethernet Interfaces

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

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

```
[edit interfaces]
```

```

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

```

For information about using the **loopback** statement, see “Configuring SONET/SDH Loopback Capability” on page 37. For information about using the **mpls** statement, see “Removing MPLS Labels from Incoming Packets” on page 60. For information about using the **path-trace** statement, see “Configuring the SONET/SDH Path Trace Identifier” on page 38. For information about using the **trigger** statement, see “Configuring SONET/SDH Defect Triggers to Be Ignored” on page 40.

Configuring the Media MTU on SONET/SDH Interfaces

The default media MTU size used on a physical interface depends on the encapsulation being used on that interface. For a listing of MTU sizes for each encapsulation type, see Configuring the Media MTU. For information about configuring the encapsulation on an interface, see “Configuring Interface Encapsulation on SONET/SDH Interfaces” on page 64.

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

```

[edit interfaces interface-name]
mtu bytes;

```

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

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

For more information, see Setting the Protocol MTU.

Enabling Passive Monitoring on SONET/SDH Interfaces

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

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

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

You can include this statement at the following hierarchy levels:

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

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

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

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

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

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

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

Removing MPLS Labels from Incoming Packets

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

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

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

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

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

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

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

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

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

Configuring the Clock Source on SONET/SDH Interfaces

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

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



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

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

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

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

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

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

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

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



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

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

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

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



NOTE: HDLC payload scrambling conflicts with traffic shaping configured using leaky bucket properties. If you configure leaky bucket properties, you must disable payload scrambling, because the Junos OS rejects configurations that have both features enabled. For more information, see “Configuring SONET/SDH HDLC Payload Scrambling” on page 39.

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

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

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

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

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

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

Damping Interface Transitions on SONET/SDH Interfaces

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

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

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

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

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

Configuring Interface Encapsulation on SONET/SDH Interfaces

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

Configuring the Encapsulation on a Physical SONET/SDH Interface

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

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

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



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

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

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

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

For more information about physical interface encapsulation, see [Configuring Interface Encapsulation on Physical Interfaces](#).

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

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

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

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

Configuring the Encapsulation on a Logical SONET/SDH Interface

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

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

You can include this statement at the following hierarchy levels:

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

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

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

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

Example: Configuring SONET/SDH Interfaces

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

```
[edit interfaces]
```

```

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

```

Configuring Aggregated SONET/SDH Interfaces

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

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

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

```

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

```

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



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

To configure aggregated SONET/SDH interfaces, assign a number for the aggregated SONET/SDH interface **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 68. You can optionally specify other physical properties that apply specifically to the aggregated SONET/SDH interfaces; for details, see “Configuring SONET/SDH Physical Interface Properties” on page 28. For a sample configuration, see “Example: Configuring Aggregated SONET/SDH Interfaces” on page 71.

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 68
- Configuring Aggregated SONET/SDH Link Speed on page 69
- Configuring Aggregated SONET/SDH Minimum Links on page 69
- Configuring Filters or Sampling on Aggregated SONET/SDH Links on page 70
- Example: Configuring Aggregated SONET/SDH Interfaces on page 71

Configuring SONET/SDH Link Aggregation

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

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

x is the interface instance number and can be from 0 through 15, for a total of 16 aggregated interfaces. You should not mix SONET and SDH mode on the same aggregated interface. You must also include a statement configuring **asx** at the **[edit interfaces]** hierarchy level. For a sample configuration, see “Example: Configuring Aggregated SONET/SDH Interfaces” on page 71.

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 [Junos OS Routing Policy Configuration Guide](#) and “Examples: Configuring Filters or Sampling on Aggregated SONET/SDH Links” on page 70.

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

Configure filtering on aggregated SONET/SDH interfaces:

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

Defining the Filter

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

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

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

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

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

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

Example: Configuring Aggregated SONET/SDH Interfaces

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

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

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

[edit interfaces]
```

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

Configuring Multicast Statistics Collection on Aggregated SONET Interfaces

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

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

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

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

To configure multicast statistics:

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

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

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

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

Related Documentation

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

PART 3

SONET/SDH Interface Configuration Statements

- Summary of SONET/SDH Interfaces Configuration Statements on page 75

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 55

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 67

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 67

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"> • ATM-over-SHDSL Overview

aps

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

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

Release Information Statement introduced before Junos OS Release 7.4.

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

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

The statements are explained separately.

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

Related Documentation • Configuring APS and MSP on page 44

atm-options

```

Syntax  atm-options {
            cell-bundle-size cells;
            ilmi;
            linear-red-profiles profile-name {
                high-plp-max-threshold percent;
                low-plp-max-threshold percent;
                queue-depth cells high-plp-threshold percent low-plp-threshold percent;
            }
            mpls {
                pop-all-labels {
                    required-depth number;
                }
            }
            pic-type (atm1 | atm2);
            plp-to-clp;
            promiscuous-mode {
                vpi vpi-identifier;
            }
            scheduler-maps map-name {
                forwarding-class class-name {
                    epd-threshold cells plp1 cells;
                    linear-red-profile profile-name;
                    priority (high | low);
                    transmit-weight (cells number | percent number);
                }
                vc-cos-mode (alternate | strict);
            }
            use-null-cw;
            vpi vpi-identifier {
                maximum-vcs maximum-vcs;
                oam-liveness {
                    up-count cells;
                    down-count cells;
                }
                oam-period (disable | seconds);
                shaping {
                    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst
                     length);
                    queue-length number;
                }
            }
        }

```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure ATM-specific physical interface properties.

The statements are explained separately.

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

Related Documentation

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

authentication-key

Syntax authentication-key *key*;

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

Release Information Statement introduced before Junos OS Release 7.4.

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

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

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

Related Documentation

- Configuring Basic APS Support on page 46
- For information about the **authentication-key** statement at the [edit interfaces *interface-name* unit *unit-number* family inet address *address* (vrrp-group | vrrp-inet6-group) *group-number*] or [edit logical-systems *logical-system-name* interfaces *interface-name* unit *unit-number* family (inet | inet6) address *address* (vrrp-group | vrrp-inet6-group) *group-number*] hierarchy level, see the [Junos OS High Availability Configuration Guide](#).

bytes

Syntax	<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 34 no-concatenate

clocking

Syntax	clocking (external [interface <i>interface-name</i>] internal);
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. interface option added in Junos OS Release 8.2.
Description	For interfaces that can use various clock sources, configure the source of the transmit clock on each interface.
Options	<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	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 the Clock Source• Configuring the Clock Source on SONET/SDH Interfaces on page 61• Clock Sources on Channelized Interfaces• Configuring a Channelized T1/E1 Interface to Drop and Insert Time Slots• loop-timing on page 100

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"> Configuring Container Interfaces on page 47

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"> Configuring Container Interfaces on page 47 container-options on page 84

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">Configuring Container Interfaces on page 47

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">Configuring Container Interfaces on page 47

encapsulation

See the following sections:

- [encapsulation \(Container Interface\) on page 85](#)
- [encapsulation \(Logical Interface\) on page 86](#)

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">• Configuring Container Interfaces on page 47

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 frame-relay-ccc frame-relay-ether-type frame-relay-ether-type-tcc frame-relay-ppp frame-relay-tcc multilink-frame-relay-end-to-end multilink-ppp ppp-over-ether ppp-over-ether-over-atm-llc vlan-bridge vlan-ccc vlan-vci-ccc vlan-tcc vlan-vpls);</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>rlsnumber</i> unit <i>logical-unit-number</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	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 ID (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 PPP (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a Link Services or Voice Services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.</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—For ATM2 IQ interfaces only, use PPP over AAL5 LLC encapsulation.</p> <p>atm-ppp-vc-mux—For ATM2 IQ interfaces only, use PPP over ATM AAL5 multiplex encapsulation.</p> <p>atm-snap—Use ATM subnetwork attachment point (SNAP) encapsulation.</p> <p>atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.</p> <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.</p> <p>atm-vc-mux—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the inet family only.</p> <p>ether-over-atm-llc—For interfaces that carry IPv4 traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.</p>

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- | | |
|------------------------------|--|
| Related Documentation | <ul style="list-style-type: none">• Configuring Interface Encapsulation on Logical Interfaces• Circuit and Translational Cross-Connects Overview• Identifying the Access Concentrator• Configuring ATM Interface Encapsulation• Configuring VLAN Encapsulation• Configuring Extended VLAN Encapsulation• Configuring ISDN Logical Interface Properties• Configuring ATM-to-Ethernet Interworking• Junos OS Services Interfaces Configuration Guide |
|------------------------------|--|

family

```

Syntax  family family {
        accounting {
            destination-class-usage;
            source-class-usage {
                (input | output | input output);
            }
        }
        access-concentrator name;
        address address {
            ... the address subhierarchy appears after the main [edit interfaces interface-name unit
                logical-unit-number family family-name] hierarchy ...
        }
        bridge-domain-type (bvlan | svlan);
        bundle interface-name;
        core-facing;
        demux-destination {
            destination-prefix;
        }
        demux-source {
            source-prefix;
        }
        duplicate-protection;
        dynamic-profile profile-name;
        filter {
            group filter-group-number;
            input filter-name;
            input-list [ filter-names ];
            output filter-name;
            output-list [ filter-names ];
        }
        interface-mode (access | trunk);
        ipsec-sa sa-name;
        isid-list all-service-groups;
        keep-address-and-control;
        mac-validate (loose | strict);
        max-sessions number;
        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
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-beqn | no-translate-fecn-and-beqn);
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    master-only;
    multipoint-destination address dlci dlci-identifier;
    multipoint-destination address {
        epd-threshold cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period (disable | seconds);
        shaping {
            (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
            sustained rate);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
}
preferred;
primary;
(vrrp-group | vrrp-inet6-group) group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-type authentication;
    authentication-key key;
    fast-interval milliseconds;
    (preempt | no-preempt) {
        hold-time seconds;
    }
}

```

```

priority number;
track {
    interface interface-name {
        bandwidth-threshold bits-per-second priority-cost number;
    }
    priority-hold-time seconds;
    route ip-address/prefix-length routing-instance instance-name priority-cost cost;
}
virtual-address [ addresses ];
virtual-link-local-address ipv6-address;
vrrp-inherit-from {
    active-interface interface-name;
    active-group group-number;
}
}
}

```

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure protocol family information for the logical interface.



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

Options *family*—Protocol family:

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


The remaining statements are explained separately.

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

Related Documentation

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

fcs

Syntax	fcs (16 32);
Hierarchy Level	[edit interfaces e1- <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.
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"> Configuring the E1 Frame Checksum Configuring the E3 Frame Checksum Configuring the SONET/SDH Frame Checksum on page 36 Configuring the T1 Frame Checksum Configuring the T3 Frame Checksum

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. The default filter group number is 0.</p> <p>Range: 0 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	<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">• Applying a Filter to an Interface• Configuring Firewall Filters (CLI Procedure)• Configuring Gigabit Ethernet Interfaces (CLI Procedure)• Example: Configuring Firewall Filters for Port, VLAN, and Router Traffic on EX Series Switches• Junos OS Services Interfaces Configuration Guide• Junos OS Routing Policy Configuration Guide• Junos OS System Basics Configuration Guide

force

Syntax	<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	<p>protect—Request the circuit to become the protect circuit.</p> <p>working—Request the circuit to become the working circuit.</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 Switching Between the Working and Protect Circuits on page 52 request on page 116

framing (SONET and SDH Interfaces)

Syntax	<code>framing (sdh sonet);</code>
Hierarchy Level	[edit interfaces <i>so-fpc/pic/port</i>]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	For the 4-port OC48 PIC with SFP installed and the 4-port OC192 PIC in T Series and M Series routers, configure SONET or SDH framing on a per-port basis. This functionality allows you to mix SONET and SDH modes on interfaces on the same PIC.
Options	<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 on page 30

hold-time

See the following sections:

- **hold-time (APS) on page 96**
- **hold-time (SONET/SDH Defect Triggers) on page 97**




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

hold-time (APS)

Syntax	hold-time <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 55• advertise-interval on page 75

hold-time (SONET/SDH Defect Triggers)

Syntax	<code>hold-time up <i>milliseconds</i> down <i>milliseconds</i>;</code>
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.
	<div>  <p>NOTE: On M Series and T Series platforms with Channelized SONET IQ PICs and Channelized SONET IQE PICs, the SONET defect alarm trigger hold-time statement is not supported.</p> </div>
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	<p>down <i>milliseconds</i>—Hold time to wait before the interface is marked down.</p> <p>Range: 1 through 65,534 milliseconds</p> <p>Default: No hold time</p> <p>up <i>milliseconds</i>—Hold time to wait before the interface is marked up.</p> <p>Range: 1 through 65,534 milliseconds</p> <p>Default: No hold time</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 Defect Hold Times on page 41

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 to Be Ignored on page 40hold-time (Physical Interface)

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"> • Configuring Aggregated Ethernet Link Speed • Configuring Aggregated SONET/SDH Link Speed on page 69

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 52

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.



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

Options	loop-timing —Configure loop timing (external) clocking. no-loop-timing —Configure line timing (internal) clocking. Default: no-loop-timing
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Channelized IQ and IQE SONET/SDH Loop Timing on page 36• Configuring the Channelized T3 Loop Timing• clocking on page 82

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

Syntax	loopback (local payload remote);
Hierarchy Level	[edit interfaces <i>ce1-fpc/pic/port</i>], [edit interfaces <i>ct1-fpc/pic/port</i>], [edit interfaces <i>t1-fpc/pic/port</i>], [edit interfaces <i>interface-name</i> ds0-options], [edit interfaces <i>interface-name</i> dsl-options], [edit interfaces <i>interface-name</i> e1-options], [edit interfaces <i>interface-name</i> e3-options], [edit interfaces <i>interface-name</i> shdsl-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.
Description	Configure a loopback connection. To turn off the loopback capability, remove the loopback statement from the configuration.



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

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

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

Options	<p>local—Loop packets, including both data and timing information, back on the local router's PIC. NxDS0 IQ interfaces do not support local loopback.</p> <p>payload—For channelized T3, T1, and NxDS0 IQ interfaces only, loop back data only (without clocking information) on the remote router's PIC. With payload loopback, overhead is recalculated. Neither ATM-over-asymmetrical digital subscriber line (ADSL) interfaces nor ATM-over-SHDSL interfaces support payload loopback.</p> <p>remote—Loop packets, including both data and timing information, back on the remote router's interface card. NxDS0 IQ interfaces do not support remote loopback.</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**
- Configuring E3 and T3 Parameters on ATM Interfaces
 - Configuring E1 Loopback Capability
 - Configuring E3 Loopback Capability
 - Configuring Channelized IQ and IQE SONET/SDH Loop Timing on page 36
 - Configuring SHDSL Operating Mode on an ATM Physical Interface
 - Configuring T1 Loopback Capability
 - Configuring T3 Loopback Capability
 - feac-loop-respond

member-interface-speed

- Syntax** `member-interface-speed speed;`
- Hierarchy Level** [edit interfaces container-options **member-interface-type**]
- Release Information** Statement introduced in Junos OS Release 9.2.
- Description** Specify container-interface member-interface speed options.
- Options** *speed*—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.
- Required Privilege Level** interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.
- Related Documentation**
- Configuring Container Interfaces on page 47
 - **container-options on page 84**

member-interface-type

Syntax	<pre>member-interface-type sonet { member-interface-speed [<i>speed</i>]; }</pre>
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	<p>sonet—Protocol type of the container interface, specify sonet.</p> <p>speed—Set interface speed to OC3, OC12, OC48, OC192, OC768, or mixed.</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 Container Interfaces on page 47• container-options on page 84



minimum-links

Syntax	<code>minimum-links <i>number</i>;</code>
Hierarchy Level	[edit interfaces <i>aex</i> aggregated-ether-options], [edit interfaces <i>aex</i> 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>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For aggregated Ethernet, SONET/SDH, multilink, link services, and voice services interfaces only, set the minimum number of links that must be up for the bundle to be labeled up.
Options	<i>number</i> —Number of links. Range: 1 through 8 (1 through 16 for Ethernet and SONET interfaces on the MX Series, M320, M120, T Series, or TX Matrix routers, and 1 through 12 for EX8200 switches) Default: 1
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Aggregated Ethernet Minimum Links• Configuring Aggregated SONET/SDH Minimum Links on page 69• Configuring Aggregated Ethernet Interfaces (CLI Procedure)• Example: Configuring Aggregated Ethernet High-Speed Uplinks Between an EX4200 Virtual Chassis Access Switch and an EX4200 Virtual Chassis Distribution Switch• Junos OS Services Interfaces Configuration Guide

mpls

Syntax	<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"> Removing MPLS Labels from Incoming Packets Removing MPLS Labels from Incoming Packets on page 60 Junos OS Services Interfaces Configuration Guide

mtu

Syntax	<code>mtu bytes;</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i>],</code> <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>],</code> <code>[edit interfaces interface-range <i>name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]</code>
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>
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>On EX Series switches, keep the following points in mind if you are configuring MTU size for jumbo frames on these special types of interfaces:</p> <ul style="list-style-type: none"> • For LAG interfaces—Configuring the jumbo MTU size on a link aggregation group (LAG) interface (aex) automatically configures the jumbo MTU size on the member links. • For RVIs—Jumbo frames of up to 9216 bytes are supported on the routed VLAN interface (RVI), which is named vlan. The RVI functions as a logical router. To route jumbo data packets on the RVI, you must configure the jumbo MTU size on the member physical interfaces of the RVI and not on the RVI itself (the vlan interface). However, for jumbo control packets—for example, to ping the RVI with a packet size of 6000 bytes or more—you must explicitly configure the jumbo MTU size on the interface named vlan (the RVI).
	<div>  <p>CAUTION: For EX Series switches, setting or deleting the jumbo MTU size on the RVI (the vlan interface) while the switch is transmitting packets might result in dropped packets.</p> </div>
	<div>  <p>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 (fxp0, or em0, or me0) interfaces or for loopback, multilink, and multicast tunnel devices.</p> </div>
Options	<p>bytes—MTU size.</p> <p>Range: 256 through 9192 bytes</p>

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

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

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

Related Documentation

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

neighbor

Syntax neighbor *address*;

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

Release Information Statement introduced before Junos OS Release 7.4.

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

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

Options *address*—Neighbor's address.

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

Related Documentation

- Configuring Basic APS Support on page 46

overflow

See the following sections:

- **overflow (Receive Bucket)** on page 108
- **overflow (Transmit Bucket)** on page 108

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• Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 62

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• Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 62

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 Between Circuit Pairs on page 57 working-circuit on page 127


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>For ATM, Ethernet, and SONET/SDH interfaces only, monitor packet flows from another router. If you include this statement in the configuration, the interface does not send keepalives or alarms, and does not participate actively on the network.</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"> Enabling Passive Monitoring on ATM Interfaces Passive Monitoring on Ethernet Interfaces Overview Enabling Passive Monitoring on SONET/SDH Interfaces on page 59 multiservice-options Junos OS Services Interfaces Configuration Guide

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 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.</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 38sonet-options on page 119

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>  <p>NOTE: The payload-scrambler statement at the [edit interfaces <i>interface-name</i> e3-options] hierarchy level is not valid for IQE PICs.</p> </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"> Configuring E3 and T3 Parameters on ATM Interfaces Configuring E3 HDLC Payload Scrambling Configuring SONET/SDH HDLC Payload Scrambling on page 39 Configuring T3 HDLC Payload Scrambling Examples: Configuring T3 Interfaces compatibility-mode

pop-all-labels

Syntax	<pre>pop-all-labels { required-depth <i>number</i>; }</pre>
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> gigether-options mpls]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>For passive monitoring on ATM and SONET/SDH interfaces only, removes up to two MPLS labels from incoming IP packets.</p> <p>This statement has no effect on IP packets with more than two MPLS labels. Packets with MPLS labels cannot be processed by the Monitoring Services PIC; if packets with MPLS labels are forwarded to the Monitoring Services PIC, they are discarded.</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">• Removing MPLS Labels from Incoming Packets• Removing MPLS Labels from Incoming Packets on page 60• Junos OS Services Interfaces Configuration Guide

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	<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 Link PIC Redundancy on page 56 • Junos OS Services Interfaces Configuration Guide

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	<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 Basic APS Support on page 46 • working-circuit on page 127

rate

Syntax	<code>rate percentage;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> receive-bucket], [edit interfaces <i>interface-name</i> transmit-bucket]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify percentage of the interface line rate that is available to receive or transmit packets.
Options	percentage —Percentage of the interface line rate that is available to receive or transmit packets. Range: 0 through 100
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Receive and Transmit Leaky Bucket PropertiesConfiguring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 62

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 SONET/SDH Interfaces on page 62transmit-bucket on page 125

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 59

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 59

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 52force on page 95

required-depth

Syntax	<code>required-depth <i>number</i>;</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i> atm-options mpls pop-all-labels],</code> <code>[edit interfaces <i>interface-name</i> sonet-options mpls pop-all-labels],</code> <code>[edit interfaces <i>interface-name</i> fastether-options mpls pop-all-labels],</code> <code>[edit interfaces <i>interface-name</i> gigether-options mpls pop-all-labels]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
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><i>number</i>—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	<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"> Removing MPLS Labels from Incoming Packets Removing MPLS Labels from Incoming Packets on page 60 Junos OS Services Interfaces Configuration Guide

revert-time

Syntax	<code>revert-time <i>seconds</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 APS revertive mode.
Default	APS operates in nonrevertive mode.
Options	<i>seconds</i> —Amount of time to wait after the working circuit has again become functional before making the working circuit active again. Range: 1 through 65,535 seconds Default: None (APS operates in nonrevertive mode)
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">Configuring Revertive Mode on page 54

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	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 RFC 2615 Support on page 39

sonet-options

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

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure SONET/SDH-specific interface properties.

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

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

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

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

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

The statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
Related Documentation	• Configuring SONET/SDH Parameters on ATM Interfaces
	• Channelized OC12/STM4 IQ and IQE Interfaces Overview
	• Channelized STM1 Interfaces Overview
	• Configuring SONET/SDH Physical Interface Properties on page 28
	• no-concatenate

speed (SONET/SDH)

Syntax	<code>speed (oc3 oc12 oc48);</code>
Hierarchy Level	<code>[edit interfaces so-<i>fpc/pic/port</i>],</code> <code>[edit interfaces so-<i>fpc/pic/port:channel</i>]</code>
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	<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 Interface Speed on page 31

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 Unidirectional Switching Mode Support on page 54

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 <i>bytes</i>;</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>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.</p>
Options	<p><i>bytes</i>—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 <i>k</i> (1000). For example, the entry <code>threshold 2k</code> 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• Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 62

transmit-bucket

Syntax	<pre>transmit-bucket { overflow discard; rate <i>percentage</i>; threshold <i>bytes</i>; }</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 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	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• Configuring Receive and Transmit Leaky Bucket Properties on SONET/SDH Interfaces on page 62• receive-bucket on page 114

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 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 to Be Ignored on page 40

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"> Configuring Virtual Tributary Mapping of Channelized STM1 Interfaces Junos OS System Basics Configuration Guide

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 APS Support on page 46 protect-circuit on page 113

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 35 sonet-options on page 119

PART 4

Index

- Index on page 131
- Index of Statements and Commands on page 137

Index

Symbols

#, comments in configuration statements.....	xxii
(), in syntax descriptions.....	xxii
10-Gigabit Ethernet interfaces	
SONET.....	58
< >, in syntax descriptions.....	xxi
[], in configuration statements.....	xxii
{ }, in configuration statements.....	xxii
(pipe), in syntax descriptions.....	xxii

A

advertise-interval statement.....	75
APS	
usage guidelines.....	55
advertisement intervals	
APS interfaces.....	55
aggregate statement	
usage guidelines.....	68
aggregated SONET interfaces.....	68
configuring.....	67
example configuration.....	71
firewall filters.....	70
example configuration.....	70
link speed.....	69
minimum links.....	69
multicast statistics.....	72
aggregated-sonet-options statement.....	76
usage guidelines.....	67
alarm triggers, SONET interfaces	
hold timers.....	41
annex statement.....	77
APS	
basic support.....	46
circuit pairs.....	46
circuits, switching between.....	52
configuration example.....	47
link PIC redundancy	
example configuration.....	56
link state replication.....	56
load sharing.....	57

load sharing between circuits	
example configuration.....	58
overview.....	44
revertive mode.....	54
timers.....	55
unidirectional mode.....	54
aps statement.....	78
annex-b.....	77
usage guidelines.....	46
atm-options statement.....	79
authentication-key statement.....	80
APS.....	46
usage guidelines.....	46
Automatic Protection Switching See APS	

B

braces, in configuration statements.....	xxii
brackets	
angle, in syntax descriptions.....	xxi
square, in configuration statements.....	xxii
bytes statement.....	81
usage guidelines.....	34

C

c2 SONET header byte.....	34
channelized OC48 interfaces	
SONET header bytes.....	34
channelized T3 interfaces	
loop timing.....	36
checksums See frame checksums	
circuit pairs, APS.....	46
clock sources.....	61, 82
clocking statement.....	82
usage guidelines.....	61
comments, in configuration statements.....	xxii
container interfaces	
ATM encapsulation.....	50
configuration example.....	47
container-devices statement.....	83
device-count.....	83
container-list statement.....	83

container-options statement.....	84
container-type statement.....	84
conventions	
text and syntax.....	xxi
curly braces, in configuration statements.....	xxii
customer support.....	xxii
contacting JTAC.....	xxii

D

damping	
interface transitions.....	63
defect triggers, SONET interfaces.....	40
configuration example.....	43
hold timers.....	41
dense wavelength-division multiplexing See DWDM	
documentation	
comments on.....	xxii
DWDM.....	27

E

encapsulation	
example configuration.....	65
media MTU size and.....	59
on logical interfaces.....	66
on physical interfaces.....	64
encapsulation statement.....	85
container interface.....	85
logical interface.....	86
logical interfaces	
usage guidelines.....	66
physical interfaces	
usage guidelines.....	64
external clock sources.....	61, 82

F

f1 SONET header byte.....	34
f2 SONET header byte.....	34
family statement.....	89
fcs statement.....	93
SONET interfaces	
usage guidelines.....	36
filter statement.....	94
filters.....	70
on aggregated links.....	70
example configuration.....	70
See also firewall filters	
font conventions.....	xxi
force statement.....	95

frame checksums	
SONET interfaces.....	36
Frame Relay encapsulation	
logical interfaces.....	66
physical interfaces.....	64
Frame Relay Ether Type encapsulation	
physical interfaces.....	64
framing statement	
SONET and SDH interfaces.....	95
usage guidelines.....	30

H

HDLC payload scrambling	
SONET interfaces.....	39
header byte values.....	34
hold-time statement.....	96
APS.....	96
usage guidelines.....	55
damping interface transitions	
usage guidelines.....	63
SONET defect triggers	
usage guidelines.....	41
SONET/SDH Defect Triggers.....	97

I

icons defined, notice.....	xx
ignore statement.....	98
incrementing STM ID.....	35
interface preservation.....	56
interface transitions	
damping.....	63
interfaces	
aggregated SONET.....	67
clock sources.....	82
configuration statements.....	4, 75
overview.....	27
internal clock sources.....	61, 82

L

LAN PHY.....	58
leaky bucket properties.....	62
link aggregation	
SONET interfaces.....	68
link speed	
SONET aggregation.....	69
link state replication	
APS.....	56
link-speed statement	
usage guidelines.....	69

load sharing	
APS.....	57
lockout statement.....	99
usage guidelines.....	52
logical systems	
configuration statements.....	20
loop timing	
channelized T3 interfaces.....	36
loop-timing statement.....	100
usage guidelines.....	36
loopback capability.....	37
SONET interfaces	
example configuration.....	38
loopback statement	
10-Gigabit Ethernet interfaces	
usage guidelines.....	58
ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and	
T1/T3.....	101
SONET interfaces	
usage guidelines.....	37

M

manuals	
comments on.....	xxii
media MTUs	
SONET interfaces.....	59
member-interface-speed statement.....	102
member-interface-type statement.....	103
minimum links for aggregation	
SONET links.....	69
minimum-links statement.....	104
usage guidelines.....	69
mpls statement.....	105
10-Gigabit Ethernet interfaces	
usage guidelines.....	58
SONET/SDH interfaces	
usage guidelines.....	60
MSP.....	44
mtu statement.....	106
SONET interfaces	
usage guidelines.....	59
MTUs	
media MTUs.....	59
physical interfaces.....	59
SONET interfaces.....	59
multicast-statistics statement	
usage guidelines	
aggregated SONET.....	72
multiplex section protection See MSP	

N

neighbor statement.....	107
usage guidelines.....	46
no-loop-timing statement.....	100
usage guidelines.....	36
no-payload-scrambler statement.....	111
SONET interfaces	
usage guidelines.....	39
no-z0-increment statement.....	128
usage guidelines.....	35
notice icons defined.....	xx

O

OC3 interfaces	
example configuration.....	66
OC48 interfaces	
SONET header bytes.....	34
OC48 PIC	
framing.....	30
overflow statement.....	108
receive bucket.....	108
transmit bucket.....	108
usage guidelines.....	62

P

paired-group statement.....	109
usage guidelines.....	57
parentheses, in syntax descriptions.....	xxii
passive monitoring flow	
SONET/SDH interfaces.....	59
passive-monitor-mode statement.....	109
usage guidelines.....	59
path trace identifier.....	38
path-trace statement.....	110
10-Gigabit Ethernet interfaces	
usage guidelines.....	58
usage guidelines.....	38
payload-scrambler statement.....	111
SONET interfaces	
usage guidelines.....	39
physical interfaces	
APS.....	44
clock sources.....	61, 82
frame checksums See frame checksums	
HDLC payload scrambling.....	39
header byte values.....	34
leaky bucket properties.....	62
loop timing.....	36

loopback capability	
SONET interfaces.....	37
media MTU size.....	59
MSP.....	44
path trace identifier.....	38
revertive mode, APS.....	54
RFC 2615 support.....	39
SONET defect triggers.....	40
configuration example.....	43
hold timers.....	41
SONET link aggregation.....	68
speed.....	31
unidirectional mode, APS.....	54
Point-to-Point Protocol encapsulation	
on physical interfaces.....	64
pop-all-labels statement.....	112
usage guidelines.....	60
preserve interfaces statement	
usage guidelines.....	56
preserve-interface statement.....	113
protect circuit, APS	
configuring.....	46
load sharing between paired groups.....	57
paired groups, switching between.....	52
protect-circuit statement.....	113
usage guidelines.....	46
R	
rate statement.....	114
usage guidelines.....	62
receive-bucket statement.....	114
usage guidelines.....	62
receive-options-packets statement.....	115
usage guidelines.....	59
receive-ttl-exceeded statement.....	115
usage guidelines.....	59
request statement.....	116
required-depth statement.....	117
usage guidelines.....	60
revert-time statement.....	118
usage guidelines.....	54
revertive mode, APS.....	54
RFC 2615 support, SONET interfaces.....	39
rfc-2615 statement.....	118
usage guidelines.....	39
S	
s1 SONET header byte.....	34

sampling on aggregated links.....	70
example configuration.....	70
SDH interfaces.....	27
configuration statements.....	28
framing.....	30
overview.....	27
physical properties.....	28
<i>See also</i> SONET interfaces	
SONET interfaces.....	27
APS.....	27
clock sources.....	61
configuration statements.....	28
damping interface transitions.....	63
defect triggers.....	40
configuration example.....	43
hold timers.....	41
encapsulation.....	64
example configuration.....	66
frame checksum.....	36
framing.....	30
HDLC payload scrambling.....	39
header byte values.....	34
incrementing STM ID.....	35
leaky bucket properties.....	62
link aggregation.....	68
loopback capability.....	37
MTU sizes.....	59
overview.....	27
path trace identifier.....	38
physical interface properties.....	28
RFC 2615 support.....	39
<i>See also</i> SDH interfaces	
sonet-options statement.....	119
usage guidelines.....	28
SONET/SDH interfaces	
interface speed.....	31
passive monitoring.....	59
port speed.....	33
speed statement	
SONET/SDH.....	121
usage guidelines.....	31
support, technical <i>See</i> technical support	
switching-mode statement.....	122
usage guidelines.....	54
Synchronous Digital Hierarchy <i>See</i> SDH interfaces	
Synchronous Optical Network <i>See</i> SONET	
interfaces	
syntax conventions.....	xxi

T

t3-options statement.....	123
technical support	
contacting JTAC.....	xxii
threshold statement.....	124
usage guidelines.....	62
timers	
APS.....	55
transitions, damping.....	63
transmit clock sources.....	61
transmit-bucket statement.....	125
usage guidelines.....	62
trigger statement.....	126
10-Gigabit Ethernet interfaces	
usage guidelines.....	58
usage guidelines.....	40

U

unidirectional mode, APS.....	54
-------------------------------	----

V

vtmapping statement.....	127
--------------------------	-----

W

WAN PHY.....	58
wavelength-division multiplexing <i>See</i> WDM	
WDM.....	27
working circuit, APS	
configuring.....	46
load sharing between paired groups.....	57
paired groups, switching between.....	52
working-circuit statement.....	127
usage guidelines.....	46

Z

z0-increment statement.....	128
usage guidelines.....	35
z3 SONET header byte.....	34
z4 SONET header byte.....	34

Index of Statements and Commands

A

advertise-interval statement.....	75
aggregated-sonet-options statement.....	76
annex statement.....	77
aps statement.....	78
annex-b.....	77
atm-options statement.....	79
authentication-key statement.....	80

B

bytes statement.....	81
----------------------	----

C

clocking statement.....	82
container-devices statement.....	83
device-count.....	83
container-list statement.....	83
container-options statement.....	84
container-type statement.....	84

E

encapsulation statement.....	85
container interface.....	85
logical interface.....	86

F

family statement.....	89
fcs statement.....	93
filter statement.....	94
force statement.....	95
framing statement	
SONET and SDH interfaces.....	95

H

hold-time statement.....	96
APS.....	96
SONET/SDH Defect Triggers.....	97

I

ignore statement.....	98
-----------------------	----

L

lockout statement.....	99
loop-timing statement.....	100
loopback statement	
ADSL, DS0, E1/E3, SONET/SDH, SHDSL, and	
T1/T3.....	101

M

member-interface-speed statement.....	102
member-interface-type statement.....	103
minimum-links statement.....	104
mpls statement.....	105
mtu statement.....	106

N

neighbor statement.....	107
no-loop-timing statement.....	100
no-payload-scrambler statement.....	111
no-z0-increment statement.....	128

O

overflow statement.....	108
receive bucket.....	108
transmit bucket.....	108

P

paired-group statement.....	109
passive-monitor-mode statement.....	109
path-trace statement.....	110
payload-scrambler statement.....	111
pop-all-labels statement.....	112
preserve-interface statement.....	113
protect-circuit statement.....	113

R

rate statement.....	114
receive-bucket statement.....	114
receive-options-packets statement.....	115
receive-ttl-exceeded statement.....	115
request statement.....	116

required-depth statement.....	117
revert-time statement.....	118
rfc-2615 statement.....	118

S

sonet-options statement.....	119
speed statement	
SONET/SDH.....	121
switching-mode statement.....	122

T

t3-options statement.....	123
threshold statement.....	124
transmit-bucket statement.....	125
trigger statement.....	126

V

vtmapping statement.....	127
--------------------------	-----

W

working-circuit statement.....	127
--------------------------------	-----

Z

z0-increment statement.....	128
-----------------------------	-----