JUNOSe™ Software
for E-series™ Routing Platforms

Physical Layer Configuration Guide

Release 9.0.x

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

Part Number: 162-01842-00, Revision A00

JUNOSe™ Software for E-series™ Routing Platforms Physical Layer Configuration Guide, Release 9.0.x
Writing: John Borelli, Sarah Lesway-Ball, Brian Wesley Simmons, Fran Singer
Editing: Ben Mann, Fran Mues
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
29 February 2008—Revision 1

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

Software License

The terms and conditions for using this software are described in the software license contained in the acknowledgment to your purchase order or, to the extent applicable, to any reseller agreement or end-user purchase agreement executed between you and Juniper Networks. By using this software, you indicate that you understand and agree to be bound by those terms and conditions.

Generally speaking, the software license restricts the manner in which you are permitted to use the software and may contain prohibitions against certain uses. The software license may state conditions under which the license is automatically terminated. You should consult the license for further details.

For complete product documentation, please see the Juniper Networks Web site at www.juniper.net/techpubs.

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 Juniper Networks, Inc. and its subsidiaries (collectively "Juniper"), and 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, and updates and releases of such software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller. "Embedded Software" means Software which Juniper has embedded in the Juniper 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 the 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 software on multiple computers requires multiple licenses, regardless of whether such computers 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 the Embedded Software on non-Juniper equipment; (j) use the 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 for the Software are exclusive of taxes, withholdings, duties, or levies (collectively "Taxes"). Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software.

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 présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

About This Guide xi

Objectives xi
Audience xi
E-series Routers xii
Documentation Conventions xii
Related E-series and JUNOSe Documentation xiv
    E-series and JUNOSe Documents xiv
    JUNOSe Configuration Guides xvii
Obtaining Documentation xvii
Documentation Feedback xviii
Requesting Technical Support xviii

Chapter 1 Configuring Channelized T3 Interfaces 1

Overview 1
    MDL/FDL Support 1
        MDL Standards 2
        FDL Standards 2
        Timeout of Received MDL and FDL Messages 2
        Frequency of FDL Path Messages 3
    Higher-Level Protocols 3
Platform Considerations 4
    CT3/T3-F0 Line Modules and CT3/T3 12 I/O Modules 4
    Exchanging Modules 5
    Interface Stack 5
    Numbering Scheme 5
        T3 Controllers 5
        T1 Channels 6
        Fractional T1 6
        HDLC Channels 7
References 7
Before You Configure an Interface 8
Configuration Tasks 8
    Configuring a T3 Controller 8
        Configuring MDL Messages 9
        Other Optional Tasks 10
    Configuring T1 Channels 12
        Optional Tasks 12
        Configuring FDL Messages 15
    Configuring an HDLC Channel 17
        Optional Tasks 17
Configuration Example 20

Testing Interfaces....20
Testing at the T3 Layer....21
Testing at the T1 Layer....23
Monitoring Interfaces....25
Setting a Baseline....26
Displaying Counters and Time Intervals....26
Output Filtering....26

Chapter 2 Configuring T3 and E3 Interfaces 41

Overview....41
MDL Support....41
MDL Standards....42
Timeout of Received MDL Messages....42
Higher-Level Protocols....43
Platform Considerations....43
COCX-F3 Line Modules and Associated I/O Modules....43
OCx/STMx/DS3-ATM Line Modules and 4xDs3 ATM I/O Modules....44
CT3/T3-F0 Line Modules and CT3/T3 12 I/O Modules....44
Interface Stack....45
Numbering Scheme....46
References....46
Before You Configure an Interface....47
Configuration Tasks....47
Configuring a T3 or an E3 Controller....47
Configuring MDL Messages....49
Optional Tasks....50
Configuring Fractional T3....52
Configuring an HDLC Channel....53
Optional Tasks....53
Configuration Examples....55
Testing Interfaces....56
Sending BERT Patterns....56
Enabling Local, Network, and Payload Loopback....57
Enabling Remote Loopback....58
Monitoring Interfaces....59
Setting a Baseline....59
Displaying Counters and Time Intervals....59
Output Filtering....60

Chapter 3 Configuring Unchannelized OCx/STMx Interfaces 67

Overview....67
APS and MSP....67
Automatic Switchover....68
Manual Switchover....68
Switching Mechanisms....69
Reversion After Switchover....69
Communication Methods....70
Higher-Level Protocols....71
Platform Considerations....71
OCx/STMx/DS3-ATM Line Modules....72
OCx/STMx POS Line Modules....72
OC48 Line Modules....73
OC3/STM1 GE/FE Line Module....73

ES2 4G Line Module....74
E120 Router Configuration....74
E320 Router Configuration....74
OCx/STMx ATM IOAs....75
OCx/STMx POS IOAs....75
Numbering Scheme....76
ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router....76
E120 Router and E320 Router....77
Interface Specifier....77
Exchanging Modules....78
References....78
Configuration Tasks....78
Configuring the SONET/SDH Layers....79
Configuring APS/MSP....83
Configuring the Working Interface....83
Configuring the Protect Interface....85
Configuring SONET/SDH Alarms....87
Configuration Example....87
Configuring APS Event Collection....88
Manual Switching to a Redundant Port....88
Testing Interfaces....89
Loopback Testing....89
Testing Connectivity....90
Monitoring SONET/SDH Interfaces....91
Monitoring Interface Statistics....91
Monitoring APS/MSP....98

Chapter 4 Configuring Channelized OCx/STMx Interfaces 101

Overview....101
SONET APS and SDH MSP....101
MDL/FDL Support....102
MDL Standards....102
FDL Standards....102
Timeout of Received MDL and FDL Messages....102
Frequency of FDL Path Messages....103
Higher-Level Protocols....103
Platform Considerations....104
cOCx/STMx FO Line Module....104
Interface Stack....105
SONET/SDH VT Controllers....106
T3 Controllers....108
HDLC....109
Numbering Scheme....109
References....109
Before You Configure an Interface....111
Configuration Tasks....111
SONET/SDH Configuration Tasks....111
Configuring Higher Layers....116
T1/E1 Configuration Tasks....116
Configuring an Unframed E1 Line....117
Configuring T1 and E1 Lines....117
Configuring T1 Interfaces to Send FDL Messages....120
Disabling Interfaces and Channel Groups....121
Configuring Higher Layers....121

T3 Configuration Tasks 122
Configuring T3 Line Parameters 122
Configuring T3 Interfaces to Send MDL Messages 124
Configuring T1 Channels on T3 Interfaces 126
Configuring T1 Channels to Send FDL Messages 128
Configuring Higher Layers 130
HDLC Channel Configuration Tasks 130
Optional Tasks 130
Configuration Examples 133
Example 1: Configuring Interfaces in SONET Mode 133
Example 2: Configuring Interfaces in SDH Mode 134
Example 3: Configuring Frame Relay 135
Example 4: Configuring PPP 136
Testing Interfaces 136
Sending BERT Patterns 136
Receiving BERT Patterns 138
Enabling Local or Network Loopback 138
Enabling Remote Loopback Testing 140
Testing Connectivity 143
Monitoring Interfaces 144
Setting a Baseline 144
Output Filtering 144
Monitoring APS/MSP 162

Chapter 5 Configuring Ethernet Interfaces 163

Ethernet Overview 164
Features 164
L2TP 165
Multinetting 165
Ethernet Interface Platform Considerations 165
Numbering Scheme 166
ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router 166
E120 Router and E320 Router 166
Interface Specifier 167
Fast Ethernet I/O Modules 167
FE-8 I/O Module 167
FE-8 SFP I/O Module 167
Gigabit Ethernet I/O Modules and IOAs 168
GE I/O Module 168
GE-2 SFP I/O Module 168
Ports on GE-2 SFP I/O Module 169
Bandwidth and Line Rate Considerations 169
GE-8 I/O Module 169
Bandwidth and Line Rate Considerations 170
Managing High-Density Ethernet 170
OC3-2 GE APS I/O Module 171
ES2-S1 GE-4 IOA 171
ES2-S1 GE-8 IOA 172
ES2 4G LM Combination 172
ES2 10G LM Combination 174
ES2-S3 GE-20 IOA 175
ES2 10G LM Combination 176
Bandwidth and Line Rate Considerations 176
Managing High-Density Ethernet 176

10-Gigabit Ethernet IOAs....177
ES2-S1 10GE IOA....177
Managing High-Density Ethernet....177
ES2-S2 10GE PR IOA....177
ES2 10G Uplink LM Combination....178
ES2 10G LM Combination....179
Ethernet References....180
High-Density Ethernet....181
Managing Port Redundancy on Gigabit Ethernet I/O Modules....181
Configuration Tasks for Ethernet....183
Configuring the Physical Interface....183
Configuring VLANs....187
Creating a VLAN Major Interface....189
Common VLAN Configurations....189
Configuring IP over VLAN....189
Configuring PPPoE over VLAN....191
Configuring MPLS over VLAN....192
Configuring IP over VLAN and PPPoE over VLAN....193
Configuring S-VLANs....197
Configuring PPPoE over S-VLAN....198
Configuring S-VLAN Tunnels for Layer 2 Services over MPLS....201
Advantages....201
Interface Stacking....202
Configuration Example....202
S-VLAN Oversubscription....204
Configuring 802.3ad Link Aggregation for Ethernet....205
LACP....206
Higher-Level Protocols....206
Load Balancing and QoS....207
Configuration Tasks for 802.3ad Link Aggregation....207
Configuring an Ethernet Physical Interface....207
Configuring a LAG Bundle....208
Configuring IP for a LAG Bundle....208
Configuring a VLAN Subinterface for a LAG Bundle....208
Configuring a PPPoE Subinterface for a LAG Bundle....208
Configuring MPLS for a LAG Bundle....209
802.3ad Link Aggregation Configuration Examples....209
Example: Configuring an IP Interface for a LAG Bundle....210
Example: Configuring a PPPoE Subinterface for a LAG Bundle....210
Example: Configuring a PPPoE Subinterface over a VLAN for a LAG Bundle....211
Example: Configuring MPLS for a LAG Bundle....212
Example: Configuring MPLS over a VLAN for a LAG Bundle....212
Configuring Ethernet Link Redundancy....214
Ethernet Link Redundancy Configuration Models....215
Ethernet Link Redundancy Configuration Diagrams....216
Ethernet Link Redundancy Behavior....220
Link Failure and Acquisition....220
LACP Configuration and Member Link Behavior....221
Member Link with Non-LAG Partner....222
Configuring Ethernet Link Redundancy....224
Configuring Higher-Level Protocols over Ethernet....225
Configuring IP over Ethernet....226
Configuring PPPoE over Ethernet....226

Configuring IP and MPLS over Ethernet....227
Configuring IP, MPLS, and PPPoE over Ethernet....228
Ethernet Link Aggregation and MPLS....229
Disabling Ethernet Interfaces....230
Monitoring Ethernet Interfaces....230
Setting Statistics Baselines....230
Displaying Interface Rate Statistics for VLAN Subinterfaces....230
Using Ethernet show Commands....233

Chapter 6 Managing Tunnel-Service and IPSec-Service Interfaces 251

Tunnel-Service and IPSec-Service Overview....251
Types of Tunnel-Server Ports....252
Dedicated Tunnel-Server Ports....252
Shared Tunnel-Server Ports....252
Types of Tunnel-Service Interfaces....253
Tunnel-Service Interface Platform Considerations....253
Supported Modules for Dedicated Tunnel-Server Ports....254
ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router....254
E120 Router and E320 Router....254
Supported Modules for Shared Tunnel-Server Ports....255
ERX-14xx Models and the ERX-310 Router....255
E120 Router and E320 Router....255
Numbering Scheme....255
ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router....255
E120 Router and E320 Router....256
Interface Specifier....256
Supported Applications for Dedicated and Shared Tunnel-Server Ports....257
Redundancy and Interface Distribution of Tunnel-Service Interfaces....257
SMs, ES2-S1 Service IOA, and Shared Tunnel-Server Modules....258
Static IP Tunnel-Service Interfaces....258
Dynamic Tunnel-Service Interfaces....258
Interface Allocation for Shared Tunnel-Server Modules....259
ISMs....259
Tunnel-Service Interface Considerations....260
Provisioning Tunnel-Service Interfaces....260
Bandwidth Limitations of Shared Tunnel-Server Ports....260
Exchanging Tunnel-Server Modules....260
Unprovisioned Tunnel-Service Interfaces....261
Configuring Tunnel-Server Ports and Tunnel-Service Interfaces....262
Identifying the Physical Location of the Tunnel-Server Port....262
Provisioning the Maximum Number of Interfaces on a Tunnel-Server Port....262
Verifying the Tunnel-Server Interface Configuration....263
Unprovisioning Tunnel-Service Interfaces....263
Monitoring Tunnel-Service Interfaces....264

Index 269

About This Guide

This preface provides the following guidelines for using the *JUNOSe™ Software for E-series™ Routing Platforms Physical Layer Configuration Guide*:

- Objectives on page xi
- Audience on page xi
- E-series Routers on page xii
- Documentation Conventions on page xii
- Related E-series and JUNOSe Documentation on page xiv
- Obtaining Documentation on page xvii
- Documentation Feedback on page xviii
- Requesting Technical Support on page xviii

Objectives

This guide provides the information that you need to configure physical interfaces on E-series routers.

An E-series router is shipped with the latest system software installed. If you need to install a future release or reinstall the system software, refer to the procedures in *JUNOSe System Basics Configuration Guide, Chapter 3, Installing JUNOSe Software*.

NOTE: If the information in the latest *JUNOSe Release Notes* differs from the information in this guide, follow the *JUNOSe Release Notes*.

Audience

This guide is intended for experienced system and network specialists working with E-series routers in an Internet access environment.

E-series Routers

Seven models of E-series routers are available:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

All models use the same software. For information about all models except the E120 router and the E320 router, see *ERX Hardware Guide, Chapter 1, ERX Overview*. For information about the E120 router and the E320 router, see *E120 and E320 Hardware Guide*, *Chapter 1*, *E120 and E320 Overview*.

In the E-series documentation, the term ERX-14xx models refers to both the ERX-1440 router and the ERX-1410 router. Similarly, the term ERX-7xx models refers to both the ERX-710 router and the ERX-705 router. The terms ERX-1440 router, ERX-1410 router, ERX-710 router, ERX-705 router, ERX-310 router, E120 router, and E320 router refer to the specific models.

Documentation Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

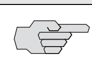
Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury.

Table 2 defines text conventions used in this guide and the syntax conventions used primarily in the *JUNOSe Command Reference Guide*. For more information about command syntax, see *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Text Conventions		
Bold text like this	Represents commands and keywords in text.	■ Issue the **clock source** command. ■ Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	host1(config)#**traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	`host1#`**`show ip ospf 2`**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	■ Emphasizes words. ■ Identifies variables. ■ Identifies chapter, appendix, and book names.	■ There are two levels of access, *user* and *privileged*. ■ *clusterId*, *ipAddress*. ■ *Appendix A*, *System Specifications*.
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the *Command Reference Guide*		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Related E-series and JUNOSe Documentation

The E-series and JUNOSe documentation set consists of several hardware and software guides, which are available in electronic and printed formats.

E-series and JUNOSe Documents

Table 3 lists and describes the E-series and JUNOSe document set. For a complete list of abbreviations used in this document set, along with their spelled-out terms, see *JUNOSe System Basics Configuration Guide, Appendix A, Abbreviations and Acronyms*.

Table 3: Juniper Networks E-series and JUNOSe Technical Publications

Document	Description
E-series Hardware Documentation	
E120 and E320 Quick Start Guide	Shipped in the box with all new E120 and E320 routers. Provides the basic procedures to help you get the routers up and running quickly.
E120 and E320 Hardware Guide	Provides the necessary procedures for getting E120 routers and E320 routers operational, including information about: ■ Installing the chassis and modules ■ Connecting cables ■ Powering up the routers ■ Configuring the routers for management access ■ Troubleshooting common issues Describes switch route processor (SRP) modules, line modules, and I/O adapters (IOAs) available for E120 and E320 routers.
E120 and E320 Module Guide	Provides detailed specifications for line modules and IOAs in E120 and E320 routers, and information about the compatibility of these modules with JUNOSe software releases. Lists the layer 2 protocols, layer 3 protocols, and applications that line modules and their corresponding IOAs support. Provides module LED information.
E-series Installation Quick Start poster or *ERX Quick Start Guide*	Shipped in the box with all new ERX routers. Provides the basic procedures to help you get an ERX router up and running quickly.
ERX Hardware Guide	Provides the necessary procedures for getting ERX-14xx models, ERX-7xx models, and ERX-310 routers operational, including information about: ■ Installing the chassis and modules ■ Connecting cables ■ Powering up the routers ■ Configuring the routers for management access ■ Troubleshooting common issues Describes switch route processor (SRP) modules, line modules, and I/O modules available for the ERX routers.

Table 3: Juniper Networks E-series and JUNOSe Technical Publications (continued)

Document	Description
ERX Module Guide	Provides detailed specifications for line modules and I/O modules in ERX-14xx models, ERX-7xx models, and ERX-310 routers, and information about the compatibility of these modules with JUNOSe software releases. Lists the layer 2 protocols, layer 3 protocols, and applications that line modules and their corresponding I/O modules support. Provides module LED information.
ERX End-of-Life Module Guide	Provides an overview and description of ERX modules that are end-of-life (EOL) and can no longer be ordered for the following routers: ■ ERX-7xx models ■ ERX-14xx models ■ ERX-310 router
JUNOSe Software Guides	
JUNOSe System Basics Configuration Guide	Provides information about: ■ Planning and configuring your network ■ Using the command-line interface (CLI) ■ Installing JUNOSe software ■ Configuring the Simple Network Management Protocol (SNMP) ■ Managing the router and its modules, including the use of high availability (HA) for SRP redundancy ■ Configuring and running a unified in-service software upgrade (ISSU) ■ Configuring passwords and security ■ Configuring the router clock ■ Configuring virtual routers
JUNOSe Physical Layer Configuration Guide	Explains how to configure, test, and monitor physical layer interfaces.
JUNOSe Link Layer Configuration Guide	Explains how to configure and monitor static and dynamic link layer interfaces.
JUNOSe IP, IPv6, and IGP Configuration Guide	Explains how to configure and monitor IP, IPv6 and Neighbor Discovery, and interior gateway protocols (RIP, OSPF, and IS-IS).
JUNOSe IP Services Configuration Guide	Explains how to configure and monitor IP routing services. Topics include: ■ Routing policies ■ Firewalls ■ Network Address Translation (NAT) ■ J-Flow statistics ■ Bidirectional forwarding detection (BFD) ■ Internet Protocol Security (IPSec) ■ Access Node Control Protocol (ANCP), also known as Layer 2 Control (L2C) ■ Digital certificates ■ IP tunnels ■ Virtual Router Redundancy Protocol (VRRP) ■ Mobile IP home agent

Table 3: Juniper Networks E-series and JUNOSe Technical Publications (continued)

Document	Description
JUNOSe Multicast Routing Configuration Guide	Explains how to configure and monitor IP multicast routing and IPv6 multicast routing. Topics include: ■ Internet Group Management Protocol (IGMP) ■ Protocol Independent Multicast (PIM) ■ Distance Vector Multicast Routing Protocol (DVMRP) ■ Multicast Listener Discovery (MLD)
JUNOSe BGP and MPLS Configuration Guide	Explains how to configure and monitor: ■ Border Gateway Protocol (BGP) routing ■ Multiprotocol Label Switching (MPLS) and related applications ■ Layer 2 services over MPLS ■ Virtual private LAN service (VPLS) ■ Layer 2 virtual private networks (L2VPNs)
JUNOSe Policy Management Configuration Guide	Explains how to configure, manage, and monitor customized policy rules for packet classification, forwarding, filtering, and flow rates. Also describes the packet mirroring feature, which uses secure policies.
JUNOSe Quality of Service Configuration Guide	Explains how to configure quality of service (QoS) features to queue, schedule, and monitor traffic flow. These features include: ■ Traffic classes and traffic-class groups ■ Drop, queue, QoS, and scheduler profiles ■ QoS parameters ■ Statistics
JUNOSe Broadband Access Configuration Guide	Explains how to configure and monitor a remote access environment, which can include the following features: ■ Authentication, authorization, and accounting (AAA) ■ Dynamic Host Configuration Protocol (DHCP) ■ Remote Authentication Dial-In User Service (RADIUS) ■ Terminal Access Controller Access Control System (TACACS+) ■ Layer 2 Tunneling Protocol (L2TP) ■ Subscriber management
JUNOSe System Event Logging Reference Guide	Describes the JUNOSe system logging feature and describes how to use the CLI to monitor your system's log configuration and system events.
JUNOSe Command Reference Guide A to M; JUNOSe Command Reference Guide N to Z	Together constitute the *JUNOSe Command Reference Guide*. Contain important information about commands implemented in the system software. Use to look up: ■ Descriptions of commands and command parameters ■ Command syntax ■ A command's related mode ■ Starting with JUNOSe Release 7.1.0, a history of when a command, its keywords, and its variables were introduced or added Use with the JUNOSe configuration guides.
JUNOSe Comprehensive Index	Provides a complete index of the JUNOSe software documentation set.
JUNOSe Glossary	Provides definitions for terms used in JUNOSe technical documentation.

Table 3: Juniper Networks E-series and JUNOSe Technical Publications (continued)

Document	Description
Release Notes	
JUNOSe Release Notes	Provide the latest information about features, changes, known problems, resolved problems, and system maximum values. If the information in the *Release Notes* differs from the information found in the documentation set, follow the *Release Notes*. Release notes are included on the corresponding software CD and are available on the Web.

JUNOSe Configuration Guides

JUNOSe software configuration guides use a bottom-up approach to describe the relationship of layers, protocols, and interfaces in the configuration process. For more information, see *Layered Approach* in *JUNOSe System Basics Configuration Guide, Chapter 1, Planning Your Network*.

The chapters in JUNOSe software configuration guides typically include the following topics:

- Conceptual and overview information
- Information you need to know or tasks you need to perform before you begin
- Platform-specific issues you need to take into consideration
- Applicable references, such as RFCs and IETF draft documents, about the protocols and features supported by the router
- Required and optional tasks, as step-by-step procedures
- Descriptions and examples of the commands you use
- Illustrations of network topologies
- Examples of command sequences for configuration, testing, and monitoring activities
- Sample displays that result when you issue the **show** command

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To order printed copies of this manual and other Juniper Networks technical documents or to order a documentation CD, which contains this manual, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the software CDs and at http://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at http://www.juniper.net/techpubs/docbug/docbugreport.html. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Technical Support

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

- **JTAC Policies**—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/customers/support/downloads/710059.pdf
- **Product Warranties**—For product warranty information, visit http://www.juniper.net/support/warranty/
- **JTAC Hours of Operation**—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Manager: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at 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 Manager 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 http://www.juniper.net/support/requesting-support.html

Chapter 1
Configuring Channelized T3 Interfaces

Use the procedures described in this chapter to configure channelized T3 (CT3) interfaces on E-series routers.

This chapter contains the following sections:

- Overview on page 1
- Platform Considerations on page 4
- References on page 7
- Before You Configure an Interface on page 8
- Configuration Tasks on page 8
- Configuration Example on page 20
- Testing Interfaces on page 20
- Monitoring Interfaces on page 25

Overview

Channelized T3 interfaces are supported by the modules described in this chapter. Configuration procedures for all channelized T3 physical interfaces are identical; however, the capabilities of the modules differ. Each port on a CT3 module offers a total bidirectional rate of 43.008 Mbps.

This section describes the features of channelized T3 interfaces. For information about configuring channelized T3 interfaces over SONET/SDH, see *Chapter 4, Configuring Channelized OCx/STMx Interfaces*.

MDL/FDL Support

Channelized T3 interfaces on some line modules support maintenance data link (MDL) messages at the T3 level and facilities data link (FDL) messages at the T1 level. For a list of the line modules that support MDL and FDL, see *ERX Module Guide*, *Appendix A*, *Module Protocol Support*.

You can use MDL and FDL messages to determine the status of a link and to display statistics for the remote end of a connection. MDL and FDL messages do not interfere with other data transmitted over the link.

MDL Standards

You can configure channelized T3 interfaces to send MDL messages that comply with ANSI T1.107a-1990 Standard for Telecommunications—Digital Hierarchy – Supplement to Formats Specification (August 1990). MDL messages identify a particular link by sharing common codes for data such as the equipment identifier, line identifier, frame identifier, and unit.

FDL Standards

Similarly, you can configure T1 channels to send FDL messages that comply with either or both of the following standards:

- ANSI T1.403-1989 Standard for Telecommunications—Network and Customer Installation Interfaces – DS1 Metallic Interface – Robbed-bit Signaling State Definitions (1989)

  FDL messages that comply with the ANSI standard identify a particular link by sharing common codes for data such as the equipment identifier, line identifier, frame identifier, and unit.

- AT&T Technical Reference 54016—Requirements for Interfacing Digital Terminal Equipment to Services Employing the Extended Superframe Format (September 1989)

  FDL messages that comply with the AT&T standard identify a particular link by sharing performance data and do not use common codes for data such as the equipment identifier, line identifier, frame identifier, and unit.

Timeout of Received MDL and FDL Messages

When a line module receives an MDL or FDL message string, it stores the strings for a period of 10 seconds after the last message was received. If the line module does not receive another message of any type containing the same string within 10 seconds, it erases the local copy of the message.

Most MDL and FDL message strings are common to all three types of messages that can be transmitted: path identifications, idle signals, and test signals. Certain message strings, however, are unique to a particular message type. Table 4 briefly describes each MDL/FDL message string and indicates (with a ✔) the types of messages in which it can be sent.

Table 4: MDL and FDL Message Strings and Message Types

Message String	Description	Path Message	Idle Signal Message	Test Signal Message
eic	Equipment identification code	✔	✔	✔
fic	Frame identification code	✔	✔	✔
generator	Generator number	–	–	✔
lic	Line identification code	✔	✔	✔

Table 4: MDL and FDL Message Strings and Message Types (continued)

Message String	Description	Path Message	Idle Signal Message	Test Signal Message
pfi	Facility identification code	✔	–	–
port	Equipment port number	–	✔	–
unit	Unit identification code	✔	✔	✔

As long as another message of any type containing the same string is received within 10 seconds, the line module retains the local copy of the message string and resets the 10-second timer for that string.

For example, if a line module receives an MDL or FDL test signal message containing an eic string, and then receives an idle signal message within 10 seconds that also contains an eic string, it retains the local copy of the most recent eic string received and resets the 10-second timer for that message. However, if 10 seconds pass without the line module receiving a path identification, test signal, or idle signal message containing an eic string, the line module erases the local copy of the eic message string.

For message strings that are unique to a particular message type, the line module must receive another message of the same type containing this string in order to retain the local copy of the string and reset the timer. For example, if the line module receives a test signal message containing a generator string and does not receive another test signal message within 10 seconds, it will erase the local copy of the generator string.

Frequency of FDL Path Messages

E-series routers transmit FDL path identifier messages every second. This behavior complies with the ANSI T1.403 specification (see *References* on page 7 for more information) and is consistent with the MDL implementation for E-series routers.

Higher-Level Protocols

See *ERX Module Guide*, *Appendix A*, *Module Protocol Support* for information about the higher-level protocols that channelized T3 interfaces support.

Platform Considerations

You can configure channelized T3 interfaces on the following E-series routers:

- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

NOTE: The E120 router and the E320 router do not support configuration of channelized T3 interfaces.

For detailed information about the modules that support channelized T3 interfaces on ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that channelized T3 modules support.

CT3/T3-F0 Line Modules and CT3/T3 12 I/O Modules

ERX-7xx models, ERX-14xx models, and the ERX-310 router support the CT3/T3-F0 line module and CT3/T3 12 I/O module. The CT3/T3-F0 line module and CT3/T3 12 I/O module support both channelized and unchannelized T3 operation. You can configure a mixture of channelized and unchannelized ports on these modules. For information about configuring unchannelized T3 ports, see *Chapter 2, Configuring T3 and E3 Interfaces*.

ERX-14xx models support up to 12 CT3/T3-F0 line modules and 12 CT3/T3 12 I/O modules, ERX-7xx models support up to 5 CT3/T3-F0 line modules and 5 CT3/T3 12 I/O modules, and the ERX-310 router supports up to two CT3/T3-F0 line modules and two CT3/T3 12 I/O modules. Each CT3/T3 12 I/O module has 12 physical T3 (DS3) ports. Each port uses two SMB connectors: one for the transmit (TX) connection and one for the receive (RX) connection.

CT3/T3-F0 line modules and CT3/T3 12 I/O modules support the following in channelized mode:

- 28 asynchronous T1 (DS1) channels per T3 port
- 24 DS0 channels (64-Kbps) per T1 interface
- 166 DS0 channels per T3 port

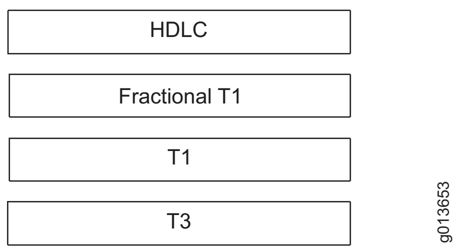
Exchanging Modules

If you replace a CT3/T3 line module and a CT3/T3 I/O module with a CT3/T3-F0 line module and a CT3/T3 12 I/O module or vice versa, you must erase the configuration of the existing modules. See **slot accept** in *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

Interface Stack

Figure 1 shows the stack for a channelized T3 interface. To configure a channelized T3 interface, configure a T3 controller, followed by a T1 channel, and then a fractional T1 channel. Finally, you must configure a High-Speed Data Link Control (HDLC) data channel on the interface.

Figure 1: Stack for Channelized T3 Interface



For more information about the layers in a channelized T3 interface, see *Numbering Scheme* on page 5.

NOTE: For a detailed description of interface types and specifiers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*. For information about interfaces, see *JUNOSe System Basics Configuration Guide, Chapter 1, Planning Your Network*.

Numbering Scheme

This section describes how to identify each layer in a channelized T3 interface stack.

T3 Controllers

A T3 controller on a channelized T3 interface is identified using the *slot/port* format where:

- *slot*—Number of the slot in which the line module resides in the chassis.

  In ERX-7xx models, line module slots are numbered 2-6; slots 0 and 1 are reserved for SRP modules. In ERX-14xx models, line module slots are numbered 0–5 and 8–13; slots 6 and 7 are reserved for SRP modules. In an ERX-310 router, line module slots are numbered 0–2; slot 0 is reserved for the SRP module.

- *port*—Number of the port on the I/O module. On a CT3/T3 12 I/O module, ports are numbered 0–11.

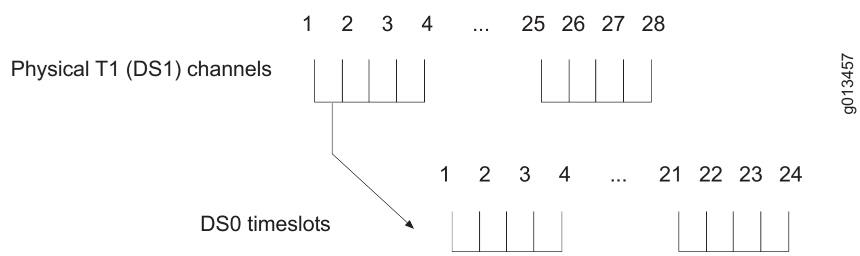
For information about installing line modules and I/O modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

T1 Channels

A T3 line consists of 28 T1 channels (or data streams). A T1 channel is identified by its number in the range 1–28.

Each T1 channel is an aggregate of 24 DS0 timeslots, as shown in Figure 2. To configure an entire T1 line, assign 24 timeslots to each channel.

Figure 2: T1 Channels and DS0 Timeslots on a T3 Line



Fractional T1

Fractional T1 is a portion of a T1 line. To configure fractional T1 on a channelized T3 interface, you assign a range of DS0 timeslots to a T1 channel and *subchannel*. A subchannel is group of timeslots. Subchannel numbers range from 1–24 and do not necessarily correspond to DS0 timeslots. The subchannel number identifies a fractional T1 channel.

For example, you might make the assignments for subchannels 1–6 as listed in Table 5.

Table 5: Sample T1 Subchannel/Timeslot Assignments

Subchannel	DS0 Timeslot
1	1–4, 10, 22–24
2	5–6
3	7–9
4	11
5	12–15, 20–21
6	16–19

To configure the subchannels listed in Table 5, use the following command to specify the T3 controller in chassis slot 0, port 1.

host1(config)#**controller t3 0/1**

Then assign the timeslots to channel 1, subchannel 1.

```
host1(config-controll)#t1 1/1 timeslots 1-4,10,22-24
host1(config-controll)#t1 1/2 timeslots 5-6
host1(config-controll)#t1 1/3 timeslots 7-9
host1(config-controll)#t1 1/4 timeslots 11
host1(config-controll)#t1 1/5 timeslots 12-15,20-21
host1(config-controll)#t1 1/6 timeslots 16-19
```

HDLC Channels

To identify an HDLC channel or the complete channelized T3 interface, use the format *slot/port*:*T1 channel/subchannel*. Refer to the preceding sections for definitions of the variables.

References

For more information about channelized T3 interfaces, consult the following resources:

- RFC 1661—The Point-to-Point Protocol (PPP) (July 1994)
- RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999)
- RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999)
- ANSI T1.107a-1990 Standard for Telecommunications—Digital Hierarchy – Supplement to Formats Specification (August 1990)
- ANSI T1.403-1989 Standard for Telecommunications—Network and Customer Installation Interfaces – DS1 Metallic Interface – Robbed-bit Signaling State Definitions (1989)
- AT&T Technical Reference 54016—Requirements for Interfacing Digital Terminal Equipment to Services Employing the Extended Superframe Format (September 1989)

For more information about bit error rate test (BERT) patterns, see:

- ITU O.151—Error performance measuring equipment operating at the primary rate and above (October 1992)
- ITU O.153—Basic parameters for the measurement of error performance at bit rates below the primary rate (October 1992)
- T1M1.3 Working Group—A Technical Report on Test Patterns for DS1 Circuits (November 1993)
- ANSI T1.404-1994 Standard for Telecommunications—Network-to-Customer – DS3 Metallic Interface Specification (1994)

Before You Configure an Interface

Before you configure a channelized T3 interface, verify the following:

- You have installed the line module and the I/O module correctly.
- Each configured line module is able to transmit data to and receive data from your switch connections.

For more information about installing line modules and I/O modules, see the *ERX Hardware Guide*.

You should also have the following information available:

- Framing type, clock source, cable length, and the loopback method for each T3 controller
- Framing type and clock source for each T1 channel
- Timeslot mapping and line speed for each fractional T1 channel
- HDLC channel information, such as data inversion information, cyclic redundancy check (CRC) type, idle character, maximum transmission unit (MTU), and maximum receive unit (MRU)

Configuration Tasks

To configure a channelized T3 interface:

1. Configure a T3 controller.
2. (Optional) Configure MDL settings.
3. (Optional) Configure other settings for the interface.
4. Configure T1 channels and subchannels.
5. Configure HDLC channels.

Configuring a T3 Controller

To configure a T3 controller:

1. Access Controller Configuration mode by specifying the T3 controller.

   host1(config)#**controller t3 0/1**

2. Enable the T3 controller.

   T3 controllers are disabled by default.

   host1(config-controll)#**no shutdown**

controller t3

- Use to specify a T3 controller in *slot/port* format.
  - *slot*—Number of the slot in which the line module resides in the chassis
  - *port*—Number of the port on the I/O module
- Example

  host1(config)#**controller t3 0/1**
- There is no **no** version.

shutdown

- Use to disable a T3 controller.
- The T3 interface is disabled by default.
- Example

  host1(config-controll)#**no shutdown**
- Use the **no** version to restart a disabled interface.

Configuring MDL Messages

You can configure a channelized T3 interface to send MDL messages. MDL messages are supported only when T3 framing uses C-bit parity, the default setting.

To configure a channelized T3 interface to send MDL messages:

1. Specify a T3 interface.

   host1(config)#**controller t3 8/0**

2. (Optional) Configure the interface to operate in an MDL carrier environment.

   host1(config-controll)#**mdl carrier**

3. Specify the MDL messages.

   host1(config-controll)#**mdl string eic "ERX-1410"**
   host1(config-controll)#**mdl string fic "FG786"**
   host1(config-controll)#**mdl string lic "Bldg 10"**
   host1(config-controll)#**mdl string pfi "Site 25"**
   host1(config-controll)#**mdl string port 0800**
   host1(config-controll)#**mdl string unit 080001**

4. Enable transmission of MDL messages.

   host1(config-controll)#**mdl transmit path-id**
   host1(config-controll)#**mdl transmit idle-signal**
   host1(config-controll)#**mdl transmit test-signal**

mdl carrier

- Use to specify that an interface is used in the carrier environment.
- Example

  host1(config-controll)#**mdl carrier**

- Use the **no** version to restore the default situation, in which the interface does not operate in the carrier environment.

mdl string

- Use to specify an MDL message.
- Example

  host1(config-controll)#**mdl string port 0800**

- Use the **no** version to restore the default value to the specified MDL message or to all MDL messages.

mdl transmit

- Use to enable transmission of MDL messages.
- Specify the keyword **path-id** to transmit path identifications every second.
- Specify the keyword **idle-signal** to send idle signals every second.
- Specify the keyword **test-signal** to transmit test signals every second.
- Example

  host1(config-controll)#**mdl transmit test-signal**

- Use the **no** version to disable transmission of the specified MDL message or all MDL messages.

Other Optional Tasks

The following configuration tasks are optional when you configure a T3 controller:

- Specify a cable length.
- Change the clock source.
- Change the framing format.
- Enable or disable SNMP link status processing.
- Assign a text description or an alias to the interface.

cablelength

- Use to adjust the transmit power appropriate to the length of the T3 cable.
- Specify a cable length in the range 1–450 feet.
- The router supports two transmit powers, one for a cable length 1–225 feet and another for a cable length 226–450 feet. Therefore, it is not necessary for you to know the exact length of your cable. You only need to know if the cable length is greater than 225 feet. For example, if your cable size exceeds 225 feet, specify any number greater than 225 (and less than 451).
- Example

  host1(config-controll)#**cablelength 300**

- Use the **no** version to restore the default value, 0 feet.

clock source

- Use to configure the transmit clock source for a T3 controller.
- Configure one end of the line as **internal** and the other end as **line**.
- Specify the keyword **line** to use a transmit clock recovered from the line's receive data stream.
- Specify the keywords **internal module** to use the line module's internal clock as the transmit clock.
- Specify the keywords **internal chassis** to use the router's clock as the transmit clock.
- Example

  host1(config-controll)#**clock source internal module**

- Use the **no** version to revert to the default, **line**.

description

- Use to assign a text description or an alias to a channelized T3 interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show controllers t3 | t1** command to display the text description.
- Example

  host1(config-controll)#**description toronto ct3 interface**

- Use the **no** version to remove the text description or alias.

framing

- Use to configure the framing format for a T3 controller.
- Specify either **m23** or **c-bit** framing.
- Choose the framing format that is compatible with the framing format of the Telco network device at the other end of the line.
- Select **c-bit** framing if you intend to configure MDL messages.

- Example

  host1(config-controll)#**framing c-bit**

- Use the **no** version to restore the default value, **c-bit**.

snmp trap link-status

- Use to enable SNMP link status processing on a T3 controller.
- Example

  host1(config-controll)#**snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

Configuring T1 Channels

To configure T1 channels and subchannels:

1. From Global Configuration mode, specify the T3 controller in slot 0, port 1.

   host1(config)#**controller t3 0/1**

2. Assign a range of timeslots to a channel and subchannel.

   For example, assign the following range of timeslots: 1, 3–8, and 10 to channel 2, subchannel 1. Timeslots 2, 9, and 11–24 are available for other subchannels.

   host1(config-controll)#**t1 2/1 timeslots 1,3-8,10**

Optional Tasks

The T1 channel configuration commands enable you to specify options for a single channel, multiple individual channels, ranges of channels, or any combination of the three types of specifications. For example:

host1(config-controll)#**t1 2,4,6-15,20-25 clock source line**

The following configuration tasks are optional when you configure T1 channels:

- Disable T1 channels.
- Change the clock source.
- Assign a text description or an alias to the interface.
- Change the framing format.
- Enable or disable SNMP link status processing.
- Configure FDL messages.

controller t3

- Use to specify a T3 controller in *slot/port* format.
  - *slot*—Number of the slot in which the line module resides in the chassis
  - *port*—Number of the port on the I/O module
- Example

  host1(config)#**controller t3 0/1**

- There is no **no** version.

t1 clock source

- Use to configure the transmit clock source for T1 channels.
- The router supports **internal** and **line** clocking.
  - If you specify internal clocking, the interface transmits data using the line module or the chassis as the internal clock. You must specify one of the following for internal clocking:
    - **module**—Specifies internal clock is from the line module itself
    - **chassis**—Specifies internal clock is from the configured router clock
  - If you specify line clocking, the interface transmits data with a clock recovered from the line's receive data stream.
- Example

  host1(config-controll)#**t1 2,4-10 clock source line**

- Use the **no** version to restore the default value, **line**.

t1 description

- Use to assign a text description or an alias to T1 or fractional T1 channels on a CT3 module.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show controllers t3 | t1** command to display the text description.
- Examples

  host1(config-controll)#**t1 2 description london t1 interface**
  host1(config-controll)#**t1 2/1 description london first ft1 interface**

- Use the **no** version to remove the text description or alias.

t1 framing

- Use to configure the framing format for T1 channels.
- You must specify either **esf** (extended superframe) or **sf** (superframe) framing.
- The framing format you choose must be compatible with the framing format at the other end of the line.

- Example

  host1(config-controll)#**t1 2 framing sf**

- Use the **no** version to restore the default value, **esf**.

t1 shutdown

- Use to disable T1 channels or a subchannel.
- To disable channels or a subchannel, specify one or more T1 channels or a subchannel in *channel* or *channel/subchannel* format.
  - *channel*—One or more T1 channels, or a range of channels in the range 1–28
  - *subchannel*—Subchannel from 1–24
- The T1 interface is enabled by default.
- Example

  host1(config-controll)#**t1 4-15,18,21,25-27 shutdown**

- Use the **no** version to restart a disabled interface.

t1 snmp trap link-status

- Use to enable SNMP link status processing on T1 channels.
- To enable or disable SNMP on an interface, specify T1 channels or subchannel in *channel* or *channel/subchannel* format.
  - *channel*—One or more T1 channels, or a range of channels in the range 1–28
  - *subchannel*—Subchannel from 1–24
- Example

  host1(config-controll)#**t1 2 snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

t1 timeslots

- Use to assign a range of DS0 timeslots to a subchannel as a single data stream.
- To configure a subchannel, specify a T1 channel in *channel/subchannel* format and a range of timeslots.
  - *channel*—T1 channel in the range 1–28
  - *subchannel*—Number from 1–24
  - dash—Represents a range of timeslots; a comma separates timeslots. For example, 1-10, 15-18 assigns timeslots 1–10 and 15–18.

- Example

  host1(config-controll)#**t1 2/1 timeslots 1,3-8,10**

- You can specify a line speed that applies to all DS0 timeslots assigned to a subchannel. The default line speed is 64 Kbps.
- Use the **no** version to delete the fractional T1 circuit.

Configuring FDL Messages

To configure T1 channels to send FDL messages:

1. Specify a T3 interface.

   host1(config)#**controller t3 8/0**

2. Specify the standard for transmission of FDL messages on both ends of the T1 connection.

   host1(config-controll)#**t1 1 fdl ansi**

3. (Optional) Configure one or more T1 channels to operate in an FDL carrier environment.

   host1(config-controll)#**t1 1 fdl carrier**

4. (ANSI signals) Specify the FDL messages.

   host1(config-controll)#**t1 1 fdl string eic "ERX-1410"**
   host1(config-controll)#**t1 1 fdl string fic "HY0019"**
   host1(config-controll)#**t1 1 fdl string lic "Bldg 10"**
   host1(config-controll)#**t1 1 fdl string unit 080001**
   host1(config-controll)#**t1 1 fdl string pfi "Site 25"**
   host1(config-controll)#**t1 1 fdl string port 0800**
   host1(config-controll)#**t1 1 fdl string generator "Test generator"**

5. Enable transmission of FDL messages.

   host1(config-controll)#**t1 1 fdl transmit path-id**

6. (Optional) Specify that the router should generate yellow alarms for the T1 channels.

   host1(config-controll)#**t1 1 yellow generate**

7. (Optional) Specify that the router should detect yellow alarms for the T1 channels.

   host1(config-controll)#**t1 1 yellow detect**

t1 fdl

- Use to specify the FDL standard for the channel.
- Specify one or more T1 channels or a range of channels in the range 1–28.
- Specify the keyword **ansi** to support the ANSI FDL standard (see *References* on page 7).
- Specify the keyword **att** to support the AT&T FDL standard (see *References* on page 7).
- Specify the keyword **all** to support both the ANSI and AT&T standards
- Specify the keyword **none** to remove the current FDL mode settings
- You can configure a different standard on each T1 channel.
- Example

  host1(config-controll)#**t1 14-20,24 fdl att**

- Use the **no** version to restore the default, none.

t1 fdl carrier

- Use to specify that T1 channels are used in the carrier environment.
- Example

  host1(config-controll)#**t1 6 fdl carrier**

- Use the **no** version to restore the default situation, in which the T1 channels do not operate in the carrier environment.

t1 fdl string

- Use to specify an FDL message as defined in the ANSI T1.403 specification.

NOTE: The router sends these FDL messages only if you have issued the **t1 fdl** command with the **ansi** or **all** keyword and then issued the **t1 fdl transmit** command.

- Example

  host1(config-controll)#**t1 6 fdl string eic "ERX-1440"**

- Use the **no** version to restore the default value to the specified FDL message or to all FDL messages.

t1 fdl transmit

- Use to configure the router to send the specified type of FDL message.
- By default, the router sends only FDL performance data messages.

NOTE: The router sends FDL messages specified with the **t1 fdl string** command only if you have issued the **t1 fdl** command with the **ansi** or **all** keyword. If you specified the **att** keyword with the **t1 fdl** command, the router sends only performance data.

- Specify the keyword **path-id** to transmit path identifications every second.
- Specify the keyword **idle-signal** to send idle signals every second.
- Specify the keyword **test-signal** to transmit test signals every second.
- Example

  host1(config-controll)#**t1 28 fdl transmit path-id**

- Use the **no** version to disable transmission of the specified FDL message or all FDL messages.

t1 yellow detect

- Use to detect yellow alarm for T1 channels.
- By default, T1 channels detect alarms.
- Example

  host1(config-controll)#**t1 6,10-14,19 yellow detect**

- Use the **no** version to disable detection of yellow alarms.

t1 yellow generate

- Use to generate a yellow alarm when a loss of frame or loss of signal condition is detected on T1 channels.
- By default, T1 channels generate alarms.
- Example

  host1(config-controll)#**t1 6,10-14,19 yellow generate**

- Use the **no** version to disable generation of yellow alarms.

Configuring an HDLC Channel

You must configure an HDLC channel for each group of fractional T1 lines and each full T1 line.

To configure an HDLC channel, specify a serial interface (for example, HDLC channel in slot 0, port 1, channel 1, subchannel 5).

host1(config)#**interface serial 0/1:1/5**

Optional Tasks

The following configuration tasks are optional when you configure an HDLC channel on a channelized T3 interface:

- Configure the CRC.
- Specify the HDLC idle character.
- Enable data inversion on the interface.
- Set the time interval for monitoring bit and packet rates.

- Set the MRU.
- Set the MTU.
- Assign a text description or an alias to the serial interface.

crc

- Use to configure the size of the CRC.
- The CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data.
- 16 and 32 indicate the number of bits per frame that are used to calculate the frame check sequence (FCS). Both the sender and receiver must use the same setting.
- Use a 32-bit CRC when transmitting long streams at fast rates and to provide better ongoing error detection.
- Example

  host1(config-if)#**crc 32**

- Use the **no** version to restore the default value, 16.

idle-character

- Use to configure the HDLC idle character.
- The idle character is sent between HDLC packets.
- Specify one of the following idle characters:
  - **flags—**Sets the idle character to 0x7E
  - **marks**—Sets the idle character to 0xFF
- Example

  host1(config-if)#**idle-character marks**

- Use the **no** version to restore the default value, 0x7E (flags).

interface serial

- Use to configure a serial interface in the *slot/port:channel/subchannel* format.
  - *slot*—Number of the slot in which the line module resides in the chassis
  - *port*—Number of the port on the I/O module
  - *channel*—T1 channel
  - *subchannel*—Subchannel in the range 1–24
- Example

  host1(config)#**interface serial 0/1:1/5**

- Use the **no** version to disable the interface.

invert data

- Use to enable data stream inversion for the interface.
- Enable data stream inversion only if it is turned on at the other end of the line.
- Example

  host1(config-if)#**invert data**

- Use the **no** version to disable data inversion.

load-interval

- Use to set the time interval at which the router calculates bit and packet rate counters.
- You can choose a multiple of 30 seconds, in the range 30–300 seconds.
- Example

  host1(config-if)#**load-interval 90**

- Use the **no** version to restore the default value, 300 seconds.

mru

- Use to configure the MRU size for the interface.
- Specify a value in the range 4–9996 bytes.
- You should coordinate this value with the network administrator on the other end of the line.
- If you configure a different MRU value in higher-level protocols, such as IP, the router uses the lower value. This can produce unexpected behavior in your network.
- Example

  host1(config-if)#**mru 1600**

- Use the **no** version to restore the default, 1600 bytes.

mtu

- Use to configure the MTU size for the interface.
- Specify a value in the range 4–9996 bytes.
- You should coordinate this value with the network administrator on the other end of the line.
- If you configure a different MTU value in higher-level protocols, such as IP, the router uses the lower value. This can produce unexpected behavior in your network.
- Example

  host1(config-if)#**mtu 1600**

- Use the **no** version to restore the default, 1600 bytes.

serial description

- Use to assign a text description or an alias to a serial HDLC interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show interfaces serial** command to display the text description.
- Example

  host1(config-if)#**serial description ottawa012 hdlc channel**

- Use the **no** version to remove the text description or alias.

Configuration Example

The following example illustrates how to configure the layers on a channelized T3 interface:

```
host1(config)#controller t3 0/1
host1(config-controll)#no shutdown
host1(config-controll)#framing c-bit
host1(config-controll)#clock source internal module
host1(config-controll)#cablelength 220
host1(config-controll)#t1 2 framing esf
lihost1(config-controll)#t1 2 clock source internal
host1(config-controll)#t1 2 loopback local
host1(config-controll)#t1 2/1 timeslots 1,3-8,10
host1(config-controll)#exit
host1(config)#interface serial 0/1:2/1
host1(config-if)#invert data
host1(config-controll)#exit
```

Testing Interfaces

If you want to run loopback tests or bit error rate tests on channelized T3 interfaces, you must enable testing at the T3 or T1 layer. See *Interface Stack* on page 5 for a description of the layers.

For a list of the modules that support bit error rate tests (BERTs) and remote loopback, see *ERX Module Guide*, *Appendix A*, *Module Protocol Support*.

NOTE: BERTs are supported on frame-based channelized T3 interfaces, with the exception of the CT3/T3 line module used with the 3-port CT3/T3 I/O module.

Testing at the T3 Layer

To enable testing at the T3 layer:

1. Change the clock source to internal.

   host1(config-controll)#**clock source internal module**

2. Configure one of the following tests:

   - Set the loopback to **local** to test the line without connecting to the network.

     host1(config-controll)#**loopback local**

   - Set the loopback to **network** to test the line connected to the network.

     host1(config-controll)#**loopback network line**

3. (Optional) Configure one of the following tests for remote loopback:

   - Set the loopback to **remote** to request that a remote device connected on a T3 interface enter into a loopback.

     host1(config-controll)#**loopback remote**

   - Configure the T3 interface to enable or disable the ability to enter into a loopback initiated by a remote device, as follows:

     - Issue the **equipment customer loopback** command to enable the router to enter into loopback when it receives an appropriate signal from the remote device.

       host1(config-controll)#**equipment customer loopback**

     - Issue the **equipment network loopback** command to disable the ability to enter into loopback initiated by a remote device.

       host1(config-controll)#**equipment network loopback**

4. Configure the line to run bit error rate tests.

   host1(config-controll)#**bert pattern 2^15 time 20**

bert

- Use to enable bit error rate tests using the specified pattern on a channelized T3 interface.
- Unlike other configuration commands, **bert** is not stored in NVRAM.
- Specify one of the following test patterns:
  - **0s**—Repetitive test pattern of all zeros, 00000...
  - **1s**—Repetitive test pattern of all ones, 11111...
  - **2^9**—Pseudorandom test pattern, 511 bits in length
  - **2^11**—Pseudorandom test pattern, 2047 bits in length

  - **2^15**—Pseudorandom test pattern, 32,767 bits in length
  - **2^20**—Pseudorandom test pattern, 1,048,575 bits in length
  - **2^20-QRSS**—Pseudorandom QRSS test pattern, 1,048,575 bits in length
  - **2^23**—Pseudorandom test pattern, 8,388,607 bits in length
  - **alt-0-1**—Repetitive alternating test pattern of zeros and ones, 01010101…
- Specify the duration of the test in the range 1–1440 minutes.
- Example

  host1(config-controll)#**bert pattern 2^15 interval 20**

- Use the **no** version to stop the test that is running.

equipment loopback

- Use to enable or disable the router's ability to enter into a loopback initiated by a remote device connected on a channelized T3 interface.

NOTE: Remote loopback is available only on channelized T3 interfaces configured to use C-bit framing.

- Specify one of the following loopback options:
  - **customer**—Enables the router to enter into loopback when it receives an appropriate signal from the remote interface
  - **network**—Disables the router's ability to enter into loopback when it receives an appropriate signal from the remote interface
- Examples

  host1(config-controll)#**equipment customer loopback**
  host1(config-controll)#**equipment network loopback**

- Use the **no** version to disable the router's ability to be placed in loopback by the remote device.

loopback

- Use to configure a loopback.
- Specify one of the following loopback options.
  - **local**—Loops the data back toward the router; on supported line modules, also sends an alarm indication signal (AIS) out toward the network
  - **network**—Loops the data toward the network before the framer processes the data
  - **payload**—Loops the data toward the network after the framer processes the data

- **remote**—Sends a far end alarm code in the C-bit framing, as defined in ANSI T1.404, to notify the remote end to activate or (when you use the **no** version) deactivate the line loopback

---

NOTE: Remote loopback is available only on channelized T3 interfaces configured to use C-bit framing.

- Example

  host1(config-controll)#**loopback local**

- Use the **no** version to restore the default configuration, no loopback.

Testing at the T1 Layer

The T1 channel testing commands enable you to specify testing parameters for a single channel, multiple individual channels, ranges of channels, or any combination of the three types of specifications. For example:

host1(config-controll)#**t1 3,6-15,22,25-27 loopback local**

To enable testing at the T1 layer:

1. Configure one of the following loopback tests.

   - Set the loopback to **local** to test the line without connecting to the network.

     host1(config-controll)#**t1 2 loopback local**

   - Set the loopback to **network** to test the line connected to the network.

     host1(config-controll)#**t1 2 loopback network line**

   - Set the loopback to **remote-loopback** to enable acceptance of loopback commands issued from a remote router.

     host1(config-controll)#**t1 2 remote-loopback**

2. Configure the line to run bit error rate tests.

   host1(config-controll)#**t1 2 bert pattern 2^11 time 10 unframed**

t1 bert

- Use to enable bit error rate tests using the specified pattern on a T1 interface.
- Unlike other configuration commands, **bert** is not stored in NVRAM.
- Specify one of the following test patterns:

NOTE: The CT3/T3-F0 line module supports only the **2^11**, **2^15**, and **2^20-O153** options.

  - **0s**—Repetitive test pattern of all zeros, 00000...
  - **1s**—Repetitive test pattern of all ones, 11111...

  - **2^11**—Pseudorandom test pattern, 2047 bits in length
  - **2^15**—Pseudorandom test pattern, 32,767 bits in length
  - **2^20-O153**—Pseudorandom test pattern, 1,048,575 bits in length
  - **2^20-QRSS**—Pseudorandom QRSS test pattern, 1,048,575 bits in length
  - **2^23**—Pseudorandom test pattern, 8,388,607 bits in length
  - **alt-0-1**—Repetitive alternating test pattern of zeros and ones, 01010101...

NOTE: The BERT patterns supported when testing the T1 layer vary depending on the line module and I/O module assembly you are using.

- Specify the duration of the test in the range 1–1440 minutes.
- Optionally, specify the unframed keyword to overwrite the framing bits.
- Example

  host1(config-controll)#**t1 2 bert pattern 2^11 interval 10 unframed**

- Use the **no** version to stop the test that is running.

t1 loopback

- Use to configure a loopback.
- Specify one of the following options:

NOTE: The CT3/T3-F0 line module does not support the **remote line inband** option.

  - **local**—Loops the router output data back toward the router at the T1 framer; on supported line modules, also sends an alarm indication signal (AIS) out toward the network
  - **network { line | payload }**—Specify the **line** keyword to loop the data back toward the network before the T1 framer and automatically set a local loopback at the HDLC controllers. Specify the **payload** keyword to loop the payload data back toward the network at the T1 framer and automatically set a local loopback at the HDLC controllers.
  - **remote line fdl ansi**—Sends a repeating 16-bit ESF data link code word (00001110 11111111) to the remote end requesting that it enter into a network line loopback. Specify the **ansi** keyword to enable the remote line facilities data link (FDL) ANSI bit loopback on the T1 channel, according to the ANSI T1.403 Specification.
  - **remote line fdl bellcore**—Sends a repeating 16-bit ESF data link code word (00010010 11111111) to the remote end requesting that it enter into a network line loopback. Specify the **bellcore** keyword to enable the remote line facilities data link (FDL) Bellcore bit loopback on the T1 channel, per the Bellcore TR-TSY-000312 Specification.

    - **remote line inband—**Sends a repeating 5-bit inband pattern (00001) to the remote end requesting that it enter into a network line loopback
    - **remote payload** [**fdl**] [**ansi**]—Sends a repeating, 16-bit, ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload facilities data link (FDL) ANSI bit loopback on the T1 channel. You can optionally specify **fdl** and **ansi**.
- If you do not specify an option, the router will set a local loopback for the channel.
- Example

  host1(config-controll)#**t1 2 loopback local**

- Use the **no** version to deactivate loopback. If you specify the **remote** keyword, the **no** version sends the 16-bit ESF data link code word or inband pattern to deactivate the loopback at the remote end based on the last activate request sent to the remote end. If you do not specify the **remote** keyword, the **no** version clears the local loopback configuration.

t1 remote-loopback

- Use to enable the acceptance of loopback commands issued from a remote router.
- Example

  host1(config-controll)#**t1 2 remote-loopback**

- Use the **no** version to restore the factory default, which is to reject loopback commands issued from a remote router.

Monitoring Interfaces

From User Exec mode, use the following **show** commands to monitor and display the T3 interface, T1 interface, and HDLC serial data channel information:

- Monitor channelized T3 interfaces on a slot and port.

  host1#**show controllers t3 0/1**

- Monitor a T1 interface.

  host1#**show controllers t3 0/1:1**

- Monitor fractional T1 subchannels.

  host1#**show controllers t3 ft1**

- Monitor the state of the serial interface or a slot/port.

  host1#**show controllers t3 serial 0/1**

Setting a Baseline

You can set a statistics baseline for serial interfaces, subinterfaces, and/or circuits using the **baseline interface serial** command. Use the **delta** keyword with the **show** commands to display statistics with the baseline subtracted.

Displaying Counters and Time Intervals

Counters and time intervals are MIB statistics, which are defined in the following specifications:

- RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999)
- RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999)

The **show controllers t3 *slot/port* all** command displays the following information:

- T3 current interval counters—Counters for the current interval
- T3 last interval counters—Counters for the previous interval
- T3 24-hour total counters—Cumulative counters for the last 24 hours or since the interface was started
- The last 24 hours of 15-minute reporting intervals (96 intervals)

The **show controllers t3 *slot/port:*channel all** command displays the following information:

- T1 current interval counters—Counters for the current interval
- T1 last interval counters—Counters for the previous interval
- T1 24-hour total counters—Cumulative counters for the last 24 hours or since the interface was started
- The last 24 hours of 15-minute reporting intervals (96 intervals)

Output Filtering

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*, for details.

baseline interface serial

- Use to set a statistics baseline for serial interfaces.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the optional **delta** keyword with the **show interfaces serial** commands to view the baseline statistics.

- Example

  host1#**baseline interface serial 2/0:1/1**

- There is no **no** version.

show controllers t3 | t1

- Use to display data and MIB statistics for a T3 interface or a T1 channel.
- Use the **brief** keyword to display the administrative and operational status of all configured T3 interfaces, or to display abbreviated information for the specified T3 interface.
- For definitions of the MIB statistics for a T3 interface, see RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999).
- For definitions of the MIB statistics for a T1 channel, see RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999).
- Field descriptions for T3 interface (T1 channel not specified)
  - Description—Text description or alias if configured for the interface
  - ifAdminStatus—One of the following administrative states of the interface:
    - ifAdminUp—Interface is administratively enabled
    - ifAdminDown—Interface is administratively disabled
    - ifAdminTesting—Interface is administratively configured in a testing state
  - snmp trap link-status—*S*tatus of SNMP trapping (enabled or disabled)
  - alarms detected—One of the following T3 alarms:
    - No alarm present—No alarms present on the line
    - Rcv RAI Failure—Remote device is sending a far end alarm failure
    - Xmt RAI Failure—Local device is sending a far end alarm failure
    - Rcv AIS—Remote device is sending an alarm indication signal (AIS)
    - Xmt AIS—Local device is sending an AIS
    - Rcv LOF—Loss of one or more frames from the remote end
    - Rcv LOS—Loss of signal at the local end
    - Undefined line status—Indicates that the line is in an undefined state

NOTE: The alarms detected field does not appear for interfaces that you disabled in the software.

  - framing—Type of framing format
  - line code—Type of line code format
  - clock source—Type of clock source
  - cable length—Cable length, in feet

- Loopback—State of loopback for the controller: enabled or disabled. If loopback is enabled, one of the following states is displayed:
  - Diagnostic—Loops the data back toward the router and sends an AIS toward the network
  - Payload—Loops the data toward the network after the framer has processed the data
  - Line—Loops the data toward the network before the data reaches the framer
- MDL Transmit Path—Status of path transmission: active or not active
- MDL Transmit Test-Signal—Status of test signal: active or not active
- MDL Transmit Idle-Signal—Status of idle signal: active or not active
- Equipment Identification Code—eic string for MDL
- Line Identification Code—lic string for MDL
- Frame Identification Code—fic string for MDL
- Unit Identification Code—unit string for MDL
- Facility Identification Code—pfi string for MDL
- Port Code—port string for MDL
- Generator Number—generator string for MDL
- BERT test—Number of current test and total number of tests
  - Test interval—Length of the BERT test
  - status—Sync (controller is synchronized with remote device) or NoSync (controller is not synchronized with remote device)
  - Sync count—Number of times the pattern detector synchronized with the incoming data pattern
  - Received bit count—Number of bits received
  - Error bit count—Number of bits with errors
- Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
- Time elapse in current interval—Reported in 15-second intervals
- P-bit errored seconds—Number of errored seconds encountered by a T3 in the current interval
- P-bit severely errored seconds—Number of severely errored seconds encountered by a T3 in the current interval
- Severely errored frame seconds—Number of severely errored framing seconds encountered by a T3 in the current interval
- Unavailable seconds—Number of unavailable seconds encountered by a T3 in the current interval
- Line code violations—Number of line code violations encountered by a T3 in the current interval
- P-bit coding violations—Number of coding violations encountered by a T3 in the current interval

  - Line errored seconds—Number of line errored seconds encountered by a T3 in the current interval
  - C-bit coding violations—Number of C-bit coding violations encountered by a T3 in the current interval
  - C-bit errored seconds—Number of C-bit errored seconds encountered by a T3 in the current interval
  - C-bit severely errored seconds—Number of C-bit severely errored seconds encountered by a T3 in the current interval

- Example 1—In this example, a T3 interface is specified.

```
host1#show controllers t3 2/0

DS3 2/0
Description: toronto ct3 interface
ifAdminStatus = ifAdminDown
snmp trap link-status = enabled
No alarms detected
Framing is C-BIT, Line Code is B3ZS, Clock Source is Line
Cable Length is 0 ft
Loopback Disabled
MDL Transmit Path is not active
MDL Transmit Test-Signal is active
MDL Transmit Idle-Signal is not active
Equipment Identification Code is ERX-1400
Line Identification Code is Bldg 10
Frame Identification Code is null string
Unit Identification Code is 080001
Facility Identification Code is Site 25
Port Code is Port 0800
Generator Number is null string
Number of valid interval - 96
Time elapse in current interval - 861
Ds3 Current Interval Counters
P-bit errored seconds          = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds            = 0
Line code violations           = 0
P-bit coding violations        = 0
Line errored seconds           = 0
C-bit coding violations        = 0
C-bit errored seconds          = 0
C-bit severely errored seconds = 0
Ds3 Last Interval Counters
P-bit errored seconds          = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds            = 0
Line code violations           = 0
P-bit coding violations        = 0
Line errored seconds           = 0
C-bit coding violations        = 0
C-bit errored seconds          = 0
C-bit severely errored seconds = 0
Ds3 24 Hour Total Counters
P-bit errored seconds          = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds            = 0
Line code violations           = 0
```

```
P-bit coding violations       = 0
Line errored seconds          = 0
C-bit coding violations       = 0
C-bit errored seconds         = 0
C-bit severely errored seconds = 0
```

- Example 2—In this example, the **brief** keyword is specified.

```
host1#show controllers t3 brief

Interfaces                  ifAdminStatus   OperationalStatus
5/0(channelized)                up             up
5/1(channelized)                up             up
5/2(channelized)                up             down
5/3(channelized)                down           down
5/4(channelized)                down           down
5/5(channelized)                down           down
5/6(channelized)                down           down
5/7(channelized)                down           down
5/8(channelized)                down           down
5/9(channelized)                down           down
5/10(channelized)               down           down
5/11(channelized)               down           down
3/0(channelized)                down           down
3/1(channelized)                down           down
3/2(channelized)                down           down
4/0:1/1(unchannelized)          up             down
4/2:1/1(channelized)            up             lowerLayerDown
```

- Field descriptions for a T1 channel
  - Description—Text description or alias if configured for the interface
  - ifOperStatus—Physical state of the interface:
    - ifOperDown—Interface is not functioning
    - ifOperLowerLayerDown—Lower layer in the interface stack is not functioning
    - ifOperNotPresent—Module has been removed from the chassis
    - ifOperTesting—Interface is being tested
    - ifOperUp—Interface is functioning
  - Yellow Alarm detection—Status of yellow alarm detection: active or not active
  - Yellow Alarm generation—Status of yellow alarm generation: active or not active
  - snmp trap link-status—Status of SNMP trapping (enabled or disabled)
  - Framing—Type of framing format
  - Clock source—Type of clock source
  - Loopback state—Type of loopback (if enabled) and status: enabled or disabled
  - Last remote loopback request sent—None or deactivate
  - FDL—Status of FDL: standard configured or not configured
  - FDL Transmit Path—Status of path transmission: active or not active

- FDL Transmit Idle-Signal—Status of idle signal: active or not active
- FDL Transmit Test-Signal—Status of test signal: active or not active
- Equipment Identification Code—eic string for FDL
- Line Identification Code—lic string for FDL
- Frame Identification Code—fic string for FDL
- Unit Identification Code—unit string for FDL
- Facility Identification Code—pfi string for FDL
- Port Code—port string for FDL
- Generator Number—generator string for FDL
- BERT test—Number of current test and total number of tests
  - Test interval—Length of the BERT test
  - status—Sync (controller is synchronized with remote device) or NoSync (controller is not synchronized with remote device)
  - Sync count—Number of times the pattern detector synchronized with the incoming data pattern
  - Received bit count—Number of bits received
  - Error bit count—Number of bits with errors
- Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
- Time elapse in current interval—Statistics are reported in 15-minute intervals
- Errored seconds—Number of errored seconds encountered by a T1 in the current interval
- Severely errored seconds—Number of severely errored seconds encountered by a T1 in the current interval
- Severely errored frame seconds—Number of severely errored framing seconds encountered by a T1 in the current interval
- Unavailable seconds—Number of unavailable seconds encountered by a T1 in the current interval
- Clock slip seconds—Number of clock slips encountered by a T1 in the current interval
- Path code violations—Number of coding violations encountered by a T1 in the current interval
- Line errored seconds—Number of line errored seconds encountered by a T1 in the current interval
- Bursty errored seconds—Number of bursty errored seconds encountered by a T1 in the current interval
- Degraded minutes—Number of minutes that a T1 line is degraded
- Line code violations—Number of line code violations encountered by a T1 in the current interval

- Example 1—In this example, a T1 channel and the **brief** keyword are specified.

```
host1#show controllers t1 2/0:1 brief

DS3 2/0:1
ifOperStatus = ifOperUp
Yellow Alarm detection is active
Yellow Alarm generation is active
snmp trap link-status = disabled
Framing is D4, Line Code is Ami, Clock Source is Internal - Module
Allocated Ds0 time slot map = 0x0
Loopback Enabled - Diagnostic
Last Remote Loopback Request Sent - Deactivate
FDL is not configured
FDL Transmit Path-Id is not active
FDL Transmit Test-Signal is not active
FDL Transmit Idle-Signal is not active
Equipment Identification Code is the null string
Line Identification Code is the null string
Frame Identification Code is the null string
Unit Identification Code is the null string
Facility Identification Code is the null string
Port Code is the null string
Generator Number is the null string
BERT test - 2 in 23
Test Interval 1 minute(s), Complete
Sync count = 1
Received bit count = 92148912
Error bit count = 17
Number of valid interval - 90
Time elapse in current interval - 580
```

- Example 2—In this example, the **brief** keyword is specified for all T1 channels.

```
host1#show controllers t1 brief

Interfaces                 ifAdminStatus   OperationalStatus
5/0:1(framed)                   up              lowerLayerDown
5/0:2(framed)                   up              lowerLayerDown
5/0:3(framed)                   up              lowerLayerDown
5/0:4(framed)                   up              lowerLayerDown
5/0:5(framed)                   up              lowerLayerDown
5/0:6(framed)                   up              lowerLayerDown
...
5/2:26(framed)                  up              lowerLayerDown
5/2:27(framed)                  up              lowerLayerDown
5/2:28(framed)                  up              lowerLayerDown
```

- Example 3—In this example, a T1 channel is specified.

```
host1#show controllers t1 1/0:1

DS1 1/0:1
Description: toronto t1 channel
ifOperStatus = ifOperUp
Yellow Alarm detection is active
Yellow Alarm generation is active
snmp trap link-status = disabled
Framing is D4, Line Code is Ami, Clock Source is Internal - Module
Allocated Ds0 time slot map = 0x0
Last Remote Loopback Request Sent - Deactivate
FDL is not configured
FDL Transmit Path-Id is not active
FDL Transmit Test-Signal is not active
```

```
FDL Transmit Idle-Signal is not active
Equipment Identification Code is the null string
Line Identification Code is the null string
Frame Identification Code is the null string
Unit Identification Code is the null string
Facility Identification Code is the null string
Port Code is the null string
Generator Number is the null string
BERT test - 2 in 23
Test Interval 1 minute(s), Complete
Sync count = 1
Received bit count = 92148912
Error bit count = 17
Number of valid interval - 90
Time elapse in current interval - 580

Ds1 Current Interval Counters
Errored seconds = 0
Severely errored second = 0
Severely errored frame seconds = 0
Unavailable seconds = 0
Clock slip seconds = 0
Path code violations = 0
Line errored seconds = 0
Bursty errored seconds = 0
Degraded minutes = 0
Line code violations = 0

Ds1 Last Interval Counters
Errored seconds = 0
Severely errored second = 0
Severely errored frame seconds = 0
Unavailable seconds = 0
Clock slip seconds = 0
Path code violations = 0
Line errored seconds = 0
Bursty errored seconds = 0
Degraded minutes = 0
Line code violations = 0

Ds1 24 Hour Total Counters
Errored seconds = 25
Severely errored second = 7
Severely errored frame seconds = 25
Unavailable seconds = 0
Clock slip seconds = 6
Path code violations = 18
Line errored seconds = 0
Bursty errored seconds = 0
Degraded minutes = 0
Line code violations = 0
```

show controllers t3 ft1

- Use to display information about the state of a fractional T1 subchannel.
- Field descriptions
  - Description—Text description or alias if configured for the interface
  - ifOperStatus—Physical status of the interface
    - ifOperUp—Interface is functioning

        - ifOperTesting—Interface is being tested
        - ifOperNotPresent—Module has been removed from the chassis
        - ifOperDown—Interface is not functioning
    - snmp trap link-status of SNMP trapping (enabled or disabled)
    - Ds0 time slot map—Fractional T1 subchannel
    - Ds0 mode—Base data rate: either Nx56 or Nx64
- The **ft1** option displays the state of the serial interface.
- The optional *slot* and *port* parameters display information about a specific slot and port.
- Example

```
host1#show controllers t3 ft1

Ft1 Interface at 2/0:1/1
Description: toronto ft1 interface
ifOperStatus = ifOperLowerLayerDown
snmp trap link-status = disabled
Ds0 time slot map = 0x1
Ds0 mode = Nx64
```

show controllers t3 remote

- Use to display MIB statistics for the remote end of a channelized T3 interface configured for MDL or for the remote end of a T1 channel configured for FDL.
- Specify the **all** option to display detailed information for all 15-minute intervals.
- For definitions of the MIB statistics for a T3 interface, see RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999).
- For definitions of the MIB statistics for a T1 channel, see RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999).
- Field descriptions for a T3 interface
    - Far End MDL Carrier bit—Status of MDL configuration on remote device connected to T3 interface
        - set—MDL is configured for carrier mode
        - not set—MDL is not configured for carrier mode
    - Far End Equipment Identification Code—eic string sent by remote device for MDL
    - Far End Line Identification Code—lic string sent by remote device for MDL
    - Far End Frame Identification Code—fic string sent by remote device for MDL
    - Far End Unit Identification Code—unit string sent by remote device for MDL
    - Far End Facility Identification Code—pfi string sent by remote device for MDL
    - Far End Generator Number—generator string sent by remote device for MDL

  - Far End Port Number—port string sent by remote device for MDL
  - Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
  - Time elapse in current interval—Number of seconds that have passed in the 15-minute (900-second) interval
  - C-bit errored seconds—Number of C-bit errored seconds encountered by a T3 in the current interval
  - C-bit severely errored seconds—Number of C-bit severely errored seconds encountered by a T3 in the current interval
  - C-bit coding violations—Number of C-bit coding violations encountered by a T3 in the current interval
  - Unavailable seconds—Number of unavailable seconds encountered by a T3 in the current interval
  - Invalid seconds—Number of seconds when statistics were not collected
- Example—In this example, a T3 interface is specified.

```
host1#show controllers t3 5/0 remote

Far End MDL Carrier bit is not set
Far End Equipment Identification Code is the null string
Far End Line Identification Code is the null string
Far End Frame Identification Code is the null string
Far End Unit Identification Code is the null string
Far End Facility Identification Code is the null string
Far End Generator Number is the null string
Far End Port Number is the null string

Number of valid interval - 3
Time elapse in current interval - 756

Ds3 Current Interval Counters
C-bit errored seconds          = 0
C-bit severely errored seconds = 0
C-bit coding violations        = 0
Unavailable seconds            = 0
Invalid seconds                = 0
Ds3 Last Interval Counters
C-bit errored seconds          = 0
C-bit severely errored seconds = 0
C-bit coding violations        = 0
Unavailable seconds            = 0
Invalid seconds                = 0

Ds3 24 Hour Total Counters
C-bit errored seconds          = 1
C-bit severely errored seconds = 1
C-bit coding violations        = 330
Unavailable seconds            = 0
Invalid seconds                = 0
```

- Field descriptions for a T1 channel
  - DS1—Identifier of T1 channel
  - Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
  - Time elapse in current interval—Number of seconds that have passed in the 15-minute (900-second) interval
  - Far End FDL Carrier bit—Status of FDL configuration on remote device connected to T1 channel
    - set—FDL is configured for carrier mode
    - not set—FDL is not configured for carrier mode
  - Far End Equipment Identification Code—eic string sent by remote device for FDL
  - Far End Line Identification Code—lic string sent by remote device for FDL
  - Far End Frame Identification Code—fic string sent by remote device for FDL
  - Far End Unit Identification Code—unit string sent by remote device for FDL
  - Far End Facility Identification Code—pfi string sent by remote device for FDL
  - Far End Generator Number—generator string sent by remote device for FDL
  - Far End Port Number—port string sent by remote device for FDL
  - Errored seconds—Number of errored seconds encountered by a T1 in the current interval
  - Severely errored seconds—Number of severely errored seconds encountered by a T1 in the current interval
  - Severely errored frame seconds—Number of severely errored framing seconds encountered by a T1 in the current interval
  - Unavailable seconds—Number of unavailable seconds encountered by a T1 in the current interval
  - Clock slip seconds—Number of clock slips encountered by a T1 in the current interval
  - Path code violations—Number of coding violations encountered by a T1 in the current interval
  - Line errored seconds—Number of line errored seconds encountered by a T1 in the current interval
  - Bursty errored seconds—Number of bursty errored seconds encountered by a T1 in the current interval
  - Degraded minutes—Number of minutes that a T1 line is degraded
- Example—In this example, a T1 channel is specified.

```
host1#show controllers t1 10/1:1 remote

DS1 10/1:1
Number of valid interval - 0
Time elapse in current interval - 0
```

```
Far End FDL Carrier bit is not set
Far End Equipment Identification Code is the null string
Far End Line Identification Code is the null string
Far End Frame Identification Code is the null string
Far End Unit Identification Code is the null string
Far End Facility Identification Code is the null string
Far End Port Number is the null string
Far End Generator Number is the null string

DS1 Current Interval Counters
Errored seconds               = 0
Severely errored second       = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Clock slip seconds            = 0
Path code violations          = 0
Line errored seconds          = 0
Bursty errored seconds        = 0
Degraded minutes              = 0

DS1 24 Hour Total Counters
Errored seconds               = 0
Severely errored second       = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Clock slip seconds            = 0
Path code violations          = 0
Line errored seconds          = 0
Bursty errored seconds        = 0
Degraded minutes              = 0
```

show controllers t3 serial

- Use to display the state of the serial interface.
- Field descriptions
  - Description—Text description or alias if configured for the interface
  - ifOperStatus—Physical status of the interface
    - ifOperUp—Interface is functioning
    - ifOperTesting—Interface is being tested
    - ifOperNotPresent—Module has been removed from the chassis
    - ifOperDown—Interface is not functioning
  - snmp trap link-status of SNMP trapping (enabled or disabled)
  - Crc type checking—Size of the cyclic redundancy check (CRC)
  - Hdlc mru—Current size of the maximum receive unit (MRU)
  - Hdlc mtu—Current size of the maximum transmission unit (MTU)
  - Hdlc interface speed—Current line speed of the interface
  - Ds0 time slot map—T1 subchannel
  - Invert data disabled—Status of the data inversion feature
- The optional *slot* and *port* parameters display information about a specific slot and port.

- Use the *slot/port:channel/subchannel* option to display information about a specific interface.
- Example

```
host1#show controllers t3 serial

Serial Interface at 2/0:1/1
ifOperStatus = ifOperLowerLayerDown
snmp trap link-status = disabled
Crc type checking - CRC16
Hdlc mru = 9996
Hdlc mtu = 9996
Hdlc interface speed = 64000
Ds0 time slot map = 0x1
Invert data disabled, Ds0 mode = Nx64

Serial Interface at 2/1:1/1
ifOperStatus = ifOperLowerLayerDown
snmp trap link-status = disabled
Crc type checking - CRC16
Hdlc mru = 9996
Hdlc mtu = 9996
Hdlc interface speed = 64000
Ds0 time slot map = 0x1
Invert data disabled, Ds0 mode = Nx64

Found 2 Serial Interfaces
```

show interfaces serial

- Use to display information about the serial interfaces you specify.
- Field descriptions
  - Fractional Interface—Location of a channelized T1 or E1 interface
  - Description—Text description or alias if configured for the interface
  - ifOperStatus—Administrative status of the interface
    - ifOperUp—Interface is functioning
    - ifOperTesting—Interface is being tested
    - ifOperNotPresent—Module has been removed from the chassis
    - ifOperDown—Interface is not functioning
    - ifOperLowerDown—Lower layer in the interface stack is not functioning
  - snmp trap link-status—Enabled or disabled
  - Encapsulation—Layer 2 encapsulation display; options include: ppp, frame-relay ietf, mlppp, mlframe-relay ietf, hdlc
  - Crc type checking—Size of the CRC
  - Hdlc mru—Current size of the MRU
  - Hdlc mtu—Current size of the MTU
  - Hdlc interface speed—Current line speed of the interface
  - Hdlc idle-character—Current idle character
  - Invert data disabled—Status of the data inversion feature

- Ds0 time slot map—Channelized T1 or E1 channel group
- Ds0 mode—Nx56 or Nx64
- 5 minute input rate—Data rates based on the traffic received in the last five minutes
- 5 minute output rate—Data rates based on the traffic sent in the last five minutes
- Interface statistics
  - Packets received—Number of packets received on the interface
  - Bytes received—Number of bytes received on the interface
  - Errored packets received—Number of packets with errors received on the interface
  - Packets sent—Number of packets sent on the interface
  - Bytes sent—Number of bytes sent on the interface

- Errored packets sent—Number of packets with errors sent from the interface
- Example

```
host1#show interfaces serial 0/1:2 brief

Serial Interface at 0/1:2
Description: ottawa012 hdlc channel
ifOperStatus = ifOperUp
snmp trap link-status = disabled
Encapsulation hdlc
Crc type checking - CRC16
Hdlc mru = 1600
Hdlc mtu = 1600
Hdlc interface speed = 768000
Hdlc idle-character marks
Invert data disabled
Ds0 time slot map = 0xfff
Ds0 mode = Nx64

Serial Interface at 13/0:2
Description: ottawa013 hdlc channel
ifOperStatus = ifOperUp
snmp trap link-status = disabled
Crc type checking - CRC16
Hdlc mru = 1600
Hdlc mtu = 1600
Hdlc interface speed = 768000
Invert data disabled
Ds0 time slot map = 0xfff000
Ds0 mode = Nx64

Found 2 Serial Interfaces
```

Chapter 2
Configuring T3 and E3 Interfaces

Use the procedures described in this chapter to configure T3 and E3 interfaces on E-series routers.

This chapter contains the following sections:

- Overview on page 41
- Platform Considerations on page 43
- References on page 46
- Before You Configure an Interface on page 47
- Configuration Tasks on page 47
- Configuration Examples on page 55
- Testing Interfaces on page 56
- Monitoring Interfaces on page 59

Overview

Unchannelized T3 (DS3) and E3 interfaces are supported by the modules described in this chapter.

Throughout this chapter, interfaces on modules that provide ATM support are called T3/E3 ATM interfaces. Similarly, interfaces on modules that provide frame (HDLC) support are called T3/E3 frame interfaces.

This section describes the features of unchannelized T3/E3 interfaces. For information about configuring unchannelized T3 (DS3) interfaces over SONET/SDH, see *Chapter 4, Configuring Channelized OCx/STMx Interfaces*.

MDL Support

T3 interfaces on some line modules support maintenance data link (MDL) messages. For a list of the line modules that support MDL, see *ERX Module Guide*, *Appendix A*, *Module Protocol Support*.

You can use MDL messages to determine the status of a link and to display statistics for the remote end of a connection. MDL messages do not interfere with other data transmitted over the link.

MDL Standards

You can configure T3 interfaces to send MDL messages that comply with ANSI T1.107a-1990 Standard for Telecommunications—Digital Hierarchy – Supplement to Formats Specification (August 1990). MDL messages identify a particular link by sharing common codes for data such as the equipment identifier, line identifier, frame identifier, and unit.

Timeout of Received MDL Messages

When a line module receives an MDL message string, it stores the strings for a period of 10 seconds after the last message was received. If the line module does not receive another message of any type containing the same string within 10 seconds, it erases the local copy of the message.

Most MDL message strings are common to all three types of messages that can be transmitted: path identifications, idle signals, and test signals. Certain message strings, however, are unique to a particular message type. Table 6 briefly describes each MDL message string and indicates (with a ✔) the types of messages in which it can be sent.

Table 6: MDL Message Strings and Message Types

Message String	Description	Path Message	Idle Signal Message	Test Signal Message
eic	Equipment identification code	✔	✔	✔
fic	Frame identification code	✔	✔	✔
generator	Generator number	–	–	✔
lic	Line identification code	✔	✔	✔
pfi	Facility identification code	✔	–	–
port	Equipment port number	–	✔	–
unit	Unit identification code	✔	✔	✔

As long as another message of any type containing the same string is received within 10 seconds, the line module retains the local copy of the message string and resets the 10-second timer for that string.

For example, if a line module receives an MDL test signal message containing an eic string, and then receives a idle signal message within 10 seconds that also contains an eic string, it retains the local copy of the most recent eic string received and resets the 10-second timer for that message. However, if 10 seconds pass without the line module receiving a path identification, test signal, or idle signal message containing an eic string, the line module erases the local copy of the eic message string.

For message strings that are unique to a particular message type, the line module must receive another message of the same type containing this string in order to retain the local copy of the string and reset the timer. For example, if the line module receives a test signal message containing a generator string and does not receive another test signal message within 10 seconds, it will erase the local copy of the generator string.

Higher-Level Protocols

See *ERX Module Guide*, *Appendix A*, *Module Protocol Support* for information about the higher-level protocols that T3 and E3 interfaces support.

Platform Considerations

You can configure unchannelized T3 and unchannelized E3 interfaces on the following E-series routers:

- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

NOTE: The E120 router and the E320 router do not support configuration of unchannelized T3/E3 interfaces.

For detailed information about the modules that support unchannelized T3/E3 interfaces on ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that unchannelized T3/E3 modules support.

COCX-F3 Line Modules and Associated I/O Modules

ERX-7xx models, ERX-14xx models, and the ERX-310 router support the COCX-F3 line modules and associated I/O modules.

ERX-14xx models support up to twelve COCX-F3 line modules and twelve corresponding I/O modules, ERX-7xx models support up to five of these line modules and five corresponding I/O modules, and the ERX-310 router supports up to two of these line modules and two corresponding I/O modules. There are twelve physical T3/E3 (DS3) ports per I/O module. Each port uses two SMB connectors: one for the transmit (TX) connection and one for the receive (RX) connection.

COCX-F3 line modules and associated I/O modules support the following:

- Clocking
- Redundancy
- Frame Relay logical interface support
- Unique IP interface support for each PPP or Frame Relay PVC interface
- HDLC
- Fractional T3 (T3 only)
- Line speeds of 45 Mbps (T3) and 34 Mbps (E3)

OCx/STMx/DS3-ATM Line Modules and 4xDs3 ATM I/O Modules

ERX-7xx models, ERX-14xx models, and the ERX-310 router support the OCx/STMx/DS3-ATM line modules and 4xDS3 ATM I/O modules.

ERX-14xx models support up to twelve OCx/STMx/DS3-ATM line modules and twelve 4xDS3 ATM I/O modules, the ERX-7xx models support up to five of these line modules and five corresponding I/O modules, and the ERX-310 router supports up to two of these line modules and two corresponding I/O modules. There are four physical T3 (DS3) ports per I/O module. Each port uses two BNC connectors: one for the transmit (TX) connection and one for the receive (RX) connection.

OCx/STMx/DS3-ATM line modules pair with 4xDS3 ATM I/O modules to support the following:

- Clocking
- Redundancy
- Frame Relay logical interface support
- Unique IP interface support for each PPP or Frame Relay PVC interface
- Line speeds of 45 Mbps

CT3/T3-F0 Line Modules and CT3/T3 12 I/O Modules

ERX-7xx models, ERX-14xx models, and the ERX-310 router support the CT3/T3-F0 line modules and CT3/T3 12 I/O modules.

The CT3/T3-F0 line module and CT3/T3 12 I/O module support both channelized and unchannelized T3 operation. You can configure a mixture of channelized and unchannelized ports on these modules. To configure these modules to support unchannelized T3 operation, issue the **no channelized** command. (See *Configuration Tasks* on page 47.) For information about configuring channelized T3 ports, see *Chapter 1, Configuring Channelized T3 Interfaces*.

ERX-14xx models support up to twelve CT3/T3-F0 line modules and twelve CT3/T3 12 I/O modules, ERX-7xx models support up to five of these line modules and five corresponding I/O modules, and the ERX-310 router supports up to two of these line modules and two corresponding I/O modules. There are twelve physical T3 (DS3) ports per I/O module. Each port uses two SMB connectors: one for the transmit (TX) connection and one for the receive (RX) connection.

CT3/T3-F0 line modules and CT3/T3 12 I/O I/O modules to support the following:

- Clocking
- Redundancy
- Frame Relay logical interface support
- Unique IP interface support for each PPP or Frame Relay PVC interface
- Line speeds of 45 Mbps

Interface Stack

Figure 3 on page 45 shows the stack for T3 ATM interfaces. Figure 4 on page 45 shows the stack for T3 frame and E3 frame interfaces.

To configure a T3 ATM interface, first configure a T3 controller. To configure ATM parameters, see *JUNOSe Link Layer Configuration Guide, Chapter 1, Configuring ATM*.

To configure a T3 frame or E3 frame interface, first configure a T3 or E3 controller, and then configure a High-Speed Data Link Control (HDLC) data channel on the controller.

Figure 3: Stack for T3 ATM Interfaces

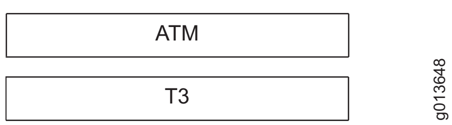
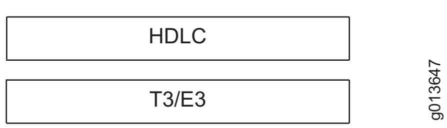


Figure 4: Stack for T3 Frame and E3 Frame Interfaces



NOTE: For a detailed description of interface types and specifiers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*. For information about interfaces, see *JUNOSe System Basics Configuration Guide, Chapter 1, Planning Your Network*.

Numbering Scheme

This section describes how to identify T3 and E3 interfaces.

A T3/E3 controller on an ATM or frame interface is identified using the *slot/port* format, where:

- *slot*—Number of the slot in which the line module resides in the chassis. In ERX-7xx models, line module slots are numbered 2-6 (slots 0 and 1 are reserved for SRP modules). In ERX-14xx models, line module slots are numbered 0–5 and 8–13 (slots 6 and 7 are reserved for SRP modules). In the ERX-310 router, the line module slots are numbered 0–2 (slot 0 is reserved for the SRP module).

- *port*—Number of the port on the I/O module. On the CT3/T3 12 I/O and E3-12 FRAME I/O modules, ports are numbered 0–11.

For information about installing line modules and I/O modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

References

For more information about T3 and E3 interfaces, consult the following resources:

- RFC 1661—The Point-to-Point Protocol (PPP) (July 1994)

- RFC 2364—PPP over AAL5 (July 1998)

- RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999)

- RFC 2516—Method for Transmitting PPP over Ethernet (PPPoE) (February 1998)

- RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5 (September 1999)

- ANSI T1.107a-1990 Standard for Telecommunications—Digital Hierarchy – Supplement to Formats Specification (August 1990)

For more information about bit error test (BERT) patterns, see:

- ITU O.151—Error performance measuring equipment operating at the primary rate and above (October 1992)

- ITU O.153—Basic parameters for the measurement of error performance at bit rates below the primary rate (October 1992)

- ANSI T1.404-1994 Standard for Telecommunications—Network-to-Customer – DS3 Metallic Interface Specification (1994)

Before You Configure an Interface

Before you configure a T3 or an E3 interface, verify that you have installed the line modules and I/O modules correctly.

You need the following information for each T3 controller:

- Framing type
- Clock source
- Cable length

You also need HDLC channel information, such as data inversion information, for interfaces that support HDLC.

Configuration Tasks

Configure a T3 interface by entering Global Configuration mode and performing the following tasks:

1. Configure a T3 controller.
2. (Optional) Configure MDL settings.
3. (Optional) Configure other settings for the interface.
4. Configure HDLC channels for T3 frame and E3 frame controllers.
5. (Optional) Configure fractional T3 for T3 frame controllers.
6. Use the appropriate **show** commands to verify your configuration.

E3 interface configuration tasks are identical to T3 interface configuration tasks, except that the CLI commands contain **e3** instead of **t3.**

For example, you configure an E3 controller with the **controller e3** command instead of the **controller t3** command.

Configuring a T3 or an E3 Controller

To configure a T3 or an E3 controller:

1. Select the T3 or E3 controller from Global Configuration mode.

   host1(config)#**controller t3 3/2**

2. Enable the T3 or E3 controller.

   host1(config-controll)#**no shutdown**

3. (CT3/T3-F0 line module only) Enable unchannelized operation for this controller.

   host1(config-controll)#**no channelized**

channelized

- Use to enable channelized T3 operation on an interface of a CT3/T3-F0 line module.
- Example

  host1(config-controll)#**channelized**
- Use the **no** version to enable unchannelized T3 operation on an interface for a CT3/T3-F0 line module.

controller e3

- Use to specify an E3 controller in *slot/port* format.
  - *slot*—Number of the slot in which the line module resides in the chassis
  - *port*—Number of the port on the I/O module
- Example

  host1(config)#**controller e3 3/2**
- There is no **no** version.

controller t3

- Use to specify a T3 controller in *slot/port* format.
  - *slot*—Number of the slot in which the line module resides in the chassis
  - *port*—Number of the port on the I/O module
- Example

  host1(config)#**controller t3 0/1**
- There is no **no** version.

shutdown

- Use to disable a T3 or an E3 controller.
- The T3 or E3 interface is disabled by default.
- Example

  host1(config-controll)#**shutdown**
- Use the **no** version to restart a disabled interface.

Configuring MDL Messages

You can configure a T3 interface to send MDL messages. MDL messages are supported only when T3 framing uses C-bit parity, the default setting.

To configure a T3 interface to send MDL messages:

1. Specify a T3 interface.

   host1(config)#**controller t3 8/0**

2. (Optional) Configure the interface to operate in an MDL carrier environment.

   host1(config-controll)#**mdl carrier**

3. Specify the MDL messages.

   host1(config-controll)#**mdl string eic "ERX-1410"**
   host1(config-controll)#**mdl string fic "FG786"**
   host1(config-controll)#**mdl string lic “Bldg 10"**
   host1(config-controll)#**mdl string pfi "Site 25"**
   host1(config-controll)#**mdl string port 0800**

4. Enable transmission of MDL messages.

   host1(config-controll)#**mdl transmit path-id**
   host1(config-controll)#**mdl transmit idle-signal**
   host1(config-controll)#**mdl transmit test-signal**

mdl carrier

- Use to specify that an interface is used in the carrier environment.
- Example

  host1(config-controll)#**mdl carrier**

- Use the **no** version to restore the default situation, in which the interface does not operate in the carrier environment.

mdl string

- Use to specify an MDL message.
- Example

  host1(config-controll)#**mdl string port 0800**

- Use the **no** version to restore the default value to the specified MDL message or to all MDL messages.

mdl transmit

- Use to enable transmission of MDL messages.
- Specify the keyword **path-id** to transmit path identifications every second.
- Specify the keyword **idle-signal** to send idle signals every second.
- Specify the keyword **test-signal** to transmit test signals every second.

- Example

  host1(config-controll)#**mdl transmit test-signal**

- Use the **no** version to disable transmission of the specified MDL message or all MDL messages.

Optional Tasks

The following configuration tasks are optional for T3 and E3 interfaces:

- Specify the cable length (T3 only).
- Change the clock source.
- Change the framing format.
- Enable cell scrambling (ATM interfaces only).
- Assign a text description or an alias to the interface.

cablelength

- Use to adjust the transmit power appropriate to the length of a T3 cable.
- Specify a cable length in the range 1–450 feet.
- The router supports two transmit powers, one for a cable length between 1–225 feet and another for a cable length between 226–450 feet. Therefore, it is not necessary to know the exact size of your cable. You only need to know if the cable size is greater than 225 feet. For example, if your cable size exceeds 225 feet, specify any number greater than 225 and less than 451.
- Example

  host1(config-controll)#**cablelength 300**

- Use the **no** version to restore the default, 0 feet.

clock source

- Use to configure the transmit clock source for a T3 or E3 line.
- Use a transmit clock on the line's receive data stream, except in rare cases such as back-to-back router tests. When performing back-to-back router tests, configure one end of the line as **internal** and the other end as **line**.
- Specify the keyword **line** to use a transmit clock on the line's receive data stream.
- Specify the keywords **internal module** to use the line module's internal clock.
- Specify the keywords **internal chassis** to use the router's clock.
- Example

  host1(config-controll)#**clock source internal module**

- Use the **no** version to revert to the default, **line**.

description

- Use to assign a text description or an alias to a T3 or E3 interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show controllers t3** or **show controllers e3** command to display the text description.
- Example

  host1(config-controll)#**description westford t3 interface**

- Use the **no** version to remove the text description or alias.

ds3-scramble

- Use to enable cell scrambling in a T3 ATM interface.
- Example

  host1(config-controll)#**ds3-scramble**

- Use the **no** version to turn off cell scrambling on the interface.

e3-scramble

- Use to enable cell scrambling in an E3 ATM interface.
- Example

  host1(config-controll)#**e3-scramble**

- Use the **no** version to turn off cell scrambling on the interface.

framing

- Use to configure the framing format for a T3 or E3 line.
- For a T3 line, you must specify one of the following:
  - T3 FRAME—**c-bit** or **m23** (the default is **c-bit**)
  - T3 ATM—**cbitadm**, **cbitplcp**, **m23adm**, or **M23plcp** (the default is **cbitplcp**)
- For an E3 line, you must specify one of the following:
  - E3 FRAME—**g751** or **g832** (the default is **g751**)
- Choose a framing format that is compatible with the framing format of the network device at the other end of the line.
- Example

  host1(config-controll)#**framing m23**

- Use the **no** version to restore the default value.

Configuring Fractional T3

You can configure fractional T3 on T3 frame interfaces. E3 frame interfaces do not support fractional E3.

Fractional T3 is a portion of a T3 transmission service and provides a set of lines with a speed that is greater than T1 (1.544 Mbps), but less than T3 (44.736 Mbps).

To configure fractional T3:

1. Set the DSU mode for the lines.
2. Set the speed of the fractional T3 lines.
3. Enable scrambling of the payload.

CAUTION: Complete all three steps at the same time. Otherwise, the interface might drop packets unexpectedly.

dsu bandwidth

- Use to set the speed for the fractional T3 lines.
- If you issue this command, be sure to issue the **dsu mode** and **scramble** commands. Otherwise, the interface might drop packets unexpectedly.
- The router offers a set of speeds in increments that depend on the DSU mode you specify. The actual speed of the fractional T3 lines will be the value closest to the fractional bandwidth you specify.
- Example

  host1(config-controll)#**dsu bandwidth 10000**

- Use the **no** version to clear the bandwidth.
- If you issue the **no** version, be sure to issue the **no dsu mode** and **no scramble** commands. Otherwise, the interface might drop packets unexpectedly.

dsu mode

- Use to set the DSU mode for the lines.
- Specify 0 for Digital Link mode or 2 for Larscom mode.
- If you issue this command, be sure to issue the **dsu bandwidth** and **scramble** commands. Otherwise, the interface might drop packets unexpectedly.
- Example

  host1(config-controll)#**dsu mode 0**

- Use the **no** version to clear the DSU mode.
- If you issue the **no** version, be sure to issue the **no dsu bandwidth** and **no scramble** commands. Otherwise, the interface might drop packets unexpectedly.

scramble

- Use to enable cell scrambling on a T3 frame interface.
- If you issue this command, be sure to issue the **dsu mode** and **dsu bandwidth** commands. Otherwise, the interface might drop packets unexpectedly.
- Example

  host1(config-controll)#**scramble**

- Use the **no** version to turn off cell scrambling on the interface.
- If you issue the **no** version, be sure to issue the **no dsu mode** and **no dsu bandwidth** commands. Otherwise, the interface might drop packets unexpectedly.

Configuring an HDLC Channel

You must configure an HDLC channel for each T3 frame or E3 frame controller.

To configure an HDLC channel, configure a serial interface (for example, HDLC channel in slot 0, 1).

host1(config)#**interface serial 0/1**

Optional Tasks

The following configuration tasks are optional when you configure an HDLC channel on a T3/E3 frame interface:

- Configure the cyclic redundancy check (CRC).
- Configure the HDLC idle character.
- Enable data inversion on the interface.
- Set the time interval for monitoring bit and packet rates.
- Set the maximum receive unit (MRU).
- Set the maximum transmit unit (MTU).
- Assign a text description or an alias to the serial interface.

crc

- Use to configure the size of the CRC.
- Specify the number of bits per frame (16 or 32) that are used to calculate the frame check sequence (FCS). Both the sender and receiver must use the same setting.
- The CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data.
- A 32-bit CRC should be used to protect longer streams at faster rates and, therefore, provide better ongoing error detection.

- Example

  host1(config-if)#**crc 32**

- Use the **no** version to restore the default value, 16.

idle-character

- Use to configure the HDLC idle character.
- The idle character is sent between HDLC packets.
- Specify one of the following idle characters:
  - **flags—**Sets the idle character to 0x7E
  - **marks**—Sets the idle character to 0xFF
- Example

  host1(config-if)#**idle-character marks**

- Use the **no** version to restore the default value, 0x7E (flags).

interface serial

- Use to configure a serial interface in the *slot/port* format.
  - *slot*—Number of the slot in which the line module resides in the chassis
  - *port*—Number of the port on the I/O module
- Example

  host1(config)#**interface serial 3/0**

- Use the **no** version to disable the interface.

invert data

- Use to enable data stream inversion for the interface.
- Enable data stream inversion only if it is turned on at the other end of the line.
- Example

  host1(config-if)#**invert data**

- Use the **no** version to disable the feature.

load-interval

- Use to set the time interval at which the router calculates bit and packet rate counters.
- Choose a multiple of 30 seconds, in the range 30–300 seconds.
- Example

  host1(config-if)#**load-interval 90**

- Use the **no** version to restore the default value, 300 seconds.

mru

- Use to configure the MRU size for the interface.
- Specify a value in the range 4–9996 bytes.
- Coordinate this value with the network administrator on the other end of the line.
- If you set this parameter to a different value for another protocol, such as IP, the router uses the lower value. This could produce unexpected behavior in your network.
- Example

  host1(config-if)#**mru 1500**

- Use the **no** version to restore the default, 1600 bytes.

mtu

- Use to configure the MTU size for the interface.
- Specify a value in the range 4–9996 bytes.
- Coordinate this value with the network administrator on the other end of the line.
- If you set this parameter to a different value for another protocol, such as IP, the router uses the lower value. This could produce unexpected behavior in your network.
- Example

  host1(config-if)#**mtu 1500**

- Use the **no** version to restore the default, 1600 bytes.

serial description

- Use to assign a text description or an alias to a serial HDLC interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show interfaces serial** command to display the text description.
- Example

  host1(config-if)#**serial description boston09 hdlc channel**

- Use the **no** version to remove the text description or alias.

Configuration Examples

To configure a T3 interface, start at the Global Configuration mode, and issue the following commands:

host1(config)#**controller t3 0/1**
host1(config-controll)#**no shutdwon**
host1(config-controll)#**framing c-bit**

```
host1(config-controll)#clock source internal module
host1(config-controll)#cablelength 220
host1#exit
```

To configure an E3 interface, use the **controller e3** command in place of the **controller t3** command.

To configure HDLC channels on a T3 serial interface, issue the following commands:

```
host1(config)#controller t3 10/0
host1(config-controll)#exit
host1(config)#interface serial 10/0
host1(config-subif)#encapsulation ppp
host1(config-subif)#ip address 192.32.10.2 255.255.255.0
```

To configure fractional T3 on an interface, issue the following commands:

```
host1(config)#controller t3 10/0
host1(config-controll)#dsu mode 0
host1(config-controll)#dsu bandwidth 10000
host1(config-controll)#scramble
```

Testing Interfaces

Testing interfaces allows you to troubleshoot problems and to check the quality of links at various layers in the interface stack. The router supports the following test options:

- Transmission of BERT patterns to remote devices
- Local loopback—Loops the data back toward the router; on supported line modules, also sends an alarm indication signal (AIS) out toward the network
- Network loopback—Loops the data toward the network before the data reaches the frame
- Payload loopback—Loops the data toward the network after the framer processes the data
- Remote loopback—Provides the ability to:
  - Request that remote devices enter into loopback
  - Be placed in loopback by remote devices

Sending BERT Patterns

The router can send BERT patterns from different layers in the interface stack on frame-based T3 interfaces.

For a list of the modules that support bit error rate tests, see *ERX Module Guide*, *Appendix A*, *Module Protocol Support*.

To send BERT patterns:

1. Select a controller.

   host1(config)#**controller t3 3/2**

2. Configure a specific layer in the interface to generate BERT patterns.

   host1(config-controll)#**bert pattern 2^11 interval 10**

   For information about BERT patterns, see *References* on page 46.

bert

- Use to enable bit error rate tests using the specified pattern on a T3 interface.
- Unlike other configuration commands, **bert** is not stored in NVRAM.
- Specify one of the following test patterns:
  - **0s**—Repetitive test pattern of all zeros, 00000...
  - **1s**—Repetitive test pattern of all ones, 11111...
  - **2^9**—Pseudorandom test pattern, 511 bits in length
  - **2^11**—Pseudorandom test pattern, 2047 bits in length
  - **2^15**—Pseudorandom test pattern, 32,767 bits in length
  - **2^20**—Pseudorandom test pattern, 1,048,575 bits in length
  - **2^20-QRSS**—Pseudorandom QRSS test pattern, 1,048,575 bits in length
  - **2^23**—Pseudorandom test pattern, 8,388,607 bits in length
  - **alt-0-1**—Repetitive alternating test pattern of zeros and ones, 01010101...
- Specify the duration of the test in the range 1–1440 minutes.
- Example

  host1(config-controll)#**bert pattern 2^11 interval 10**

- Use the **no** version to stop the test that is running.

Enabling Local, Network, and Payload Loopback

To enable local, network, or payload loopback testing of a T3 or E3 line, use the **clock source** and **loopback** commands from Controller Configuration mode.

1. Change the clock source to internal.

   host1(config-controll)#**clock source internal module**

2. Specify a loopback.

   host1(config-controll)#**loopback local**

Enabling Remote Loopback

You can enable remote loopback capability on frame-based T3 interfaces configured to use C-bit framing. Remote loopback is *not* supported on E3 ATM, E3 FRAME, and T3 ATM interfaces.

For a list of the modules that support remote loopback, see *ERX Module Guide*, *Appendix A*, *Module Protocol Support*.

To enable remote loopback:

1. Change the clock source to internal.

   host1(config-controll)#**clock source internal module**

2. Ensure that the line is configured to use C-bit framing, which is the default for frame-based T3 interfaces.

   host1(config-controll)#**framing c-bit**

3. Configure one of the following loopback tests:

   - Set the loopback to **remote** to request that a remote device connected on a T3 interface enter into a loopback.

     host1(config-controll)#**loopback remote**

   - Configure the T3 interface to enable or disable the ability to enter into a loopback initiated by a remote device, as follows:

     - Issue the **equipment customer loopback** command to enable the router to enter into loopback when it receives an appropriate signal from the remote device.

       host1(config-controll)#**equipment customer loopback**

     - Issue the **equipment network loopback** command to disable the ability to enter into loopback initiated by a remote device.

       host1(config-controll)#**equipment network loopback**

equipment loopback

- Use to enable or disable the router's ability to enter into a loopback initiated by a remote device connected on a T3 interface.

NOTE: Remote loopback is available only on frame-based T3 interfaces configured to use C-bit framing.

- Specify one of the following loopback options:
  - **customer**—Enables the router to enter into loopback when it receives an appropriate signal from the remote interface
  - **network**—Disables the router's ability to enter into loopback when it receives an appropriate signal from the remote interface

- Examples

  host1(config-controll)#**equipment customer loopback**
  host1(config-controll)#**equipment network loopback**

- Use the **no** version to disable the router's ability to be placed in loopback by the remote device.

loopback

- Use to configure a loopback.
- Specify one of the following loopback options:
  - **local**—Loops the data back toward the router; on supported line modules, also sends an alarm indication signal (AIS) out toward the network
  - **network**—Loops the data toward the network before the framer processes the data
  - **payload**—Loops the data toward the network after the framer processes the data
  - **remote**—Sends a far end alarm code in the C-bit framing, as defined in ANSI T1.404, to notify the remote end to activate or (when you use the **no** version) deactivate the line loopback

NOTE: Remote loopback is available only on frame-based T3 interfaces configured to use C-bit framing.

- Example

  host1(config-controll)#**loopback local**

- Use the **no** version to restore the default configuration, no loopback.

Monitoring Interfaces

From User Exec mode, use the following **show** commands to monitor and display the T3 or E3 interface information:

host1#**show controllers t3 0/1**
host1#**show controllers e3 3/2**

Setting a Baseline

You can set a statistics baseline for serial interfaces using the **baseline interface serial** command. Use the **delta** keyword with the **show** commands to display statistics with the baseline subtracted.

Displaying Counters and Time Intervals

Counters and time intervals are MIB statistics, which are defined in RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999).

The **show controllers t3 *slot/port* all** command displays the following interface information:

- Status information
- T3 current interval counters—Displays the counters for the current interval
- T3 last interval counters—Displays the counters for the previous interval
- T3 24-hour total counters—Displays the cumulative counters for the last 24-hours or since the interface was started
- The last 24-hours of 15-minute reporting intervals (96 intervals)

The **show controllers e3 *slot/port* all** command displays identical information for an E3 controller (except where noted).

Output Filtering

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*.

baseline interface serial

- Use to set a statistics baseline for serial interfaces.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the optional **delta** keyword with the **show interfaces serial** commands to view the baseline statistics.
- Example

  host1#**baseline interface serial 2/0**
- There is no **no** version.

show controllers e3
show controllers t3

- Use to display the parameters and MIB statistics on an interface.
- Use the **brief** keyword to display the administrative and operational status of all configured T3 or E3 interfaces, or to display abbreviated information for the specified T3 or E3 interface.
- For definitions of the MIB statistics, see RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999)

- Field descriptions
  - Description—Text description or alias if configured for the interface
  - ifAdminStatus—One of the following administrative states of the interface:
    - ifAdminUp—Interface is administratively enabled
    - ifAdminDown—Interface is administratively disabled
    - ifAdminTesting—Interface is administratively configured in a testing state
  - snmp trap link-status—Status of SNMP trapping (enabled or disabled)
  - alarms detected—One of the following T3 alarms (not applicable for E3):
    - No alarm present—No alarms present on the line
    - Rcv RAI Failure—Remote device is sending a far end alarm failure
    - Xmt RAI Failure—Local device is sending a far end alarm failure
    - Rcv AIS—Remote device is sending an alarm indication signal (AIS)
    - Xmt AIS—Local device is sending an AIS
    - Rcv LOF—Loss of one or more frames from the remote end
    - Rcv LOS—Loss of signal at the local end

NOTE: The alarms detected field does not appear for interfaces that you disabled in the software.

  - framing—Type of framing format
  - line code—Type of line code format
  - clock source—Type of clock source
  - cable length—Cable length, in feet (this field is not present for E3 controllers)
  - Loopback—State of loopback for the controller: enabled or disabled. If loopback is enabled, one of the following states is displayed:
    - Diagnostic—Data loops back toward the router and sends an alarm AIS toward the network
    - Payload—Data loops toward the network after the framer has processed the data
    - Line—Data loops toward the network before the data reaches the framer
  - loopback state—State of loopback for the controller: enabled or disabled
  - DSU mode—Mode of the fractional T3 lines: Digital Link mode or Larscom mode
  - DSU bandwidth—Speed of the fractional T3 lines
  - DSU scramble—Status of scrambling for fractional T3: on or off
  - MDL Transmit Path—Indicates whether the transmission is active or not active (T3 only)

- MDL Transmit Test-Signal—Indicates if the transmission is active or not active (T3 only)
- MDL Transmit Idle-Signal—Indicates if the transmission is active or not active (T3 only)
- Equipment Identification Code—eic string for MDL (T3 only)
- Line Identification Code—lic string for MDL (T3 only)
- Frame Identification Code—fic string for MDL (T3 only)
- Facility Identification Code—fic string for MDL (T3 only)
- Equipment Port—port string for MDL (T3 only)
- Unit Identification Code—unit string for MDL (T3 only)
- Facility Identification Code—pfi string for MDL (T3 only)
- Port Code—port string for MDL (T3 only)
- Generator Number—generator string for MDL (T3 only)
- BERT test—Number of current test and total number of tests (T3 only)
  - Test interval—Length of the BERT test
  - status—Sync (controller is synchronized with remote device) or NoSync (controller is not synchronized with remote device)
  - Sync count—Number of times the pattern detector synchronized with the incoming data pattern
  - Received bit count—Number of bits received
  - Error bit count—Number of bits with errors
- Number of valid intervals—Number of 15-minute intervals since the T3 or E3 module was last powered on or reset
- Time elapse in current interval—Number of seconds that have passed in the 15-minute (900 second) interval
- Errored seconds—Number of errored seconds encountered by an E3 (not applicable for T3) in the current interval (this field is not present for T3 controllers)
- P-bit errored seconds—Number of errored seconds encountered by a T3 (not applicable for E3) in the current interval (this field is not present for E3 controllers)
- Severely errored seconds—Number of severely errored seconds encountered by an E3 (not applicable for T3) in the current interval (this field is not present for T3 controllers)
- P-bit severely errored seconds—Number of severely errored seconds encountered by a T3 (not applicable for E3) in the current interval (this field is not present for E3 controllers)
- Severely errored frame seconds—Number of severely errored framing seconds encountered by a T3 or E3 in the current interval
- Unavailable seconds—Number of unavailable seconds encountered by a T3 or E3 in the current interval

  - Line code violations—Number of line code violations encountered by a T3 or E3 in the current interval
  - P-bit coding violations—Number of coding violations encountered by a T3 (not applicable for E3) in the current interval (this field is not present for E3 controllers)
  - Coding violations—Number of coding violations encountered by an E3 (not applicable for T3) in the current interval (this field is not present for T3 controllers)
  - Line errored seconds—Number of line errored seconds encountered by a T3 or E3 in the current interval
  - C-bit coding violations—Number of C-bit coding violations encountered by a T3 (not applicable for E3) in the current interval (this field is not present for E3 controllers)
  - C-bit errored seconds—Number of C-bit errored seconds encountered by a T3 (not applicable for E3) in the current interval (this field is not present for E3 controllers)
  - C-bit severely errored seconds—Number of C-bit severely errored seconds encountered by a T3 (not applicable for E3) in the current interval (this field is not present for E3 controllers)

- Example 1

```
host1#show controllers t3 2/0

DS3 2/0
Description: boston09 hdlc channel
ifAdminStatus = ifAdminDown
snmp trap link-status = enabled
No alarms detected
Framing is C-BIT, Line Code is B3ZS, Clock Source is Line
Cable Length is 0 ft
Loopback Disabled
DSU Mode is Larscom
DSU Bandwidth is 4000
DSU Scrambler is off
MDL Transmit Path is not active
MDL Transmit Test-Signal is active
MDL Transmit Idle-Signal is not active
Equipment Identification Code is ERX-1400
Line Identification Code is Bldg 10
Frame Identification Code is null string
Unit Identification Code is 080001
Facility Identification Code is Site 25
Port Code is Port 0800
Generator Number is null string

Number of valid interval - 96
Time elapse in current interval - 861

Ds3 Current Interval Counters
P-bit errored seconds          = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds            = 0
Line code violations           = 0
P-bit coding violations        = 0
Line errored seconds           = 0
```

```
C-bit coding violations       = 0
C-bit errored seconds         = 0
C-bit severely errored seconds = 0

Ds3 Last Interval Counters
P-bit errored seconds         = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Line code violations          = 0
P-bit coding violations       = 0
Line errored seconds          = 0
C-bit coding violations       = 0
C-bit errored seconds         = 0
C-bit severely errored seconds = 0
Ds3 24 Hour Total Counters
P-bit errored seconds         = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Line code violations          = 0
P-bit coding violations       = 0
Line errored seconds          = 0
C-bit coding violations       = 0
C-bit errored seconds         = 0
C-bit severely errored seconds = 0
```

- Example 2—In this example, the **brief** keyword is specified.

```
host1#show controllers t3 brief

Interfaces                 ifAdminStatus   OperationalStatus
5/0(channelized)               up              up
5/1(channelized)               up              up
5/2(channelized)               up              down
5/3(channelized)               down            down
5/4(channelized)               down            down
5/5(channelized)               down            down
5/6(channelized)               down            down
5/7(channelized)               down            down
5/8(channelized)               down            down
5/9(channelized)               down            down
5/10(channelized)              down            down
5/11(channelized)              down            down
3/0(channelized)               down            down
3/1(channelized)               down            down
3/2(channelized)               down            down
4/0:1/1(unchannelized)         up              down
4/2:1/1(channelized)           up              lowerLayerDown
```

show controllers t3 remote

- Use to display MIB statistics for the remote end of a T3 interface configured for MDL.
- Specify the **all** option to display detailed information for all 15-minute intervals.
- For definitions of the MIB statistics for a T3 interface, see RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999).

- Field descriptions
  - Far End MDL Carrier bit—Status of MDL configuration on remote device connected to T3 interface
    - set—MDL is configured for carrier mode
    - not set—MDL is not configured for carrier mode
  - Far End Equipment Identification Code—eic string sent by remote device for MDL
  - Far End Line Identification Code—lic string sent by remote device for MDL
  - Far End Frame Identification Code—fic string sent by remote device for MDL
  - Far End Unit Identification Code—unit string sent by remote device for MDL
  - Far End Facility Identification Code—pfi string sent by remote device for MDL
  - Far End Generator Number—generator string sent by remote device for MDL
  - Far End Port Number—port string sent by remote device for MDL
  - Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
  - Time elapse in current interval—Number of seconds that have passed in the 15-minute (900-second) interval
  - C-bit errored seconds—Number of C-bit errored seconds encountered by a T3 in the current interval
  - C-bit severely errored seconds—Number of C-bit severely errored seconds encountered by a T3 in the current interval
  - C-bit coding violations—Number of C-bit coding violations encountered by a T3 in the current interval
  - Unavailable seconds—Number of unavailable seconds encountered by a T3 in the current interval
  - Invalid seconds—Number of seconds when statistics were not collected
- Example—This example specifies a T3 interface.

```
host1#show controllers t3 5/0 remote

Far End MDL Carrier bit is not set
Far End Equipment Identification Code is the null string
Far End Line Identification Code is the null string
Far End Frame Identification Code is the null string
Far End Unit Identification Code is the null string
Far End Facility Identification Code is the null string
Far End Generator Number is the null string
Far End Port Number is the null string

Number of valid interval - 3
Time elapse in current interval - 756

Ds3 Current Interval Counters
C-bit errored seconds         = 0
C-bit severely errored seconds = 0
```

```
C-bit coding violations       = 0
Unavailable seconds           = 0
Invalid seconds               = 0

Ds3 Last Interval Counters
C-bit errored seconds         = 0
C-bit severely errored seconds = 0
C-bit coding violations       = 0
Unavailable seconds           = 0
Invalid seconds               = 0

Ds3 24 Hour Total Counters
C-bit errored seconds         = 1
C-bit severely errored seconds = 1
C-bit coding violations       = 330
Unavailable seconds           = 0
Invalid seconds               = 0
```

Chapter 3

Configuring Unchannelized OCx/STMx Interfaces

This chapter provides information you need to configure unchannelized SONET/SDH interfaces on E-series routers.

This chapter contains the following sections:

- Overview on page 67
- Platform Considerations on page 71
- References on page 78
- Configuration Tasks on page 78
- Testing Interfaces on page 89
- Monitoring SONET/SDH Interfaces on page 91

Overview

SONET/SDH interfaces are supported by the modules described in this chapter. This section describes features that are available with SONET/SDH interfaces.

APS and MSP

E-series routers support Automatic Protection Switching (APS) and Multiplex Section Protection (MSP) on selected I/O modules that provide SONET/SDH connections. This feature provides a redundant connection if a primary SONET/SDH connection fails.

For a list of I/O modules that support APS/MSP, see *ERX Module Guide*, *Appendix A*, *Module Protocol Support*.

NOTE: The E120 router and the E320 router do not support APS/MSP.

I/O modules that support APS/MSP have some ports designated for primary operation and other ports designated for redundant operation. For APS/MSP to work correctly, you must provide connections from a primary port and a corresponding redundant port to the remote device. The remote device must also support APS/MSP.

You configure a *working interface* on the primary port and a corresponding *protect interface* on the redundant port of the I/O module. The working interface provides the primary connection, and the protect interface provides the redundant connection.

The router sends and receives data through both interfaces; however, in normal operation, only the signal on the working interface is used. If the signal on the primary interface fails, the router can use the signal on the protect interface. The process by which the router switches to the protect interface is called *switchover*.

When you configure APS/MSP, you must assign a working interface and a corresponding protect interface to a unique group. This group establishes the relationship between the interfaces. Within the group, each interface is identified by an APS/MSP *channel number*. For information about identifying the channel number, see *Numbering Scheme* on page 76.

You must pair a working interface and its corresponding protect interface on an I/O module to form a valid linear APS 1 + 1 group. For example, on an I/O module that provides four working (primary) ports and four protect (redundant) ports, the working interface ports are numbered 0–3, and the protect interface ports are numbered 4–7. Table 7 lists the pairings required to form four valid APS 1 + 1 groups on this I/O module. Each working/protect port pair (for example, port 0 and port 4) forms a valid APS 1 + 1 group.

Table 7: Sample Pairings for Valid APS/MSP Groups

Pair This Working Port	With This Protect Port
0	4
1	5
2	6
3	7

Automatic Switchover

Provided you have not issued the **aps lockout** command for the protect interface, the router switches over to the protect interface if it detects signal failure. You can set the SONET/SDH alarms that determine signal failure and signal degradation.

Manual Switchover

When the router is running and you have configured the I/O module for APS/MSP, you can cause switchover by issuing the **aps force** or **aps manual** command.

Switching Mechanisms

E-series routers support both *bidirectional* and *unidirectional* APS switching modes. By default, the router uses bidirectional switching mode.

Bidirectional Switching Mode

In bidirectional switching mode, the router switches both ends of an APS pair to the same working interface or to the same protect interface when either end determines that a switch is required.

Possible reasons for initiating a bidirectional switch include:

- Detection of a signal failure
- Receipt of an **aps force** or **aps manual** command from the local end of an APS pair
- Reversion to the working interface after a failure has been corrected and the timeout value specified in the **aps revert** command has expired

The devices at both the local and remote ends of an APS pair must support bidirectional switching for the router to implement bidirectional switching mode. Otherwise, the router implements unidirectional switching mode at both ends of the APS pair.

The router detects support for bidirectional switching by interpreting the values of the K1 and K2 bytes in the SONET/SDH frame. For details about the meanings of the values of K1 and K2 bytes, see *Communication Methods* on page 70.

Unidirectional Switching Mode

In unidirectional switching mode, the router switches only one end of an APS pair to the working interface or to the protect interface when that end determines that a switch is required. Possible reasons for initiating a unidirectional switch are the same as those described in *Bidirectional Switching Mode* for initiating a bidirectional switch.

Reversion After Switchover

A failed interface automatically reverts from the protect interface to the working interface after the router detects that the working interface is operational and the timeout value specified in the **aps revert** command has expired. Reversion applies only to recovery from failures.

You can configure the router to revert to the working interface at a specified time after it recovers. This feature enables you to use the protect interface as a redundant connection that functions only when the working interface is not available.

Communication Methods

The router communicates with the remote device by using the K1 and K2 bytes in the line overhead of the SONET/SDH frame. The values of these bytes determine the switching and protect actions. Table 8 and Table 9 on page 71 list the meanings of the values of the K1 and K2 bytes. The bytes are defined in Telcordia document GR-253—Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, Revision 3 (September 2000). See requirement objects R5-56 [179] and R5-58 [181] for information about bit ordering and meaning for the K1 byte; see R5-67 [190v2] for information about the K2 byte.

Table 8: Explanation of K1 Byte

Bit Value (12345678)	Meaning
Bits 1–4 represent a request.	
0000	No request
0001	Do not revert
0010	Reverse request
0011	Not used
0100	Exercise
0101	Not used
0110	Wait-to-restore
0111	Not used
1000	Manual switch
1001	Not used
1010	Low-priority signal degradation
1011	High-priority signal degradation
1100	Low-priority signal failure
1101	High-priority signal failure
1110	Forced switch
1111	Lockout of protection
Bits 5–8 represent the channel number.	
0	Channel number of protect interface
0001–1110	Channel number of working interface

Table 9: Explanation of K2 Byte

Bit Value (12345678)	Meaning
Bits 1–4 represent the channel number.	
0	Channel number of protect interface
0001–1110	Channel number of working interface
Bit 5 indicates the type of redundancy.	
0	1 + 1 architecture
Bits 6–8 indicate the switching mode.	
000– 011	Reserved for future use
100	Unidirectional mode
101	Bidirectional mode
110	Line remote defect indication (RDI)
111	Line alarm indication signal (AIS)

Higher-Level Protocols

See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the higher-level protocols that the interfaces described in this chapter support.

Platform Considerations

You can configure unchannelized SONET/SDH interfaces on the following E-series routers:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

This section describes the line modules and I/O modules that support SONET/SDH interfaces.

For detailed information about the modules that support SONET/SDH interfaces on ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that SONET/SDH modules support.

For detailed information about the modules that support SONET/SDH interfaces on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the protocols and applications that SONET/SDH modules support.

OCx/STMx/DS3-ATM Line Modules

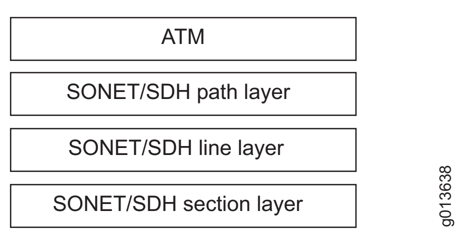
OCx/STMx/DS3-ATM line modules pair with OC3-4 I/O modules to deliver unchannelized OC3/STM1 ATM operation through four line interfaces.

OCx/STMx/DS3-ATM line modules pair with OC12 I/O modules to deliver unchannelized OC12/STM4 ATM operation through one line interface.

I/O modules that support single-mode (intermediate reach or long haul) or multimode operation through SC full duplex connectors are available. I/O modules that support SONET Automatic Protect Switching (APS) 1 + 1 redundancy and SDH Multiplex Section Protection (MSP) are also available.

Figure 5 shows the interface stack for OCx/STMx/DS3-ATM interfaces.

Figure 5: Interface Stack for OCx/STMx/DS3-ATM Interfaces



NOTE: For a detailed description of interface types and specifiers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*. For information about interfaces, see *JUNOSe System Basics Configuration Guide, Chapter 1, Planning Your Network*.

OCx/STMx POS Line Modules

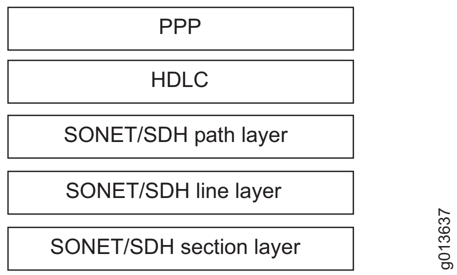
OCx/STMx POS line modules pair with OC3-4 I/O modules to deliver unchannelized OC3/STM1 POS operation through four line interfaces.

OCx/STMx POS line modules pair with OC12 I/O modules to deliver unchannelized OC12/STM4 POS operation through one line interface.

I/O modules that support single-mode (intermediate reach or long haul), or multimode operation through SC full duplex connectors are available. I/O modules that support APS/MSP are also available.

Figure 6 shows the interface stack for OCx/STMx POS interfaces.

Figure 6: Interface Stack for OCx/STMx POS and OC48/STM16 Interfaces



OC48 Line Modules

OC48 line modules pair with OC48 FRAME I/O modules to deliver unchannelized OC48/STM16 POS operation through one line interface.

The OC48 I/O module supports single-mode (intermediate reach or long haul) operation through an SC full duplex connector.

The interface stack for the OC48/STM16 interfaces is the same as that for OCx/STMx POS interfaces (Figure 6).

The OC48 line module can be installed in the router’s turbo slots, numbered 2 and 4. When the OC48 line module is installed in a turbo slot, it spans slots 2–3 and 4–5. The bandwidth of slot 3 or slot 5 is used for a line module in slot 2 or slot 4 if that line module requires the turbo slot.

NOTE: If a line module is installed in slot 3 or slot 5, and the line module in slot 2 or 4 requires bandwidth, the system configures the line module it detects first. The state of the other line module is displayed in the **show version** command output as disabled (cfg error).

OC3/STM1 GE/FE Line Module

The OC3/STM1 GE/FE line module pairs with the OC3-2 GE APS I/O module to deliver unchannelized OC3/STM1 ATM operation through two line interfaces and Gigabit Ethernet operation through one line interface.

The OC3-2 GE APS I/O module uses a range of small form-factor pluggable transceivers (SFPs) to support different optical modes and cabling distances, and accepts up to three LC-style fiber-optic connectors. You can configure ports 0 and 1 for OC3/STM1 ATM interfaces; port 2 is reserved for a Gigabit Ethernet interface.

The interface stack for OC3/STM1 ATM interfaces on the OC3-2 GE APS I/O module is the same as for OCx/STMx/DS3-ATM interfaces. (See Figure 5 on page 72.)

For more information about configuring a Gigabit Ethernet interface on this I/O module, see *OC3-2 GE APS I/O Module* on page 171.

NOTE: The OC3-2 GE APS I/O module does not support APS in the current release.

ES2 4G Line Module

The E120 router and the E320 router support the ES2 4G LM. Other E-series routers do not support the ES2 4G LM. For more information about modules on the E120 router and the E320 router, see the *E120 and E320 Module Guide*.

The ES2 4G LM supports IOAs that support single-mode operation (intermediate reach or long haul). IOAs are available in a half-height size, which enables you to configure them in either of the two IOA bays that are available for each slot. For more information about installing IOAs, see the *E120 and E320 Hardware Guide*.

In the current release, the ES2 4G LM pairs with IOAs to provide OCx/STMx ATM, OCx/STMx POS, Gigabit Ethernet, 10-Gigabit Ethernet, and tunnel-service interfaces.

NOTE: For more information about configuring a Gigabit Ethernet interface or 10-Gigabit Ethernet interface, see *Chapter 5, Configuring Ethernet Interfaces*.

For more information about configuring a tunnel-service interface by using the Tunnel Server IOA, see *Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces*.

E120 Router Configuration

The 120 Gbps switch fabric of the E120 router allocates 10 Gbps of overall bandwidth to each line module slot. The line interface on the ES2 4G LM when installed in a 120 Gbps fabric configuration is 3.9 Gbps; you can achieve this rate with random packet sizes from 64–1518 bytes or a mixture of packet sizes that represent Internet mix traffic (IMIX).

E320 Router Configuration

The 100 Gbps switch fabric of the E320 router allocates 3.4 Gbps of overall bandwidth to each regular line module slot and 10 Gbps of overall bandwidth to each of the turbo slots (slots 2 and 4). The line interface on the ES2 4G LM when installed in a 100 Gbps fabric configuration is 3.4 Gbps; you can achieve this rate with packet sizes greater than 128 bytes.

The 320 Gbps switch fabric of the E320 router allocates 10 Gbps of overall bandwidth to each line module slot. The line interface on the ES2 4G LM when installed in a 320 Gbps fabric configuration is 3.9 Gbps; you can achieve this rate with random packet sizes from 64–1518 bytes or a mixture of packet sizes that represent Internet mix traffic (IMIX).

OCx/STMx ATM IOAs

The ES2 4G LM pairs with the ES2-S1 OC3-8 STM1 ATM IOA to deliver unchannelized OC3/STM1 ATM operation through eight line interfaces. You can install the ES2-S1 OC3-8 STM1 ATM IOA in both IOA bays.

The ES2 4G LM also pairs with the ES2-S1 OC12-2 STM4 ATM IOA to deliver unchannelized OC12/STM4 ATM operation through two line interfaces. You can install the ES2-S1 OC12-2 STM4 ATM IOA in both IOA bays.

The interface stack for both of these IOAs is the same as for OCx/STMx/DS3-ATM interfaces. (See Figure 5 on page 72.)

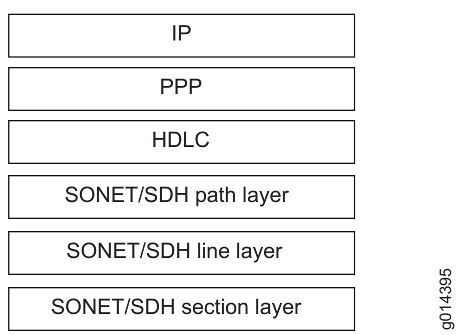
OCx/STMx POS IOAs

The ES2 4G LM pairs with the ES2-S1 OC12-2 STM4 POS IOA to deliver unchannelized OC12/STM4 POS operation through two line interfaces. You can install the ES2-S1 OC12-2 STM4 POS IOA in both IOA bays.

The ES2 4G LM also pairs with the ES2-S1 OC48 STM16 POS IOA to deliver unchannelized OC48/STM16 POS operation through one line interface. In the current release, you can install the ES2-S1 OC48 STM16 POS IOA in only one of the IOA bays per slot.

Figure 7 shows the interface stack for OCx/STMx POS interfaces on the ES2 4G LM.

Figure 7: Interface Stack for OCx/STMx POS Interfaces



Numbering Scheme

When configuring or managing an interface, you must know the numbering scheme for identifying an interface. The numbering scheme depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

Use the *slot/port* format to identify unchannelized SONET/SDH interfaces. Interfaces that support APS/MSP also use the APS/MSP *channel number*.

- *slot*—Number of the slot in which the line module resides in the chassis.

  In ERX-7xx models, line module slots are numbered 2–6; slots 0 and 1 are reserved for SRP modules. In ERX-14xx models, line module slots are numbered 0–5 and 8–13; slots 6 and 7 are reserved for SRP modules. In an ERX-310 router, line module slots are numbered 1–2; slot 0 is reserved for the SRP module.

- *port*—Number of the port on the I/O module.

  On the OC3-2 GE APS I/O module, you can configure only unchannelized SONET/SDH interfaces on ports 0 and 1; port 2 is reserved for a Gigabit Ethernet interface.

  On I/O modules that support APS/MSP, each primary port has a corresponding redundant port. The number of the primary port, but not that of the redundant port, is used to identify the interface. The primary port is above the corresponding redundant port on the I/O modules.

  Primary port numbers range from 0 to *n–1*, where *n* is the total number of primary ports on the module. For example, if a module has one primary port, that port is labeled 0. On some I/O modules, redundant ports are labeled with a port number followed by the letter R. For example, port 3R is the redundant port for the primary port labeled 3. However, on some two-port modules, the primary port is labeled 0 and the redundant port is labeled 1.

  On I/O modules that support APS/MSP, the port numbers for the working (primary) interfaces are assigned the lower half of the numbered interfaces, whereas the port numbers for the protect (redundant) interfaces are assigned the upper half of the numbered interfaces. For example, on an I/O module that provides four primary ports and four redundant ports, the working interface ports are numbered 0–3 and the protect interface ports are numbered 4–7. Similarly, on an I/O module that provides one primary port and one redundant port, the working interface is port 0 and the protect interface is port 1.

- APS/MSP *channel number*—Identifier of the working or protect (redundant) interface for configuration purposes. (See *Bidirectional Switching Mode* on page 69.)

  The protect interface is always assigned channel number 0. The working interface is always assigned channel number 1.

See *Chapter 1, Configuring Channelized T3 Interfaces*, for information about slot numbering.

For information about installing line modules and I/O modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

E120 Router and E320 Router

Use the *slot/adapter/port* format to identify unchannelized SONET/SDH interfaces.

NOTE: The E120 router and the E320 router do not support path channelization.

- *slot*—Number of the slot in which the line module resides in the chassis.

  In the E120 router, line module slots are numbered 0–5. In the E320 router, line module slots are numbered 0–5 and 11–16. For both routers, slots 6 and 7 are reserved for SRP modules; slots 8–10 are reserved for switch fabric modules (SFMs).

- *adapter*—number of the bay in which the I/O adapter (IOA) resides.

  This identifier applies to the E120 and E320 routers only. In the software, adapter 0 identifies the right IOA bay (E120 router) and the upper IOA bay (E320 router); adapter 1 identifies the left IOA bay (E120 router) and the lower IOA bay (E320 router).

- *port*—Number of the port on the IOA.

For information about installing line modules and IOAs in the E120 and E320 routers, see *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*.

Interface Specifier

The configuration examples in this chapter use the format for ERX-7xx models, ERX-14xx models, and the ERX-310 router to specify a SONET/SDH interface. (The format is described in *Numbering Scheme* on page 76.*)*

For example, the following command specifies a SONET/SDH interface on port 0 of an I/O module in slot 0.

host1(config)#**controller sonet 4/0**

When you configure a SONET/SDH interface on an E120 router or an E320 router, you must include the adapter identifier as part of the interface specifier. For example, the following command specifies a SONET/SDH interface on port 0 of the IOA installed in the lower adapter bay (0) of slot 3.

host1(config)#**controller sonet 3/0/0**

For more information about interface types and specifiers on E-series models, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

Exchanging Modules

If you replace an OC3 I/O module with an OCx/STMx line module and a corresponding OC3-4 I/O module or vice versa, you must erase the configuration of the existing modules. See **slot accept** in *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

On the E120 and E320 routers, if you replace an ES2-S1 OC3-8 STM1 ATM IOA with an ES2-S1 OC12 STM4 POS IOA, you must erase the configuration of the existing IOA. See **adapter accept** or **slot accept** in *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

References

For more information about MIB support for unchannelized SONET/SDH interfaces, see RFC 2558—Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999).

For more information about APS/MSP, consult the following resources:

- Telcordia document GR-253—Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, Revision 3 (September 2000)
- ITU-T G.783—Characteristics Of Synchronous Digital Hierarchy (SDH) Multiplexing Equipment Functional Blocks: Annex A – Multiplex Section Protection (MSP) Protocol, Commands And Operation (1990)
- Definitions of Managed Objects for SONET Linear APS Architectures—draft-ietf-atommib-sonetaps-mib-05.txt (November 2001 expiration)
- RFC 3498—Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures (March 2003)

Configuration Tasks

When configuring an unchannelized SONET/SDH interface, you first configure ATM or POS on the interface. For details on configuring POS and ATM, see *JUNOSe Link Layer Configuration Guide, Chapter 1, Configuring ATM,* and *JUNOSe Link Layer Configuration Guide, Chapter 6, Configuring Packet over SONET.*

- On an OCx/STMx/DS3-ATM line module with an OC3-4 or OC12 I/O module, you can configure only ATM interfaces.
- On an OCx/STMx POS line module with an OC3-4 or OC12 I/O module, you can configure only POS interfaces.
- On an OC48 line module with an OC48 FRAME I/O module, you can configure only POS interfaces.
- On an OC3/STM1 GE/FE line module with an OC3-2 GE APS I/O module, you can configure only ATM interfaces on ports 0 and 1.

- On an ES2 4G LM with an ES2-S1 OC12-2 STM4 POS IOA or an ES2-S1 OC48 STM16 POS IOA, you can configure only POS interfaces.
- On an ES2 4G LM with an ES2-S1 OC3-8 STM1 ATM IOA or an ES2-S1 OC12-2 STM4 ATM IOA, you can configure only ATM interfaces.

Configuring the SONET/SDH Layers

When you configure ATM or POS on an interface, you automatically configure default settings at the SONET/SDH layer. To modify the default settings:

1. Select an interface on which you want to configure SONET or SDH.
2. Specify the type of interface: SONET or SDH.
3. Specify a clock source for the interface.
4. (Optional) Assign a text description or an alias to the interface.
5. Disable processing of SNMP link status information for the section and line layers of the interface.
6. Enable processing of SNMP link status information for the path layer of the interface.
7. (Not recommended) Overwrite the automatic setting for the path signal label (C2) byte.
8. Configure the router to use remote defect indications (RDIs) at the path layer to determine the operational status of a path.
9. (MPLS fast reroute over SONET/SDH interfaces) Specify the time that the router waits to set an alarm when the router records a defect at the path layer.
10. (MPLS fast reroute over SONET/SDH interfaces) Specify the time that the router waits to set an alarm when the router records a defect at the line or section layer.
11. Shut down (disable) an interface.

clock source

- Use to configure the transmit clock source for the interface.
- In most cases, accept the default option, **line**. This setting allows the interface to derive the transmit clock from the received clock. In certain circumstances, it might be appropriate to generate a clock from one of the internal sources (options **module** or **chassis**).
- Specify the keyword **line** to use a transmit clock on the line’s receive data stream.
- Specify the keywords **internal module** to use the line module’s internal clock.
- Specify the keywords **internal chassis** to use the router’s clock.

- On a cOC3/STM1 I/O module, you can configure some ports with internal clock sources and others with line clock sources. However, all ports with internal clock sources must use either the router's clock or the module's clock. You cannot configure some ports on the I/O module to use the router's clock and others to use the module's clock.
- To change the clock source of the ports on a cOC3/STM1 I/O module from the router's clock to the module's clock or vice versa, change the clock source of all ports firstly to the line setting, and then to the new internal clock setting.
- Example

  host1(config-controll)#**clock source internal module**

- Use the **no** version to revert to the default, **line**.

controller sonet

- Use to select an interface on which you want to configure SONET or SDH.
- Use the interface specifier in *slot/port:path-channel* format (ERX-14xx models, ERX-7xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 router and E320 router). The E120 and E320 routers do not support path channelization, and therefore does not support the *path-channel* specifier.
- Example 1—Selects a SONET interface on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1(config)#**controller sonet 4/0**

- Example 2—Selects an SONET interface on the E320 router

  host1(config)#**controller sonet 3/0/0**

- There is no **no** version.

description

- Use to assign a text description or an alias to an unchannelized SONET interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 64 characters.
- Use the **show controllers sonet** command to display the text description.
- Example

  host1(config-controll)#**description boston-sonet-interface**

- Use the **no** version to remove the text description or alias.

path description

- Use to assign a text description or an alias to an unchannelized SONET path.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 64 characters.

- Example

  host1(config-controll)#**path description westford**

- Use the **no** version to remove the description.

path overhead c2

- Use to overwrite the automatic setting for the path signal label (C2) byte.
- By default, the value of the C2 byte for the path is determined by the layers configured above the SONET/SDH interface and set automatically. The E-series router sets this default value in accordance with RFC 2558. (See *References* on page 78.)

CAUTION: Use this command only if you know that the automatic setting does not match the setting on the remote device. Otherwise, the remote device might send an unexpected value, and the router might lose data.

- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path overhead c2 20**

- Use the **no** version to restore the default setting, in which the value of the C2 byte is determined by the layers configured above the SONET/SDH interface.

path shutdown

- Use to disable a path.
- Paths are enabled by default.
- Example

  host1(config-controll)#**path shutdown**

- Use the **no** version to restart a disabled path.

path snmp trap link-status

- Use to enable SNMP link-status processing for the path layer of the interface.
- The default is disabled.
- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

path trigger alarm prdi

- Use to configure the router to use remote defect indications (RDIs) at the path layer to determine the operational status of a path.
- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path trigger alarm prdi**

- Use the **no** version to restore the default setting, in which the software uses loss of pointer and AIS defects at the path layer to determine the operational status of a path.

path trigger delay

- Use to set the time that the router waits to set an alarm when the router records a defect at the path layer.
- Change this value from the default only when you are using MPLS fast reroute over a SONET/SDH interface.
  - Specify a value of 0 milliseconds if the interface does not use APS/MSP or if you want MPLS to have priority over APS/MSP.
  - Specify a value of at least 100 milliseconds if this interface uses APS/MSP and you want APS/MSP to have priority over MPLS.
- Do not specify a path identifier for unchannelized SONET/SDH interfaces.
- Example

  host1(config-controll)#**path trigger delay msec 1000**

- Use the **no** version to restore the default setting, 2500 milliseconds.

sdh

- Use to specify that the interface supports SDH.
- Example

  host1(config-controller)#**sdh**

- Use the **no** version to revert to SONET operation on this interface.

shutdown

- Use to disable a SONET/SDH interface.
- SONET/SDH interfaces are enabled by default.
- Example

  host1 (config-controll)#**shutdown**

- Use the **no** version to restart a disabled interface.

snmp trap link-status

- Use to enable SNMP link-status processing for the section and line layers of the interface.
- The default is enabled.
- Example

  host1(config-controll)#**no snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

trigger delay

- Use to set the time that the router waits to set an alarm when the router records a defect at the line or section layer.
- Change this value from the default only when you are using MPLS fast reroute over a SONET/SDH interface.
  - Specify a value of 0 milliseconds if the interface does not use APS/MSP or if you want MPLS to have priority over APS/MSP.
  - Specify a value of at least 100 milliseconds if this interface uses APS/MSP and if you want APS/MSP to have priority over MPLS.
- Example

  host1(config-controll)#**trigger delay msec 1000**

- Use the **no** version to restore the default setting, 2500 milliseconds.

Configuring APS/MSP

For APS/MSP, you must configure a working interface and a corresponding protect interface. You must also assign each pair of working and protect interfaces to a unique group.

NOTE: Configuring the working interface before you configure the protect interface is not required. You can configure the working interface before or after you configure the protect interface.

NOTE: The E120 router and the E320 router does not support APS/MSP.

Configuring the Working Interface

To configure the working interface:

1. Select the interface.

   host1(config)#**controller sonet 4/0**

2. Specify the APS group to which the working and protect interfaces will belong.

   host1(config-controll)#**aps group boston**

3. Specify the interface as the working interface.

   host1(config-controll)#**aps working**

aps group

- Use to specify the group to which the working and protect interfaces will belong.
- Specify the name of the APS group.
- Example

  host1(config-controll)#**aps group boston**

- Use the **no** version to remove a group of APS interfaces.

aps working

- Use to specify the working interface.
- Optionally, you can specify 1 as the channel number for the working interface. Because the working interface is always assigned channel number 1, this is the only valid option.
- Examples

  host1(config-controll)#**aps working**
  host1(config-controll)#**aps working 1**

- Use the **no** version to prevent the interface from acting as a working interface.

threshold

- Use to set thresholds for the bit error rates associated with APS/MSP alarms.
- This command does not apply to the working interface. You can issue this command only for the protect interface.
- Specify one of the following keywords to indicate the alarm level:
  - **sd-ber**—Bit error rate that specifies signal degradation
  - **sf-ber**—Bit error rate that specifies signal failure
- Specify an integer *n* in one of the following ranges, where *n* corresponds to a rate of 10^{-n} (10e-*n*) errors per second.
  - For **sd-ber**, an integer in the range 5–9; the default value is 5
  - For **sf-ber**, an integer in the range 3–5; the default value is 3
- Example

  host1(config-controll)#**threshold sf-ber 4**

- Use the **no** version to restore the default, 5 (for **sd-ber**) or 3 (for **sf-ber**), for the specified alarm.

Configuring the Protect Interface

To configure the protect interface:

1. Select the interface.

   host1(config)#**controller sonet 4/1**

2. Specify the APS group to which the protect and working interfaces will belong.

   host1(config-controll)#**aps group boston**

3. Specify the protect interface.

   host1(config-controll)#**aps protect**

4. (Optional) Prevent the protect interface from taking over automatically if the working interface fails.

   host1(config-controll)#**aps lockout**

5. (Optional) Enable the router to revert to the working interface when it recovers.

   host1(config-controll)#**aps revert 7**

6. (Optional) Specify that switchover takes place in unidirectional mode.

   host1(config-controller)#**aps unidirectional**

aps group

- Use to specify the group to which the working and protect interfaces will belong.
- Specify the name of the APS group.
- Example

  host1(config-controll)#**aps group boston**

- Use the **no** version to remove a group of APS interfaces.

aps lockout

- Use to prevent the protect interface from taking over if the working interface fails.
- You can issue this command only for the protect interface, not for the working interface.
- The **aps lockout** command has a higher priority than the **aps force** command, **aps manual** command, a remote reversion request, a signal failure request, or a signal degradation.
- Optionally, you can specify 0 as the channel number for the protect interface. Because the protect interface is always assigned channel number 0, this is the only valid option.
- The resulting configuration is stored in NVS for SRP module or line module reloads and SNMP.

- Examples

  host1(config-controll)#**aps lockout**
  host1(config-controll)#**aps lockout 0**

- Use the **no** version to restore the default situation, in which the protect interface can take over if the working interface fails.

aps protect

- Use to configure an interface as a protect interface.
- You can issue this command only for the protect interface, not for the working interface.
- Optionally, you can specify 0 as the channel number for the protect interface. Because the protect interface is always assigned channel number 0, this is the only valid option.
- Examples

  host1(config-controll)#**aps protect**
  host1(config-controll)#**aps protect 0**

- Use the **no** version to remove the protect interface from the APS group.

aps revert

- Use to revert to the original working interface when it recovers.
- Specify the number of minutes in the range 5–7, after which the router will switch to the working interface.
- You can issue this command only for the protect interface, not for the working interface.
- Example

  host1(config-controll)#**aps revert 7**

- Use the **no** version to restore the default setting, in which the router does not revert to the working interface when it recovers.

aps unidirectional

- Use to specify that the router should switch to the protect interface using the unidirectional mode switching mechanism.
- You can issue this command only for the protect interface, not for the working interface.
- Example

  host1(config-controller)#**aps unidirectional**

- Use the **no** version to restore the default setting, bidirectional mode.

Configuring SONET/SDH Alarms

To configure the bit error rates that determine signal degradation and signal failure on the working interface:

1. Select the protect interface.

   host1(config)#**controller sonet 4/1**

2. Specify the bit error rate at which the router should generate an alarm indicating signal degradation.

   host1(config-controller)#**threshold sd-ber 6**

3. Specify the bit error rate at which the router should generate an alarm indicating signal failure and switch from the working interface to the protect interface.

   host1(config-controller)#**threshold sf-ber 5**

threshold

- Use to set thresholds for the bit error rates associated with APS/MSP alarms.
- You can issue this command only for the protect interface. It does not apply to the working interface.
- Specify one of the following keywords to indicate the alarm level:
  - **sd-ber**—Bit error rate that specifies signal degradation
  - **sf-ber**—Bit error rate that specifies signal failure
- Specify an integer *n* in one of the following ranges, where *n* corresponds to a rate of 10^{-n} (10e-*n*) errors per second.
  - For **sd-ber**, an integer in the range 5–9; the default value is 5
  - For **sf-ber**, an integer in the range 3–5; the default value is 3
- Example

  host1(config-controll)#**threshold sf-ber 4**
- Use the **no** version to restore the default, 5 (for **sd-ber**) or 3 (for **sf-ber**), for the specified alarm.

Configuration Example

The following example shows how to configure working and protect interfaces for APS/MSP.

1. Configure the working interface.

   host1(config)#**controller sonet 3/0**
   host1(config-controller)#**aps group boston**
   host1(config-controller)#**aps working 1**

2. Configure the protect interface.

```
host1(config-controller)#controller sonet 3/1
host1(config-controller)#aps group boston
host1(config-controller)#aps protect 0
host1(config-controller)#aps unidirectional
host1(config-controller)#aps revert 30
host1(config-controller)#threshold sf-ber 4
```

Configuring APS Event Collection

To configure line modules to deliver APS events to the necessary SNMP traps, issue the **aps events** command from Global Configuration mode.

aps events

- Use to enable line modules to deliver APS events to the necessary SNMP traps.
- Use the *list* variable to deliver the following types of APS events:
  - all—Configure notification of all APS events
  - channel-mismatch—Configure notification of APS channel mismatches
  - feplf—Configure notification of APS far-end protection line failures
  - mode-mismatch—Configure notification of APS mode mismatches
  - psbf—Configure notification of APS protection signal byte failures
  - switchover—Configure notification of APS switchovers
- Example

  host1(config)#**aps events channel-mismatch**

- Use the **no** version to disable the delivery of APS events from line modules to SNMP traps.

Manual Switching to a Redundant Port

To switch from the working interface to the protect interface manually, issue the **aps force** command or the **aps manual** command. The **aps force** command overrides any switchover settings you configured on the protect interface; the **aps manual** command does not override those settings.

aps force

- Use to switch from the working interface to the assigned protect interface unless a request of equal or higher priority is in effect.
- You can issue this command only for the protect interface, not for the working interface.
- The **aps force** command has a higher priority than the **aps manual** command, a remote reversion request, a signal failure request on a working channel, or a signal degradation request on a working channel.
- The resulting configuration is not stored in NVS for SRP module or line module reloads; however, it is stored in NVS for use with SNMP.

- You must specify one of the following channel numbers:
  - 0—Switches from the protect interface back to the working interface
  - 1—Switches from the working interface to the protect interface
- Examples

```
host1(config-controll)#aps force 0
host1(config-controll)#aps force 1
```

- Use the **no** version to revert to the original working interface.

aps manual

- Use to switch from the working interface to the protect interface unless a command of equal or higher priority is in effect.
- You can issue this command only for the working interface, not for the protect interface.
- The **aps manual** command has a higher priority than a remote reversion request.
- The resulting configuration is not stored in NVS for SRP module or line module reloads; however, it is stored in NVS for use with SNMP.
- You must specify one of the following channel numbers:
  - 0—Switches from the protect interface back to the working interface
  - 1—Switches from the working interface to the protect interface
- Examples

```
host1(config-controll)#aps manual 0
host1(config-controll)#aps manual 1
```

- Use the **no** version to revert to the original working interface.

Testing Interfaces

You can enable loopback tests at the SONET/SDH level. You can also test for connectivity between an interface and the SONET/SDH interface at the other end of the line.

Loopback Testing

To configure loopback testing at the SONET/SDH level, use the **loopback** command.

loopback

- Use to configure the type of loopback at the SONET/SDH layer.
- Specify one of the following options:
  - **local**—Loops the data back toward the router
  - **network**—Loops the data toward the network before the data reaches the frame.

- Example

  host1(config)#**controller sonet 4/0**
  host1(config-controller)#**loopback network**

- Use the **no** version to disable loopback.

Testing Connectivity

Use the **path overhead j1** command to check for connectivity between the router and a SONET/SDH device at the other end of the line. This command defines:

- A message that the router sends from the specified interface to the SONET/SDH device at the other end of the line.

- A message that the router expects to receive on the specified interface from the SONET/SDH device at the other end of the line.

When you define a message that the interface sends, you must monitor receipt of that message at the remote end.

When you define a message that the interface expects to receive, you should configure the remote device to transmit the same message to the interface. You can then use the **show controllers sonet** command to compare the expected and receive messages.

You must remove trace messages before you can change the port type from SONET to SDH or vice versa. Otherwise, you see the following error message:

```
% Cannot set port mode (path trace message is set)
```

path overhead j1

- Use to define messages that the router sends to or expects to receive from a SONET/SDH device connected to one of its SONET interfaces.
- Do not specify a path identifier for unchannelized SONET interfaces.
- Specify the keyword **msg** for a message that the router transmits for this path.
- Specify the keyword **exp-msg** to define a message that the router expects to receive on this path.
- Define a message of up to 62 characters for SONET or up to 15 characters for SDH.
- Configure the remote device to send the same message that the router expects to receive on this path. You can then compare the expected and received messages in the display of the **show controllers sonet** command.
- Example for unchannelized SONET interfaces:

  host1(config-controller)#**path overhead j1 msg hello**

- Use the **no** version to restore the default situation, in which all the characters in the transmitted or expected message are zeros.

Monitoring SONET/SDH Interfaces

You can monitor interface statistics and APS/MSP settings.

NOTE: The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

Monitoring Interface Statistics

You can set statistics baselines for the section, line, and path layers using the **baseline interface sonet** commands.

To display statistics for SONET and SDH interfaces, use the **show controllers sonet** commands. Use the **delta** options to display statistics with the baseline subtracted.

baseline line interface sonet

- Use to set a statistics baseline for the SONET/SDH line layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet line** command to view the baseline statistics.
- Example 1—Sets a baseline for SONET line layer interfaces on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1#**baseline line interface sonet 2/0**

- Example 2—Sets a baseline for SONET line layer interfaces on the E320 router

  host1#**baseline line interface sonet 3/0/0**

- There is no **no** version.

baseline path interface sonet

- Use to set a statistics baseline for the SONET/SDH path layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet path** command to view the baseline statistics.

- Example 1—Sets a baseline for SONET path layer interfaces on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1#**baseline path interface sonet 2/0**

- Example 2—Sets a baseline for SONET path layer interfaces on the E320 router

  host1#**baseline path interface sonet 3/0/0**

- There is no **no** version.

baseline section interface sonet

- Use to set a statistics baseline for the SONET/SDH section layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet section** commands to view the baseline statistics.
- Example 1—Sets a baseline for SONET section layer interfaces on ERX-14xx models, ERX-7xx models, or the ERX-310 router

  host1#**baseline section interface sonet 2/0**

- Example 2—Sets a baseline for SONET section layer interfaces on the E320 router

  host1#**baseline section interface sonet 3/0/0**

- There is no **no** version.

show controllers sonet

- Use to display the configuration for SONET and SDH interfaces.
- Field descriptions
  - Interface specifier in *slot/port* format (ERX-14xx models, ERX-7xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 and E320 routers)
  - non channelized—Unchannelized path
  - channelized—Number of channels and speed for the interface
  - ifAdminStatus—Configured status of the interface: up or down
  - description—Configured description of the controller
  - snmp trap link-status—State of SNMP link-status processing for the section and line layers of the interface: enabled or disabled
  - alarms used for operational status calculation—Types of defects that the router uses to determine the operational status of the interface at the section and line layers
  - defect trigger soaking delay—Time that the router waits to set an alarm when the router records a defect at the section or line layer

- Operational Status—Physical state of the interface:
  - up—Interface is operational
  - down, failure alarm—Interface is not operational; type of defect that caused failure is specified
  - time since last status change—Time since the module was rebooted
- Loopback State—Type of loopback configured on the interface
- Mode—Type of interface: SONET or SDH
- Timing source—Type of clock source configured for the channel:
  - line—Internal clock is from the line module itself
  - chassis—Internal clock is from the configured router clock
- Receive FIFO Overruns—Number of times received FIFO was overrun
- Current section defects—Number of suspect bit patterns found in several consecutive frames in section layer
- Current line defects—Number of suspect bit patterns found in several consecutive frames in line layer
- Received SONET overhead—Section and line overhead bytes present in the receive side of the interface at any particular time
- Transmitted SONET overhead—Section and line overhead bytes present in the transmit side of the interface at any particular timeChannel configuration—Parameters for specific controllers. The actual parameters depend on the controller.
  - ifAdminStatus—State of the controller in the software configuration: up or down
  - snmp trap link-status—State of SNMP link status processing for the path layer: enabled or disabled
  - alarms used for operational status calculation—Types of defects that the router uses to determine the operational status of the interface at the path layer
  - defect trigger soaking delay—Time that the router waits to set an alarm when the router records a defect at the path layer
  - c2 byte—Setting of path signal byte: set by upper interface type (automatic setting) or configured value
  - Operational Status—Physical state of the controller: up, down, or lowerLayerDown
  - time since last status change: time the controller has been in the current physical state
- Received SONET Path overhead—Path overhead bytes present in the receive side of the interface at any particular time
- Transmitted SONET Path overhead—Path overhead bytes present in the transmit side of the interface at any particular time

- Example

```
host1#show controllers sonet 1/0

oc3 1/0
non channelized
ifAdminStatus: up
description: link1
snmp trap link-status: enabled
alarms used for operational status calculation: LOS LOF AIS RDI
defect trigger soaking delay: 2500 milliseconds
Operational Status: down, failure alarm: AIS
      time since last status change: 07:33:12
Loopback State: none
Mode: sonet
Timing source: line
Receive FIFO Overruns: 0, Framer stats: 0/0
Current section defects: none
Current line    defects: AIS


Received SONET overhead:
F1      :  n/a, J0      :  n/a, K1      : 0xFF, K2      : 0xFF, S1      : 0xFF
Transmitted SONET overhead:
F1      : 0x00, J0      : 0x01, K1      : 0x00, K2      : 0x00, S1      : 0x00

Channel configuration:
channel = 0, path = oc3, hierarchy = 1/0, current path defects: LowerLayerDefect
 ifAdminStatus: up
 snmp trap link-status: disabled
 alarms used for operational status calculation: LOP AIS
 defect trigger soaking delay: 2500 milliseconds
 c2 byte set by upper interface type
 Operational Status: lowerLayerDown
       time since last status change: 07:33:12


Received SONET Path overhead:
F2      :  n/a, Z3      :  n/a, Z4      :  n/a, C2      : 0xFF, C2Exp   : 0x00
Transmitted SONET Path overhead:
F2      : 0x00, Z3      : 0x00, Z4      : 0x00, C2      : 0x00
```

show controllers sonet line | path | section

- Use to display statistics for the different layers in channelized SONET and SDH interfaces. Figure 5 on page 72 and Figure 6 on page 73 show the layers in the interfaces.
- For definitions of the MIB statistics, see RFC 2558—Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999).
- Specify an interface in *slot/port* format (ERX-14xx models, ERX-7xx models, and the ERX-310 router) or *slot/adapter/port* format (E120 and E320 routers).
- To view statistics for a layer, specify the type of layer.
- To view all statistics for all sessions, specify the **total** keyword.
- To view baselined statistics for all intervals, specify the **delta total** keywords.

- Field descriptions
  - Current Interval Counters—Statistics for the current 15-minute interval

    The following fields may appear in line, path, or section:

    - ES—Number of errored seconds encountered by a T1 or an E1 in an interval
    - SES—Number of severely errored seconds encountered in an interval
    - UAS—Number of unavailable seconds encountered in an interval
    - SEFS—Number of severely errored framing seconds encountered in an interval
    - (Code Violations)—Number of coding violations encountered in an interval (BIP-B1, BIP-B2, BIP-B3)
    - RDI—Number of remote defect indications
    - AIS—Number of alarm indication signals
    - BERR-SF—Number of bit error rate signal failures
    - BERR-SD—Number of bit error rate signal degrades
    - LOS—Number of loss of signal alarms
    - LOF—Number of loss of frame alarms
    - LOP—Number of loss of pointers
    - UNEQ—Number of unequipped alarms
    - PLM—Number of payload mismatchs
  - Last Interval Counters—Statistics for the previous 15-minute interval
  - Current Far End Interval Counters—Statistics for the remote connection associated with the SONET/SDH path in the current 15-minute interval
    - REI—Number of remote error indications
  - Far End Last Interval Counters—Statistics for the remote connection associated with the SONET/SDH path in the previous 15-minute interval
  - Total Interval Counters—Statistics for all intervals or baselined statistics
  - Total Far End Counters—Statistics for all remote connections associated with the SONET/SDH path
- Example 1—Shows the MIB statistics for the path layer on interface 1/0.

```
host1#show controllers sonet 1/0 path

Channel number 0

Number of valid intervals - 31
Time elapsed in current interval - 141
Current status                  = LowerLayerDefect

Current Path Interval Counters          Seconds      Counts        State
ES                                            0
SES                                           0
UAS                                         141
RDI                                         141            0       Active
AIS                                         141            0       Active
LOP                                           0            0       OK
```

```
UNEQ                                       0             0       OK
PLM                                      141             0       Active
BIP-B3  (Code Violation)                   0             0


Last Path Interval Counters            Seconds      Counts
ES                                         0
SES                                        0
UAS                                      900
RDI                                      900             0
AIS                                      900             0
LOP                                        0             0
UNEQ                                       0             0
PLM                                      900             0
BIP-B3  (Code Violation)                   0             0


Total Path Counters                    Seconds      Counts
ES                                         0
SES                                        0
UAS                                    27255
RDI                                    27255             0
AIS                                    27255             0
LOP                                        0             0
UNEQ                                       0             0
PLM                                    27255             0
BIP-B3  (Code Violation)                   0             0


Current Far End Path Interval Counters   Seconds      Counts
ES                                         0
SES                                        0
UAS                                      141
REI                                        0             0

Far End Last Path Interval Counters     Seconds      Counts
ES                                         0
SES                                        0
UAS                                      900
REI                                        0             0

Total Far End Path Counters            Seconds      Counts
ES                                         0
SES                                        0
UAS                                    27255
REI                                        0             0
```

- Example 2—Shows the MIB statistics for the line layer on interface 1/0.

host1#**show controllers sonet 1/0 line**

```
Number of valid intervals - 31
Time elapsed in current interval - 114
Current status                   = AIS


Current Line Interval Counters         Seconds      Counts        State
ES                                         0
SES                                        0
UAS                                      113
RDI                                        0             0       OK
AIS                                      113             0       Active
BERR-SF                                    0             0       OK
```

```
BERR-SD                                  0             0       OK
BIP-B2 (Code Violation)                  0             0


Last Line Interval Counters          Seconds      Counts
ES                                       0
SES                                      0
UAS                                    900
RDI                                      0             0
AIS                                    900             0
BERR-SF                                  0             0
BERR-SD                                  0             0
BIP-B2 (Code Violation)                  0             0


Total Line Counters                  Seconds      Counts
ES                                       0
SES                                      0
UAS                                  27227
RDI                                      0             0
AIS                                  27227             1
BERR-SF                                  0             0
BERR-SD                                  0             0
BIP-B2 (Code Violation)                  0             0


Current Far End Line Interval Counters   Seconds      Counts
ES                                       0
SES                                      0
UAS                                      0
REI                                      0             0

Far End Last Line Interval Counters  Seconds      Counts
ES                                       0
SES                                      0
UAS                                      0
REI                                      0             0

Total Far End Line Counters          Seconds      Counts
ES                                       0
SES                                      0
UAS                                     10
REI                                      0             0
```

- Example 3—Shows the MIB statistics for the section layer on interface 1/0.

host1#**show controllers sonet 1/0 section**

```
Number of valid intervals - 31
Time elapsed in current interval - 49
Current status                  = No Defect

Current Section Interval Counters    Seconds      Counts        State
ES                                       0
SES                                      0
SEFS                                     0
LOS                                      0             0       OK
LOF                                      0             0       OK
BIP-B1 (Code Violation)                  0             0

Last Section Interval Counters       Seconds      Counts
ES                                       0
SES                                      0
```

```
SEFS                                          0
LOS                                           0             0
LOF                                           0             0
BIP-B1 (Code Violation)                       0             0


Total Section Counters                   Seconds      Counts
ES                                            1
SES                                           1
SEFS                                          0
LOS                                           0             0
LOF                                           0             0
BIP-B1 (Code Violation)                       1            16
```

- Example 4—Shows all statistics for all sessions for the section layer on interface 2/0.

```
host1#show controllers sonet 2/0 section total

Number of valid intervals - 31
Time elapsed in current interval - 244

Total Section Counters                   Seconds      Counts
ES                                            1
SES                                           1
SEFS                                          0
LOS                                           0             0
LOF                                           0             0
BIP-B1 (Code Violation)                       1            16
```

Monitoring APS/MSP

You can use the **show aps** commands to monitor APS/MSP.

show aps

- Use to display information about interfaces on which APS/MSP is configured.
- Use the **all** keyword to display information from all APS/MSP groups. In the output, partially configured controllers are displayed with `none` and include only the group name.
- Field descriptions
  - sonet x/y—Location of the SONET/SDH interface
  - protect group—Name of the APS group that contains the working interface and the corresponding protect interface
  - channel—Number of the APS channel; 0 identifies the protect interface, 1 identifies the working interface
  - ~—Interface is not currently active
  - Selected—Interface is active
  - ~Selected—Interface is not active
  - Bidirectional—Router switches to the protect interface using the bidirectional switching mechanism
  - Unidirectional—Router switches to the protect interface using the unidirectional mode switching mechanism

  - Nonrevertive—Router does not revert to the working interface when it recovers
  - Revertive—Router reverts to the working interface when it recovers
  - Disabled—APS/MSP is disabled on the interface
  - Enabled—APS/MSP is enabled on the interface

- Example 1

```
host1#show aps
sonet 5/1 protect group one channel 0  ~Selected Unidirectional Nonrevertive
sonet 5/0 working group one channel 1   Selected Enabled
```

- Example 2

```
host1#show aps all
aps events: disabled
sonet 4/0 working group group-4 channel 1   Selected Enabled
sonet 4/1 protect group group-4 channel 0  ~Selected Unidirectional
Nonrevertive
sonet 2/0 working group group-2 channel 1   Selected Enabled
sonet 2/1 protect group group-2 channel 0  ~Selected Unidirectional
Nonrevertive
sonet 12/0
sonet 12/1
sonet 12/2 none    group partial-group
sonet 12/3
sonet 12/4
sonet 12/5
sonet 12/6
sonet 12/7
```

show aps group

- Use to display information about all APS/MSP groups or a specified APS/MSP group.
- Field descriptions
  - Aps group—Name of the APS group for which information is displayed
  - Current Conditions—Current state of the group
  - Rx (K1/K2)—Value, meaning, and channel number of the received K1 and K2 bytes (see Table 8 on page 70 and Table 9 on page 71)
  - Tx (K1/K2)—Value, meaning, and channel number of the transmitted K1 and K2 bytes (see Table 8 on page 70 and Table 9 on page 71)
  - Counters—Statistics for APS group
    - ModeMismatch—Number of differences detected in the local and remote switching mechanisms (unidirectional or bidirectional modes)
    - ChanMismatch—Number of differences detected between the number of the channel in the transmitted K1 byte and the number of the channel in the received K2 byte

    - PSBF—Number of protection switching byte failures detected (no 3 consecutive SONET/SDH frames out of the last 12 contain identical K1 bytes)
    - FEPLF—Number of far-end protection line failures (signal failures detected on protect interface)
  - Aps channel—Number, interface specifier (in *slot/port* format), and protect/working designation of the APS channel for which information is displayed
    - aps-protect—Identifies the protect interface
    - aps-working—Identifies the working interface
  - Current Conditions—Current state of the interface for this channel
    - lockedOut—Indicates that the router is configured to prevent the protect interface from taking over if the primary interface fails
    - SD—Indicates that signal degradation is detected
    - SF—Indicates that signal failure is detected
    - switched—Indicates that the router has switched from the working interface to the protect interface
  - Counters—Statistics for APS channel
    - SignalDegrades—Number of degraded signals detected
    - SignalFailures—Number of failed signals detected
    - Switchovers—Number of times the router has switched from the working interface to the protect interface
    - LastSwitchover—Length of time that the working interface was active when the router last switched from the working interface to the protect interface; a value of Not Applicable indicates that no switchovers have occurred
- Example

```
host1#show aps group
Aps group bos
  Current Conditions: PSBF
  Rx(K1/K2): 00/00, No Request on channel 0
  Tx(K1/K2): f0/05, Lockout of Protection on channel 0
  Counters
    ModeMismatch = 0
    ChanMismatch = 0
    PSBF         = 1
    FEPLF        = 0
  Aps channel 0  (5/4) (aps-protect)
    Current Conditions: SF
    Counters
      SignalDegrades = 0
      SignalFailures = 1
  Aps channel 1  (5/0) (aps-working)
    Current Conditions: None
    Counters
      SignalDegrades = 0
      SignalFailures = 0
      Switchovers    = 0
      LastSwitchover = Not Applicable
```

Chapter 4

Configuring Channelized OCx/STMx Interfaces

Use the procedures described in this chapter to configure channelized OC3/STM1 and OC12/STM4 (cOCx/STMx) interfaces on E-series routers.

This chapter contains the following sections:

- Overview on page 101
- Platform Considerations on page 104
- References on page 109
- Before You Configure an Interface on page 111
- Configuration Tasks on page 111
- Configuration Examples on page 133
- Testing Interfaces on page 136
- Monitoring Interfaces on page 144

Overview

Channelized OC3/STM1 and OC12/STM4 interfaces are supported by the modules described in this chapter.

This section describes the features of cOCx/STMx interfaces.

SONET APS and SDH MSP

The router supports Automatic Protection Switching (APS) and Multiplex Section Protection (MSP) on selected I/O modules that provide SONET/SDH connections. This feature provides a redundant connection if a primary SONET/SDH connection fails. For a list of I/O modules that support APS/MSP, see *ERX Module Guide, Appendix A, Module Protocol Support*. For an overview of APS/MSP, see *Bidirectional Switching Mode* in *Chapter 3, Configuring Unchannelized OCx/STMx Interfaces*.

MDL/FDL Support

Interfaces on cOCx/STMx line modules support maintenance data link (MDL) messages at the T3 level and facilities data link (FDL) messages at the T1 level. For a list of the line modules that support MDL and FDL, see *ERX Module Guide, Appendix A, Module Protocol Support*.

You can use MDL and FDL messages to determine the status of a link and to display statistics for the remote end of a connection. MDL and FDL messages do not interfere with other data transmitted over the link.

MDL Standards

You can configure channelized T3 interfaces to send MDL messages that comply with ANSI T1.107a-1990 Standard for Telecommunications—Digital Hierarchy – Supplement to Formats Specification (August 1990). MDL messages identify a particular link by sharing common codes for data such as the equipment identifier, line identifier, frame identifier, and unit.

FDL Standards

Similarly, you can configure T1 channels to send FDL messages that comply with either or both of the following standards:

- ANSI T1.403-1989 Standard for Telecommunications—Network and Customer Installation Interfaces – DS1 Metallic Interface – Robbed-bit Signaling State Definitions (1989)

  FDL messages that comply with the ANSI standard identify a particular link by sharing common codes for data such as the equipment identifier, line identifier, frame identifier, and unit.

- AT&T Technical Reference 54016—Requirements for Interfacing Digital Terminal Equipment to Services Employing the Extended Superframe Format (September 1989)

  FDL messages that comply with the AT&T standard identify a particular link by sharing performance data and do not use common codes for data such as the equipment identifier, line identifier, frame identifier, and unit.

Timeout of Received MDL and FDL Messages

When a line module receives an MDL or FDL message string, it stores the strings for a period of 10 seconds after the last message was received. If the line module does not receive another message of any type containing the same string within 10 seconds, it erases the local copy of the message.

Most MDL and FDL message strings are common to all three types of messages that can be transmitted: path identifications, idle signals, and test signals. Certain message strings, however, are unique to a particular message type. Table 10 on page 103 briefly describes each MDL/FDL message string and indicates (with an ✔) the types of messages in which it can be sent.

Table 10: MDL and FDL Message Strings and Message Types

Message String	Description	Path Message	Idle Signal Message	Test Signal Message
eic	Equipment identification code	✔	✔	✔
fic	Frame identification code	✔	✔	✔
generator	Generator number	–	–	✔
lic	Line identification code	✔	✔	✔
pfi	Facility identification code	✔	–	–
port	Equipment port number	–	✔	–
unit	Unit identification code	✔	✔	✔

As long as another message of any type containing the same string is received within 10 seconds, the line module retains the local copy of the message string and resets the 10-second timer for that string.

For example, if a line module receives an MDL or FDL test signal message containing an eic string, and then receives a idle signal message within 10 seconds that also contains an eic string, it retains the local copy of the most recent eic string received and resets the 10-second timer for that message. However, if 10 seconds pass without the line module receiving a path identification, test signal, or idle signal message containing an eic string, the line module erases the local copy of the eic message string.

For message strings that are unique to a particular message type, the line module must receive another message of the same type containing this string in order to retain the local copy of the string and reset the timer. For example, if the line module receives a test signal message containing a generator string and does not receive another test signal message within 10 seconds, it erases the local copy of the generator string.

Frequency of FDL Path Messages

E-series routers transmit FDL path identifier messages every second. This behavior complies with the ANSI T1.403 specification (listed in *References* on page 109) and is consistent with the MDL implementation for E-series routers.

Higher-Level Protocols

See *ERX Module Guide*, *Appendix A*, *Module Protocol Support* for information about the higher-level protocols that cOCx/STMx interfaces support.

Platform Considerations

You can configure cOCx/STMx interfaces on the following E-series routers:

- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

For detailed information about the modules that support cOCx/STMx interfaces on ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that cOCx/STMx modules support.

cOCx/STMx F0 Line Module

The cOCx/STMx F0 line module pairs with either a cOC3/STM1 I/O module or a cOC12/STM4 I/O module to support channelized T3 (DS3), T1, E1, FT1, and FE1 signaling. Each connection is made through standard SC connectors.

The cOCx/STMx line module supports the following:

- 3 unchannelized/channelized DS3s per OC3
- 84 framed T1s per OC3/STM1
- 63 framed/unframed E1s per OC3/STM1
- 500 fractional T1/E1s per OC3/STM1

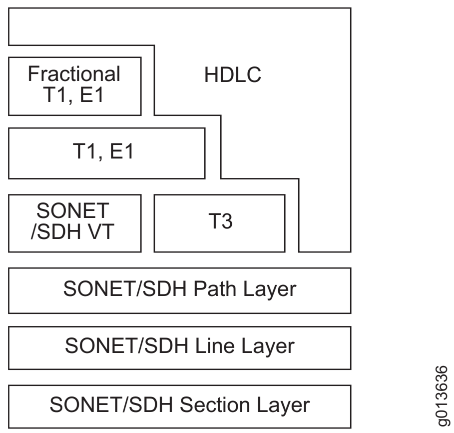
You can combine the cOCx/STMx line module with four-port cOC3/STM1 I/O modules or one-port cOC12/STM4 I/O modules. cOC3/STM1 I/O modules support one OC3/STM1 per port. cOC12/STM4 I/O modules support all four OC3/STM1s on one port.

The cOCx/STMx line module and its corresponding I/O modules can support either E1 or T1 operation. These modules cannot support E1 and T1 operation simultaneously.

Interface Stack

Figure 8 shows the stack for cOCx/STMx interfaces.

Figure 8: Stack for cOCx/STMx Interfaces



NOTE: For a detailed description of interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*. For information about interfaces, see *JUNOSe System Basics Configuration Guide, Chapter 1, Planning Your Network*.

The *section* layer manages the transport of STS/STM frames across the physical path. This layer is responsible for frame alignment, scrambling, error detection, error monitoring, signal reception, and signal regeneration.

The *line* layer manages the transport of SONET/SDH payloads, which are embedded in a sequence of STS/STM frames in the physical medium. This layer is responsible for multiplexing and synchronization.

The *path* layer maps the user payload into a SONET/SDH format suitable for the line layer. This layer transports the actual network services (such as T1s and T3s) between SONET/SDH multiplexing devices and provides end-to-end transmission.

When you configure a cOCx/STMx interface, be sure you understand its position in the SONET or SDH hierarchy. This implementation of SONET and SDH uses the term *path* to identify an STS-1 or STM-1 line. You must know how to identify the path for the configuration and the higher-level *controllers*, such as T3 or unframed E1 over SONET VT.

SONET/SDH VT Controllers

SONET/SDH VT on cOCx/STMx interfaces support these options:

- A fractional T1 or E1 line

  You assign *channel groups* of *timeslots* to configure fractional T1 or E1 over SONET/SDH VT on cOCx/STMx interfaces. A channel group is the fraction of the T1 or E1 line and comprises up to 24 T1 timeslots or up to 31 E1 timeslots. The default channel group speed for both T1 and E1 is 64 Kbps; 56 Kbps is also available.

- An unframed E1 line

  Unframed E1 lines have no timeslots reserved for framing. The router creates one channel for an unframed E1 line and assigns the number one to that channel.

NOTE: To configure a whole T1 or E1 line, assign 24 T1 or 31 E1 timeslots to a channel group or configure an unframed E1 line.

To identify a controller over SONET/SDH VT, you must consider the multiplexing for SONET and SDH *virtual tributaries*. In SONET, an STS-1 frame can be divided into seven virtual tributary (VT) groups. Similarly, for SDH, an STM-0 frame can be divided into seven tributary units (TUs). Each group or unit contains a number of virtual tributaries; that number depends on the VT type or TU name. Table 11 lists the VT types and TU names that the router supports.

Table 11: Tributary Standards That cOCx/STMx Interfaces Support

VT Type (SONET)	TU Name (SDH)	Number of Tributaries in a Group	Signal Standard
VT1.5	TU-11	4	T1
Not supported	TU-12	3	E1

Figure 9 shows the structure for SONET, and Figure 10 shows the structure for SDH.

Figure 9: SONET Multiplexing

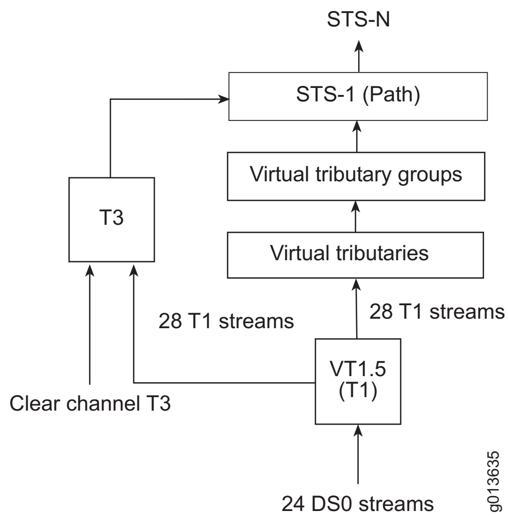
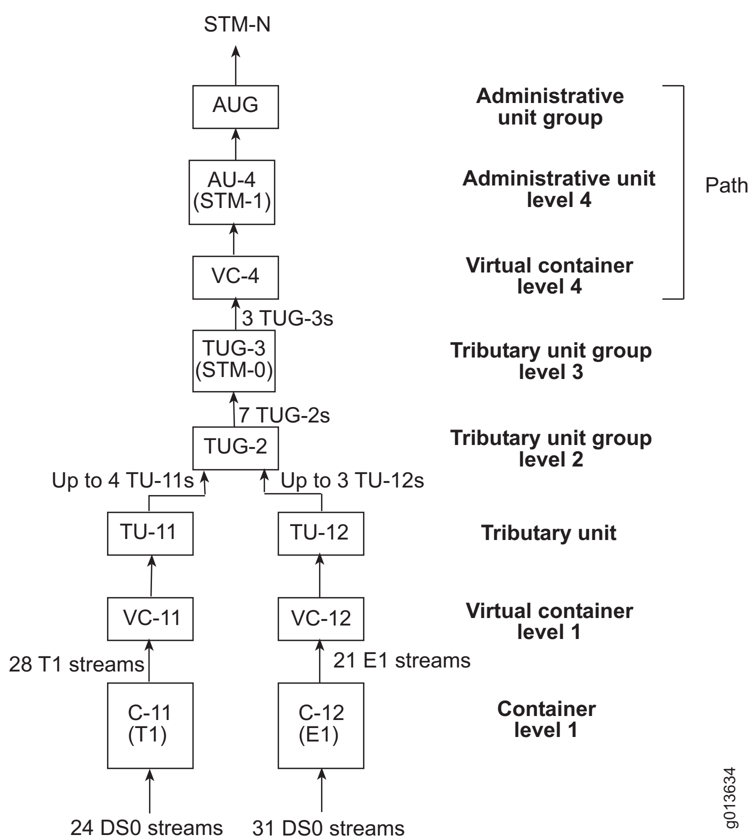


Figure 10: SDH Multiplexing



For both SONET/SDH VT configurations, you must identify the path and controllers above the path layer. Table 12 shows the identifiers for these configurations, and Table 13 provides definitions for the identifiers.

Table 12: Identifiers for SONET/SDH VT Controllers

Configuration	Identifier	Example
Unframed E1	*pathChannel/pathPayload/tributaryGroup/tributaryNumber/channelNumber*	10/1/2/2/1
NOTE: The router automatically assigns the channel number one to an unframed E1 line.		
Fractional T1 or E1	*pathChannel/pathPayload/tributaryGroup/tributaryNumber/channelGroup*	10/1/2/2/1

Table 13: Definitions for Identifiers for SONET/SDH VT Controllers

Identifier	Definition	Value
pathChannel	An STS-1 or STM-1 line	A number in the range 1–2147483648
pathPayload	Number of the payload within the path	In SONET mode, *pathPayload* is always 1. In SDH mode, *pathPayload* is the number of the TUG-3 group.
tributaryGroup	Number of the tributary group within the path	In SONET mode, *tributary group* is the number of the VT group. In SDH mode, *tributaryGroup* is the number of the TUG-2 group.
tributaryNumber	Number of the tributary within the group	In SONET mode, *tributaryNumber* is the number of the VT. In SDH mode, *tributaryNumber* is the number of the TUG-1 group or tributary unit.
channelGroup	A fraction of a T1 or an E1 line	A number in the range 1-24 for T1 or 1-31 for E1

T3 Controllers

You can configure the STS-1 frame to carry a single T3 signal through asynchronous mapping. As Figure 9 on page 107 shows, T3 on cOCx/STMx interfaces supports the following options:

- An unchannelized T3 controller
- A T3 controller channelized to DS0 (fractional T1). To configure fractional T1 over T3 on cOCx/STMx interfaces, you assign *timeslots* (also known as *subchannels*) to the T1 channel. Each T1 channel supports 24 T1 timeslots.

For any configuration, you must identify the path and each controller in the layers above the path layer. For example, for a T3 controller channelized to T1, you must identify the path channel, the T3 channel, and the T1 channel. Table 14 presents the identifiers for the T3 configurations.

Table 14: Identifiers for T3 Controllers

Configuration	identifier	Example
Unchannelized T3	*pathChannel/ds3-channel-number*	1/1
T3 channelized to DS0	*pathChannel/ds3Channel-number/ds1-channel-number/subchannelNumber*	1/1/10/15

HDLC

You must configure HDLC over the T3, unframed E1, or fractional T1/E1 line that you configure on an interface. As Figure 8 on page 105 shows, HDLC is at the top layer of the interface stack.

Numbering Scheme

A cOCx/STMx interface is identified by the *slot/port* format, where:

- *slot*—Number of the slot in which the line module resides in the chassis. In ERX-7xx models, line module slots are numbered 2-6 (slots 0 and 1 are reserved for SRP modules). In ERX-14xx models, line module slots are numbered 0–5 and 8–13 (slots 6 and 7 are reserved for SRP modules). In an ERX-310 router, line module slots are numbered 1–2 (slot 0 is reserved for the SRP module).

- *port*—Number of the port on the I/O module

  A cOC3/STM1 I/O module has four ports. Each port accepts one pair of SC-style fiber connectors.

  The cOC12/STM4 I/O module has one or two ports. On an I/O module that supports two ports, one port is active (primary) and the other is redundant. Cabling both ports provides a redundant path to the interface. If the active port fails, the redundant port automatically becomes active. You can configure only port 0 on a cOC12/STM4 I/O module. Port 0 accepts one pair of SC-style fiber connectors.

  On I/O modules that support APS/MSP, the port numbers for the working (primary) interfaces are assigned the lower half of the numbered interfaces, whereas the port numbers for the protect (redundant) interfaces are assigned the upper half of the numbered interfaces. For example, on an I/O module that provides one primary port and one redundant port, the working interface is port 0 and the protect interface is port 1.

- APS/MSP *channel number*—Identifier of the working or protect interface for configuration purposes

  The protect interface is always assigned channel number 0. The working interface is always assigned channel number 1.

For information about installing line modules and I/O modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

References

For more information about MIB support for cOCx/STMx interfaces, consult the following resources:

- RFC 1661—The Point-to-Point Protocol (PPP) (July 1994)

- RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999)

- RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999)
- RFC 2558—Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999)

For more information about APS/MSP, consult the following resources:

- Telcordia document GR-253—Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, Revision 3 (September 2000)
- ITU-T G.783—Characteristics Of Synchronous Digital Hierarchy (SDH) Multiplexing Equipment Functional Blocks: Annex A – Multiplex Section Protection (MSP) Protocol, Commands And Operation (1990)
- Definitions of Managed Objects for SONET Linear APS Architectures—draft-ietf-atommib-sonetaps-mib-05.txt (November 2001 expiration)
- RFC 3498—Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures (March 2003)

For more information about bit error rate test (BERT) patterns, consult the following resources:

- ITU O.151—Error performance measuring equipment operating at the primary rate and above (October 1992)
- ITU O.153—Basic parameters for the measurement of error performance at bit rates below the primary rate (October 1992)
- T1M1.3 Working Group—A Technical Report on Test Patterns for DS1 Circuits (November 1993)
- ANSI T1.404-1994 Standard for Telecommunications—Network-to-Customer – DS3 Metallic Interface Specification (1994)

For more information about MDL/FDL support on cOCx/STMx interfaces, consult the following resources:

- ANSI T1.107a-1990 Standard for Telecommunications—Digital Hierarchy – Supplement to Formats Specification (August 1990)
- ANSI T1.403-1989 Standard for Telecommunications—Network and Customer Installation Interfaces – DS1 Metallic Interface – Robbed-bit Signaling State Definitions (1989)
- AT&T Technical Reference 54016—Requirements for Interfacing Digital Terminal Equipment to Services Employing the Extended Superframe Format (September 1989)

Before You Configure an Interface

Before you configure a cOCx/STMx interface, verify the following:

- You have installed the line module and the I/O module correctly.
- Each configured line is able to transmit data to and receive data from your switch connections.

For more information about installing modules, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

Make sure you also have the following information available:

- Framing type, clock source, and the cable length for each controller
- Framing type, line code, and clock source for each channel
- Timeslot mapping and line speed for each fractional channel
- HDLC channel information, such as data inversion information, CRC type, idle character, MTU, and MRU

Configuration Tasks

The following sections describe how to configure the layers on cOCx/STMx interfaces.

SONET/SDH Configuration Tasks

To configure SONET/SDH on a cOCx/STMx interface:

1. Select an interface.
2. Specify a clock source for the interface.
3. Specify that the mode be SDH, or accept the default mode, SONET.
4. (Optional) Assign a text description or an alias to the interface.
5. (Optional) Disable processing of SNMP link status information for the section and line layers of the interface.
6. Configure the path for the interface.
7. (Optional—not recommended) Overwrite the automatic setting for the path signal label (C2) byte.
8. (Optional) Enable processing of SNMP link status information for the path layer of the interface.
9. (Optional) Configure the router to use remote defect indications (RDIs) at the path layer to determine the operational status of a path.

10. (MPLS fast reroute over SONET/SDH interfaces) Specify the time duration after which the router sets an alarm when it records a defect at the path layer.

11. (MPLS fast reroute over SONET/SDH interfaces) Specify the time duration after which the router sets an alarm when it records a defect at the line or section layer.

12. Configure APS/MSP for the interface.

    For information about configuring APS/MSP, see *Configuring APS/MSP* in *Chapter 3, Configuring Unchannelized OCx/STMx Interfaces*.

You must now configure the next layer on the interface: E1, T1, or E3. See *T1/E1 Configuration Tasks* on page 116 or *T3 Configuration Tasks* on page 122.

clock source

- Use to configure the transmit clock source for the interface.
- For production networks, configure all STMx ports on the line module for internal chassis timing. You must also ensure that the chassis reference clock is of good quality — Stratum 3 or better, recovered either from a known good STM port or from one of the BITS inputs.
- Although the CLI enables you to specify the keywords **internal module** to use the line module's internal clock, in a production network we recommend that you do not do this. Instead, specify the keywords **internal chassis** to use the router's internal clock.
- For production networks, never specify the keyword **line** to use the line's receive clock as the transmit clock. Although the CLI enables this configuration, it is not supported because jitter transfer is not compliant for this timing and because pointer adjustments takes place on the outgoing link.
- In a nonproduction network, you can configure some ports with internal clock sources and others with line clock sources. However, all ports with internal clock sources must use either the router's clock or the module's clock. You cannot configure some ports on the I/O module to use the router's clock and others to use the module's clock.
- To change the clock source of the ports on a cOC3/STM1 I/O module from the router's clock to the module's clock or vice versa, first change the clock source of all ports to the line setting, and then to the new internal clock setting.
- Example

  host1(config-controll)#**clock source internal chassis**

- Use the **no** version to revert to the default, **line**.

controller sonet

- Use to select an interface on which you want to configure channelized SONET or SDH.
- Example

  host1(config)#**controller sonet 4/0**

- There is no **no** version.

description

- Use to assign a text description or an alias to a channelized SONET interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 64 characters.
- Use the **show controllers sonet** command to display the text description.
- Example

  host1(config-controll)#**description boston-sonet-interface**

- Use the **no** version to remove the text description or alias.

path

- Use to configure paths over channelized SONET and SDH interfaces.
- Specify the correct identifier for the type of interface. See *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide* for details of the syntax.
- Example for a cOC3/STM1 interface

  host1(config-controller)#**path 2 oc1**

- Example for a cOC12/STM4 interface in SONET mode

  host1(config-controller)#**path 2 oc1 1/2**

- Example for a cOC12/STM4 interface in SDH mode

  host1(config-controller)#**path 2 stm1 2**

- Use the **no** version to delete a SONET or SDH path.

path description

- Use to assign a text description or an alias to a channelized SONET path.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 64 characters.
- Example

  host1(config-controll)#**path 2 description westford**

- Use the **no** version to remove the description.

path overhead c2

- Use to overwrite the automatic setting for the path signal label (C2) byte.
- By default, the value of the C2 byte for the path is determined by the layers configured above the SONET/SDH interface and set automatically. The E-series router sets this default value in accordance with RFC 2558. (See *References* on page 109.)

CAUTION: Use this command only if you know that the automatic setting does not match the setting on the remote device. Otherwise, the remote device might send an unexpected value, and the router might lose data.

- Example

  host1(config-controll)#**path 2 overhead c2 20**

- Use the **no** version to restore the default setting, in which the value of the C2 byte is determined by the layers configured above the SONET/SDH interface.

path shutdown

- Use to disable a specified path.
- Paths are enabled by default.
- Example

  host1(config-controll)#**path 2 shutdown**

- Use the **no** version to restart a disabled path.

path snmp trap link-status

- Use to enable SNMP link status processing for the path layer of the interface.
- The default is disabled.
- Example

  host1(config-controll)#**path 2 snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

path trigger alarm prdi

- Use to configure the router to use remote defect indications (RDIs) at the path layer to determine the operational status of a path.
- Example

  host1(config-controll)#**path 2 trigger alarm prdi**

- Use the **no** version to restore the default setting, in which the software uses loss of pointer and AIS defects at the path layer to determine the operational status of a path.

path trigger delay

- Use to set the time duration after which the router sets an alarm when it records a defect at the path layer.
- Change this value from the default only when you are using MPLS fast reroute over a SONET/SDH interface.
  - Specify a value of 0 milliseconds if this interface does not use APS/MSP or if MPLS should have priority over APS/MSP.
  - Specify a value of at least 100 milliseconds if this interface uses APS/MSP and if APS/MSP should have priority over MPLS.
- Example

  host1(config-controll)#**path 2 trigger delay msec 1000**
- Use the **no** version to restore the default setting, 2500 milliseconds.

sdh

- Use to specify that the interface supports SDH.
- Example

  host1(config-controller)#**sdh**
- Use the **no** version to revert to SONET operation on this interface.

snmp trap link-status

- Use to enable SNMP link status processing for the section and line layers of the interface.
- The default is enabled.
- Example

  host1(config-controll)#**no snmp trap link-status**
- Use the **no** version to disable SNMP link status processing.

trigger delay

- Use to set the time duration after which the router sets an alarm when it records a defect at the line or section layer.
- Change this value from the default only when you are using MPLS fast reroute over a SONET/SDH interface.
  - Specify a value of 0 milliseconds if the interface does not use APS/MSP or if MPLS should have priority over APS/MSP.
  - Specify a value of at least 100 milliseconds if this interface uses APS/MSP and if APS/MSP should have priority over MPLS.
- Example

  host1(config-controll)#**trigger delay msec 1000**
- Use the **no** version to restore the default setting, 2500 milliseconds.

Configuring Higher Layers

You must now configure the next layer on the interface: E1, T1, or T3. See *T1/E1 Configuration Tasks* on page 116 or *T3 Configuration Tasks* on page 122.

T1/E1 Configuration Tasks

Before you configure T1 or E1 on an interface, you must configure SONET or SDH. See *SONET/SDH Configuration Tasks* on page 111.

To configure a T1 or an E1 over SONET or SDH on a cOCx/STMx interface:

1. Configure a tributary for the path.
2. (Optional) Assign a text description or an alias to the interface.
3. Configure one of the following:
   - An unframed E1 line. (See *Configuring T1 and E1 Lines* on page 117.)
   - A T1 or an E1 line. (See *Configuring T1 and E1 Lines* on page 117.)

For detailed examples, see *Configuration Examples* on page 133.

path ds1|e1

- Use to create and configure SONET tributaries, SDH tributaries, and T1 or E1 on the path.
- Example

  host1(config-controller)#**path 2 ds1 1/7/4 vt15**
- Use the **no** version to delete SONET and SDH tributaries.

path ds1|e1 description

- Use to assign a text description or an alias to a T1/E1 over SONET/SDH VT layer on channelized SONET and SDH interfaces.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show controllers sonet ds1|e1** command to display the text description.
- Example

  host1(config-controller)#**path 2 ds1 1/7/4 description nyc01**
- Use the **no** version to remove the text description or alias.

Configuring an Unframed E1 Line

Use the following command to configure an unframed E1 line.

path e1 unframed

- Use to configure an unframed E1 on the path.
- You cannot configure a mixture of T1 and E1 lines on the same cOCx/STMx line module.
- When you issue this command, the router creates one channel for the unframed E1 line, and assigns the number one to that channel.
- Example

  host1(config-controller)#**path 1 e1 1/7/4**
  host1(config-controller)#**path 1 e1 1/7/4 unframed**

- Use the **no** version to delete an unframed E1 interface from the path.

Configuring T1 and E1 Lines

You can configure T1 and E1 interfaces on paths and tributaries. To do so, complete the following steps:

1. Configure the clock source. You must coordinate this setting with the other end of the line to establish which end is the transmit (internal) clock and which is the receive (line) clock.
2. (Optional) Configure the framing format.
3. (Optional) Enable processing of SNMP link status information about an interface and its associated tributary.
4. Configure the T1 or E1 line parameters.
5. (Optional) Enable processing of SNMP link status information about a channel group.
6. (Optional—T1 only) Configure FDL messages.
7. (Optional) Assign a text description or an alias to the interface.

path ds1|e1 channel-group description

- Use to assign a text description or an alias to a DS1 (T1) or an E1 channel group for channelized SONET and SDH interfaces.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show controllers sonet ds1|e1** command to display the text description.

- Example

  host1(config-controller)#**path 10 e1 1/5/1 channel-group 4 description westford e1 151.4**

- Use the **no** version to remove the text description or alias.

path ds1|e1 channel-group shutdown

- Use to disable a T1 or an E1 channel group.
- T1 and E1 channel groups are enabled by default.
- Example

  host1 (config-controll)#**path 12 e1 1/4/1 channel-group 2 shutdown**

- Use the **no** version to restart a disabled channel group.

path ds1|e1 channel-group snmp trap link-status

- Use to enable SNMP link status processing for a T1 or an E1 channel group.
- The default is disabled.
- Example

  host1(config-controll)#**path 2 ds1 1/1/1 channel-group 2 snmp trap link-status**

- Use the **no** version to disable SNMP link status processing for a T1 or an E1 channel group.

path ds1|e1 channel-group timeslots

- Use to configure T1 or E1 line parameters.
- You cannot configure a mixture of T1 and E1 lines on the same cOCx/STMx line module.
- Specify a T1 or E1 channel group number, and assign a range of timeslots.
- To configure a whole T1 or E1 line, assign all the timeslots to the channel group.
- You can specify a line speed that applies to all DS0 timeslots assigned to a channel group.
- Example

  host1(config-controll)#**path 2 ds1 1/1/1 channel-group 2 timeslots 5-6**

- Use the **no** version to remove the timeslots from the channel group.

path ds1|e1 clock source

- Use to configure the transmit clock source for the T1 or E1 interface.
- Select a clock as follows:
  - Specify the keyword **line** to use a transmit clock recovered from the line's receive data stream.
  - Specify the keywords **internal module** to use the line module's internal clock.
  - Specify the keywords **internal chassis** to use the router's clock.

- You can usually accept the default option, **line**, to use a transmit clock recovered from the line's receive data stream, except in rare cases such as back-to-back router tests. When performing back-to-back router tests, configure one end of the line as **internal** and the other end as **line**.
- On a cOC3/STM1 I/O module, you can configure some interfaces with internal clock sources and others with line clock sources. However, all interfaces with internal clock sources must use either the router's clock or the module's clock. You cannot configure some interfaces on the I/O module to use the router's clock and others to use the module's clock.
- To change the clock source of the interfaces on a cOC3/STM1 I/O module from the router's clock to the module's clock or vice versa, first change the clock source of all ports to the line setting, and then to the new internal clock setting.
- Example

  host1(config-controll)#**path 12 e1 1/4/1 clock source line**
- Use the **no** version to restore the default value, **line**.

path ds1|e1 framing

- Use to configure the framing format for a T1 or an E1 interface.
- For T1, specify **esf** (extended superframe) or **sf** (superframe). The default is **esf**.
- The HDLC idle character differs from non–E-series implementations. For T1 interfaces, if you configure SF, the router sets the HDLC idle character to 0xFF. If you configure ESF, the router sets the HDLC idle character to 0x7E.
- For E1, specify **crc4** or **no-crc4**. The default is **crc4**.
- Choose a framing format that is compatible with the framing format at the other end of the line.
- Example

  host1(config-controll)#**path 12 e1 1/4/1 framing no-crc4**
- Use the **no** version to restore the default value.

path ds1|e1 snmp trap link-status

- Use to enable SNMP link status processing for a T1 or an E1 interface and its associated tributary.
- The default is disabled.
- Example

  host1(config-controll)#**path 2 ds1 1/1/1 snmp trap link-status**
- Use the **no** version to disable SNMP link status processing.

Configuring T1 Interfaces to Send FDL Messages

You can configure a T1 interface to send FDL messages. To configure FDL:

1. Specify a SONET interface.

   host1(config)#**controller sonet 8/0**

2. Specify the standard for transmission of FDL messages on both ends of the T1 connection.

   host1(config-controll)#**path 2 ds1 1/1/1 fdl ansi**

3. (Optional) Configure the interface to operate in an FDL carrier environment.

   host1(config-controll)#**path 2 ds1 1/1/1 fdl carrier**

4. (Optional) Specify the FDL messages.

   host1(config-controll)#**path 2 ds1 1/1/1 fdl string eic "ERX-1410"**
   host1(config-controll)#**path 2 ds1 1/1/1 fdl string lic "Bldg 10"**
   host1(config-controll)#**path 2 ds1 1/1/1 fdl string fic "GY788"**
   host1(config-controll)#**path 2 ds1 1/1/1 fdl string unit 080001**

5. Enable transmission of FDL messages.

   host1(config-controll)#**path 2 ds1 1/1/1 fdl transmit idle-signal**

path ds1 fdl

- Use to specify the FDL standard for the interface.
- Specify the keyword **ansi** to support the ANSI FDL standard (see *References* on page 109).
- Specify the keyword **att** to support the AT&T FDL standard (see *References* on page 109).
- Specify the keyword **all** to support both the ANSI and AT&T standards.
- Specify the keyword **none** to remove the current FDL mode settings.
- You can configure a different standard on each T1 channel.
- Example

  host1(config-controll)#**path 2 ds1 1/1/1 fdl att**

- Use the **no** version to restore the default, none.

path ds1 fdl carrier

- Use to specify that an interface is used in the carrier environment.
- Example

  host1(config-controll)#**path 2 ds1 1/1/1 fdl carrier**

- Use the **no** version to restore the default situation, in which the T1 interface does not operate in the carrier environment.

path ds1 fdl string

- Use to configure an FDL message as defined in the ANSI T1.403 specification.

NOTE: The router sends these FDL messages only if you have issued the **path ds1 fdl** command with the **ansi** or **all** keyword and then issued the **path ds1 fdl transmit** command.

- Example

  host1(config-controll)#**path 2 ds1 1/1/1 fdl string eic "ERX-1440"**

- Use the **no** version to restore the default value to the specified FDL message or to all FDL messages.

path ds1 fdl transmit

- Use to configure the router to send the specified type of FDL message on the T1 channel.
- By default, the router sends no FDL messages.

NOTE: The router sends FDL messages specified with the **path ds1 fdl string** command only if you have issued the **path ds1 fdl** command with the **ansi** or **all** keyword. If you specified the **att** keyword with the **path ds1 fdl** command, the router sends only performance data.

- Specify the keyword **path-id** to transmit path identifications every second.
- Specify the keyword **idle-signal** to send idle signals every second.
- Specify the keyword **test-signal** to transmit test signals every second.
- Example

  host1(config-controll)#**path 2 ds1 1/1/1 fdl transmit path-id**

- Use the **no** version to disable transmission of the specified FDL message or all FDL messages.

Disabling Interfaces and Channel Groups

To disable interfaces and channel groups, use the following commands.

path ds1|e1 shutdown

- Use to disable a T1 or an E1 interface.
- T1 and E1 interfaces are enabled by default.
- Example

  host1 (config-controll)#**path 12 e1 1/4/1 shutdown**

- Use the **no** version to restart a disabled interface.

Configuring Higher Layers

You must configure HDLC over the top layer of the T1/E1 interface. See *HDLC Channel Configuration Tasks* on page 130.

T3 Configuration Tasks

Before you configure T3 on an interface, you must configure SONET or SDH on the interface. See *SONET/SDH Configuration Tasks* on page 111.

To configure T3 over SONET or SDH on a cOCx/STMx interface, complete the following actions:

1. Configure a T3 path over the SONET and SDH interfaces.
2. Configure T3 line parameters (for both clear channel T3 lines and multiplexed T3 lines composed of fractional T1 lines).
3. (Optional) Configure T1 or fractional T1 line parameters.

For detailed examples, see *Configuration Examples* on page 133.

path ds3

- Use to create and configure a T3 path over SONET and SDH interfaces.
- Example

  host1(config-controller)#**path 2 ds3 1 channelized**

- Use the **no** version to delete a path.

Configuring T3 Line Parameters

Complete the following steps to configure T3 line parameters. Configure these parameters for both clear channel and multiplexed T3 lines.

1. Configure the clock source. You must coordinate this setting with the other end of the line to establish which end is the transmit (internal) clock and which is the receive (line) clock.
2. (Optional) Assign a text description or an alias to the interface.
3. (Optional) Configure the framing format.
4. (Optional) Enable processing of SNMP link status information about an interface.
5. (Optional) Configure MDL settings.
6. (Optional) Configure T1 channels.

path ds3 clock source

- Use to configure the transmit clock source for the T3 line.
- Select a clock as follows:
  - Specify the keyword **line** to use a transmit clock recovered from the line's receive data stream.
  - Specify the keywords **internal module** to use the line module's internal clock.
  - Specify the keywords **internal chassis** to use the router's clock.
- You can usually accept the default option, **line**, to use a transmit clock recovered from the line's receive data stream, except in rare cases such as back-to-back router tests. When performing back-to-back router tests, configure one end of the line as **internal** and the other end as **line**.
- On a cOC3/STM1 I/O module, you can configure some interfaces with internal clock sources and others with line clock sources. However, all interfaces with internal clock sources must use either the router's clock or the module's clock. You cannot configure some interfaces on the I/O module to use the router's clock and others to use the module's clock.
- To change the clock source of the interfaces on a cOC3/STM1 I/O module from the router's clock to the module's clock or vice versa, first change the clock source of all ports to the line setting, and then to the new internal clock setting.
- Example

  host1(config-controll)#**path 12 ds3 1 clock source line**

- Use the **no** version to restore the default value, **line**.

path ds3 description

- Use to assign a text description or an alias to a T3 (DS3) over channelized SONET/SDH interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show controllers sonet ds3** command to display the text description.
- Example

  host1(config-controller)#**path 12 ds3 1 description boston_t3**

- Use the **no** version to remove the text description or alias.

path ds3 framing

- Use to configure the framing format for a T3 interface.
- Specify **c-bit** parity framing or **m23** multiplexer framing.
- Example

  host1(config-controll)#**path 12 ds3 1 framing m23**

- Use the **no** version to restore the default value, **c-bit** parity framing.

path ds3 shutdown

- Use to disable a T3 interface.
- T3 interfaces are enabled by default.
- Example

  host1(config-controll)#**path 12 ds3 1 shutdown**

- Use the **no** version to restart a disabled interface.

path ds3 snmp trap link-status

- Use to enable SNMP link status processing for a T3 interface.
- The default disables SNMP link status processing.
- Example

  host1(config-controll)#**path 12 ds3 1 snmp trap link-status**

- Use the **no** version to disable SNMP link status processing.

Configuring T3 Interfaces to Send MDL Messages

You can configure a T3 interface to send MDL messages. MDL messages are supported only when the T3 framing is set for C-bit parity, the default setting.

To configure a T3 interface to send MDL messages:

1. Specify a SONET interface.

   host1(config)#**controller sonet 8/0**

2. (Optional) Configure the interface to operate in an MDL carrier environment.

   host1(config-controll)#**path 12 ds3 1 mdl carrier**

3. Specify the MDL messages.

   host1(config-controll)#**path 12 ds3 1 mdl string eic "ERX 1410"**
   host1(config-controll)#**path 12 ds3 1 mdl string fic "FG786"**
   host1(config-controll)#**path 12 ds3 1 mdl string lic "Bldg 2"**
   host1(config-controll)#**path 12 ds3 1 mdl string pfi "Site 1"**
   host1(config-controll)#**path 12 ds3 1 mdl string port 0800**
   host1(config-controll)#**path 12 ds3 1 mdl string unit 080001**

4. Enable transmissions of MDL messages.

   host1(config-controll)#**path 12 ds3 1 mdl transmit path-id**
   host1(config-controll)#**path 12 ds3 1 mdl transmit idle-signal**
   host1(config-controll)#**path 12 ds3 1 mdl transmit test-signal**

path ds3 mdl carrier

- Use to specify that an interface is used in the carrier environment.
- Example

  host1(config-controll)#**path 12 ds3 1 mdl carrier**

- Use the **no** version to restore the default situation, in which the interface does not operate in the carrier environment.

path ds3 mdl string

- Use to specify an MDL message.
- Example

  host1(config-controll)#**path 12 ds3 1 mdl string port 0800**

- Use the **no** version to restore the default value to the specified MDL message or to all MDL messages.

path ds3 mdl transmit

- Use to enable transmission of MDL messages.
- Specify the keyword **path-id** to transmit path identifications every second.
- Specify the keyword **idle-signal** to send idle signals every second.
- Specify the keyword **test-signal** to transmit test signals every second.
- Example

  host1(config-controll)#**path 12 ds3 1 mdl transmit test-signal**

- Use the **no** version to disable transmission of the specified type of MDL messages or all MDL messages.

Configuring T1 Channels on T3 Interfaces

To configure T1 and fractional T1 channels over T3 interfaces:

1. Configure the T1 path.
2. Configure the clock source.

   You must coordinate this setting with the other end of the line to establish which end is the transmit (internal) clock and which is the receive (line) clock.
3. (Optional) Assign a text description or an alias to the interface.
4. (Optional) Configure the framing format.
5. (Optional) Enable processing of SNMP link status information about an interface.
6. Configure the T1 line parameters.

   You can specify parameters for a single channel, multiple individual channels, ranges of channels, or any combination of the three types of specifications. For example:

   host1(config-controll)#**path 12 ds3 1 t1 25-28**
7. (Optional) Enable processing of SNMP link status information about a channel group.

path ds3 t1

- Use to create and configure the T1 path over SONET and SDH interfaces.
- Example

  host1(config-controll)#**path 12 ds3 1 t1 25-28**
- Use the **no** version to delete a path.

path ds3 t1 clock source

- Use to configure the transmit clock source for the T3 line.
- Use a transmit clock recovered from the line's receive data stream, except in rare cases such as back-to-back router tests. When performing back-to-back router tests, configure one end of the line as **internal** and the other end as **line**.
- Specify the keyword **line** to use a transmit clock recovered from the line's receive data stream.
- Specify the keywords **internal module** to use the line module's internal clock.
- Specify the keywords **internal chassis** to use the router's clock.
- On a cOC3/STM1 I/O module, you can configure some ports with internal clock sources and others with line clock sources. However, all ports with internal clock sources must use either the router's clock or the module's clock. You cannot configure some ports on the I/O module to use the router's clock and others to use the module's clock.

- To change the clock source of the ports on a cOC3/STM1 I/O module from the router's clock to the module's clock or vice versa, change the clock source of all ports first to the line setting, and then to the new internal clock setting.
- Example

  host1(config-controll)#**path 12 ds3 1 t1 28 clock source internal chassis**

- Use the **no** version to restore the default value, **line** clocking.

path ds3 t1 description

- Use to assign a text description or an alias to a T1 or fractional T1 channel on a T3 (DS3) over channelized SONET/SDH interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show controllers sonet ds3** command to display the text description.
- Examples

  host1(config-controller)#**path 12 ds3 1 t1 28 description boston_t1_on_t3**
  host1(config-controller)#**path 12 ds3 1 t1 28/5**
  description washington_fractional_t1_on_t3

- Use the **no** version to remove the text description or alias.

path ds3 t1 framing

- Use to configure the T1 framing format for a T3 interface.
- You must specify either **esf** (extended superframe) or **sf** (superframe) framing.
- The framing format you choose must be compatible with the framing format at the other end of the line.
- Example

  host1(config-controll)#**path 12 ds3 1 t1 28 framing sf**

- Use the **no** version to restore the default value, **esf** framing.

path ds3 t1 shutdown

- Use to disable T1 channels or a subchannel.
- T1 channels and subchannels are enabled by default.
- Examples

  host1(config-controll)#**path 12 ds3 t1 5,9,14-17 shutdown**
  host1(config-controll)#**path 12 ds3 t1 28/5 shutdown**

- Use the **no** version to restart a disabled interface.

path ds3 t1 snmp trap link-status

- Use to enable SNMP link status processing for T1 channels or a subchannel.
- The default disables SNMP link status processing.
- Examples

  host1(config-controll)#**path 2 ds3 3 t1 28 snmp trap link-status**
  host1(config-controll)#**path 2 ds3 3 t1 28/5 snmp trap link-status**

- Use the **no** version to disable SNMP link status processing for a T1 channel.

path ds3 t1 timeslots

- Use to assign a range of DS0 timeslots to a subchannel as a single data stream.
- You can specify a line speed for all DS0 timeslots assigned to a subchannel.
- Examples

  host1(config-controll)#**path 2 ds3 1 t1 28 timeslots 1-10**
  host1(config-controll)#**path 2 ds3 1 t1 28/1 timeslots 1-10 speed 56**

- Use the **no** version to delete the fractional T1 circuit.

Configuring T1 Channels to Send FDL Messages

To configure T1 channels to send FDL messages:

1. Specify a SONET interface.

   host1(config)#**controller sonet 8/0**

2. Specify the standard for transmission of FDL messages on both ends of the T1 connection.

   host1(config-controll)#**path 2 ds3 1 t1 28 fdl ansi**

3. (Optional) Configure the interface to operate in an FDL carrier environment.

   host1(config-controll)#**path 2 ds3 1 t1 28 fdl carrier**

4. (ANSI signals) Specify the FDL messages.

   host1(config-controll)#**path 2 ds3 1 t1 28 fdl string eic "ERX-1410"**
   host1(config-controll)#**path 2 ds3 1 t1 28 fdl string lic "Bldg 10"**
   host1(config-controll)#**path 2 ds3 1 t1 28 fdl string fic "GY788"**
   host1(config-controll)#**path 2 ds3 1 t1 28 fdl string unit 080001**

5. Enable transmission of FDL messages.

   host1(config-controll)#**path 2 ds3 1 t1 28 fdl transmit idle-signal**

path ds3 t1 fdl

- Use to specify the FDL standard for the interface.
- Specify the T1 channels in the range 1 through 28.
- Specify the keyword **ansi** to support the ANSI FDL standard (see *References* on page 109).
- Specify the keyword **att** to support the AT&T FDL standard (see *References* on page 109).
- Specify the keyword **all** to support both the ANSI and AT&T standards
- Specify the keyword **none** to remove the current FDL mode settings
- You can configure a different standard on each T1 channel.
- Example

  host1(config-controll)#**path 2 ds3 1 t1 20-28 fdl att**

- Use the **no** version to restore the default, no specified FDL standard.

path ds3 t1 fdl carrier

- Use to specify that T1 channels are used in the carrier environment.
- Example

  host1(config-controll)#**path 2 ds3 1 t1 4,6,10-14 fdl carrier**

- Use the **no** version to restore the default situation, in which the T1 channel does not operate in the carrier environment.

path ds3 t1 fdl string

- Use to configure an FDL message as defined in the ANSI T1.403 specification.

NOTE: The router sends these FDL messages only if you have issued the **path ds3 t1 fdl** command with the **ansi** or **all** keyword and then issued the **path ds3 t1 fdl transmit** command.

- Example

  host1(config-controll)#**path 2 ds3 1 t1 28 fdl string eic "ERX-1440"**

- Use the **no** version to restore the default value to the specified FDL message or to all FDL messages.

path ds3 t1 fdl transmit

- Use to configure the router to send the specified type of FDL message.
- By default, the router sends only FDL performance data messages.

NOTE: The router sends FDL messages specified with the **path ds3 t1 fdl string** command only if you have issued the **path ds3 t1 fdl** command with the **ansi** or **all** keyword. If you specified the **att** keyword with the **path ds3 t1 fdl** command, the router sends only performance data.

- Specify the keyword **path-id** to transmit path identifications every second.
- Specify the keyword **idle-signal** to send idle signals every second.
- Specify the keyword **test-signal** to transmit test signals every second.
- Example

  host1(config-controll)#**path 2 ds3 1 t1 28 fdl transmit path-id**

- Use the **no** version to disable transmission of the specified FDL message or all FDL messages.

Configuring Higher Layers

You must configure HDLC over the top layer of the T3 interface. See *HDLC Channel Configuration Tasks* on page 130.

HDLC Channel Configuration Tasks

You must configure HDLC over the T3, T1, unframed E1, or fractional T1/E1 line that you configure on an interface. As Figure 8 on page 105 shows, HDLC must be the top layer of the interface stack.

To configure an HDLC channel, specify a serial interface. For example:

host1(config)#**interface serial 4/0:1/1/1/1**

Optional Tasks

The following configuration tasks are optional when you configure an HDLC channel on a channelized T3 interface:

- Configure the CRC.
- Configure the HDLC idle character.
- Enable data inversion on the interface.
- Set the MRU.
- Set the MTU.
- Assign a text description or an alias to the serial interface.

crc

- Use to configure the size of the CRC.
- Specify the number of bits (16 or 32) that are used to calculate the frame check sequence (FCS). Both the sender and receiver must use the same setting.
- The CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data.

- A 32-bit CRC should be used to protect longer streams at faster rates and, therefore, provide better ongoing error detection.
- Example

  host1(config-if)#**crc 32**

- Use the **no** version to restore the default, 16.

idle-character

- Use to configure the HDLC idle character.
- The idle character is sent between HDLC packets.
- Specify one of the following idle characters:
  - **flags**—Sets the idle character to 0x7E
  - **marks**—Sets the idle character to 0xFF
- Example

  host1(config-ifs)#**idle-character marks**

- Use the **no** version to restore the default value, 0x7E (flags).

interface serial

- Use to specify a serial interface.
- Example for unframed E1 interface

  host1(config)#**interface serial 4/0:1/1/1/1/1**

- Example for fractional T1/E1 interface

  host1(config)#**interface serial 4/0:1/1/1/1/1**

- Example for unchannelized T3 interface

  host1(config)#**interface serial 4/0:1/1**

- Example for T3 interface channelized to fractional T1

  host1(config)#**interface serial 4/0:1/1/10/22**

- Use the **no** version to remove the interface.

invert data

- Use to enable data stream inversion for the interface.
- Enable data stream inversion only if it is turned on at the other end of the line.
- Example

  host1(config-if)#**invert data**

- Use the **no** version to disable the feature.

mru

- Use to configure the MRU size for the interface.
- Specify a value in the range 4–9996 bytes.
- Coordinate this value with the network administrator on the other end of the line.
- If you set this value with a different value for another protocol, such as IP, the router uses the lower value. The lower MRU might cause unexpected results in the network.
- Example

  host1(config-if)#**mru 1500**
- Use the **no** version to restore the default, 1600 bytes.

mtu

- Use to configure the MTU size for the interface.
- Specify a value in the range 4–9996 bytes.
- You should coordinate this value with the network administrator on the other end of the line.
- You can set a different MTU value in higher-level protocols, such as IP. If you do, the router uses the lower value. The lower MTU might cause unexpected results in the network.
- Example

  host1(config-if)#**mtu 1500**
- Use the **no** version to restore the default, 1600 bytes.

serial description

- Use to assign a text description or an alias to a serial HDLC interface.
- You can use this command to help you identify the interface and keep track of interface connections.
- The description or alias can be a maximum of 80 characters.
- Use the **show interfaces serial** command to display the text description.
- Example

  host1(config-if)#**serial description ottawa012 hdlc channel**
- Use the **no** version to remove the text description or alias.

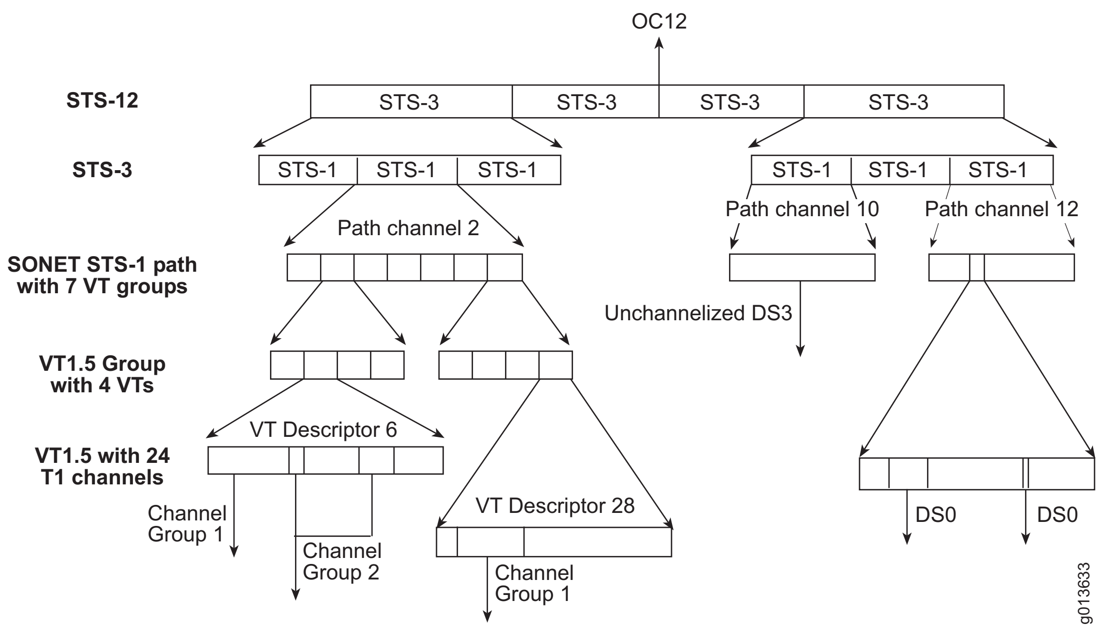
Configuration Examples

This section provides some configuration examples to illustrate how to use the CLI commands.

Example 1: Configuring Interfaces in SONET Mode

The following example illustrates how to configure T1 lines on channelized SONET interfaces, as shown in Figure 11.

Figure 11: Configuring Fractional T1 in SONET Mode



1. Select an OC-12 SONET controller.

   host1(config)#**controller sonet 4/0**

2. Configure two STS-1 paths.

   host1(config-controller)#**path 2 oc1 1/2**
   host1(config-controller)#**path 10 oc1 4/1**

3. Configure two VT1.5 tributaries on SONET path channel 2.

   host1(config-controller)#**path 2 ds1 1/2/2 vt15**
   host1(config-controller)#**path 2 ds1 1/7/4 vt15**

4. Configure two fractional T1 lines on VT 1/2/2 in path 2.

   host1(config-controller)#**path 2 ds1 1/2/2 channel-group 1 timeslots 1-10**
   host1(config-controller)#**path 2 ds1 1/2/2 channel-group 2 timeslots 11, 21-26**

5. Configure a fractional T1 line on VT 1/7/4 in path 2.

   host1(config-controller)#**path 2 ds1 1/7/4 channel-group 1 timeslots 2-7**
6. Configure an unchannelized T3 on SONET path channel 10.

   host1(config-controller)#**path 10 ds3 1 unchannelized**

7. Configure a channelized T3 on SONET path channel 12.

   host1(config-controller)#**path 12 ds3 1 channelized**

8. Configure a T1 channel on the channelized T3 on SONET path channel 12.

   host1(config-controller)#**path 12 ds3 1 t1 4**

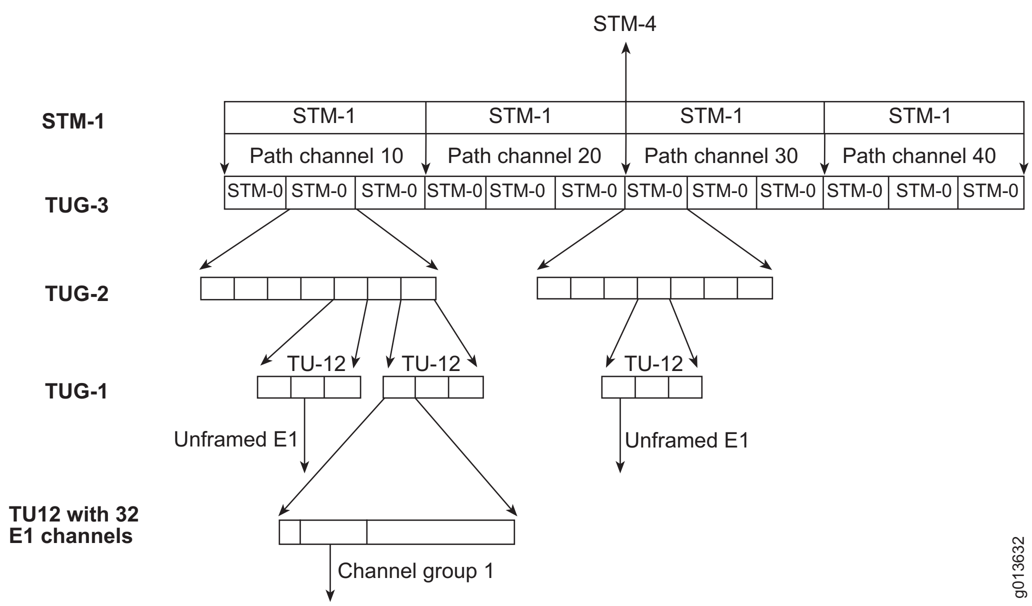
9. Configure two fractional T1 lines on the T3 in path channel 12.

   host1(config-controller)#**path 12 ds3 1 t1 4/1 timeslots 3-8**
   host1(config-controller)#**path 12 ds3 1 t1 4/2 timeslots 20**

Example 2: Configuring Interfaces in SDH Mode

The following example illustrates how to configure fractional E1 and unframed E1 lines in SDH mode, as shown in Figure 12.

Figure 12: Configuring Fractional E1 and Unframed E1 in SDH Mode



1. Select an OC-12 SONET controller.

   host1(config)#**controller sonet 4/0**

2. Switch to SDH mode.

   host1(config-controller)#**sdh**

3. Configure four STM-1 paths. An OC-12 interface has four STM-1 paths.

   host1(config-controller)#**path 10 stm1 1**
   host1(config-controller)#**path 20 stm1 2**
   host1(config-controller)#**path 30 stm1 3**
   host1(config-controller)#**path 40 stm1 4**

4. Configure a TU-12 on TUG-2 #7 on TUG-3 #2 of path 10.

   host1(config-controller)#**path 10 e1 2/7/1 tu12**

5. Configure a TU-12 on TUG-2 #5 on TUG-3 #2 of path 10.

   host1(config-controller)#**path 10 e1 2/5/2 tu12**

6. Configure a fractional E1 line on tributary 2/7/1 of path 10.

   host1(config-controller)#**path 10 e1 2/7/1 channel-group 1 timeslots 2-5**

7. Configure an unframed E1 line on tributary 2/5/2 of path 10.

   host1(config-controller)#**path 10 e1 2/5/2 unframed**

8. Configure a TU-12 on TUG-2 #4 on TUG-3 #1 of path 30.

   host1(config-controller)#**path 30 e1 1/4/1 tu12**

9. Configure an unframed E1 line on tributary 1/4/1 of path 30.

   host1(config-controller)#**path 30 e1 1/4/1 unframed**

Example 3: Configuring Frame Relay

The following example illustrates how to configure Frame Relay on VT 1/7/4 in path 2 of the configuration shown in Figure 11.

1. Select the interface on which you want to configure Frame Relay.

   host1(config)#**interface serial 4/0:2/1/7/4/1**

2. Specify Frame Relay as the encapsulation method on the interface.

   host1(config-if)#**encapsulation frame-relay ietf**

3. Configure the interface as a DTE, DCE, or NNI.

   host1(config-if)#**frame-relay intf-type dce**

Example 4: Configuring PPP

The following example illustrates how to configure PPP on VT 1/2/2 in path 2 of the configuration shown in Figure 11.

1. Select the interface on which you want to configure PPP.

   host1(config)#**interface serial 4/0:2/1/2/2/1**

2. Specify PPP as the encapsulation method on the interface.

   host1(config-if)#**encapsulation ppp**

Testing Interfaces

Testing interfaces allows you to troubleshoot problems and to check the quality of links at various layers in the interface stack. The router supports the following test options:

- Transmission of BERT patterns to remote devices
- Receipt of BERT patterns from remote devices
- Local loopback—The ability to loop the data back toward the router; on supported line modules, also sends an alarm indication signal (AIS) out toward the network
- Network loopback—The ability to loop the data toward the network before the data reaches the frame
- Remote loopback, which provides:
  - The ability to request that remote devices enter into loopback
  - The ability to be placed in loopback by remote devices
- Connectivity tests to remote devices

Sending BERT Patterns

The router can send BERT patterns from different layers in the interface stack. For a list of the modules that support bit error rate tests (BERTs), see *ERX Module Guide, Appendix A, Module Protocol Support*.

To send BERT patterns:

1. Select a controller.
2. Configure a specific layer in the interface to generate BERT patterns.

   For information about BERT patterns, see *References* on page 109.

path ds1|e1 bert

- Use to enable bit error rate tests using the specified pattern at the T1/E1 over SONET/SDH VT layer.
- Unlike other configuration commands, **path ds1|e1 bert** is not stored in NVRAM.
- Specify one of the following options:
  - **2^11**—Pseudorandom test pattern, 2047 bits in length
  - **2^15**—Pseudorandom test pattern, 32,767 bits in length
  - **2^20-O153**—Pseudorandom test pattern, 1,048,575 bits in length
- Specify the duration of the test in the range 1–1440 minutes.
- Optionally, specify the **unframed** keyword to overwrite the framing bits.
- Example

  host1(config-controll)#**path 12 ds1 1/3/4 bert pattern 2^11 interval 10 unframed**

- Use the **no** version to stop the test that is running.

path ds3 bert

- Use to enable bit error rate tests using the specified pattern at the T3 layer.
- Unlike other configuration commands, **path ds3 bert** is not stored in NVRAM.
- Specify one of the following options:
  - **0s**—Repetitive test pattern of all zeros, 00000...
  - **1s**—Repetitive test pattern of all ones, 11111...
  - **2^9**—Pseudorandom test pattern, 511 bits in length
  - **2^11**—Pseudorandom test pattern, 2047 bits in length
  - **2^15**—Pseudorandom test pattern, 32,767 bits in length
  - **2^20**—Pseudorandom test pattern, 1,048,575 bits in length
  - **2^20-QRSS**—Pseudorandom QRSS test pattern, 1,048,575 bits in length
  - **2^23**—Pseudorandom test pattern, 8,388,607 bits in length
  - **alt-0-1**—Repetitive alternating test pattern of zeros and ones, 01010101...
- Specify the duration of the test in the range 1–1440 minutes.
- Example

  host1(config-controll)#**path 12 ds3 2 bert pattern 0s interval 10**

- Use the **no** version to stop the test that is running.

path ds3 t1 bert

- Use to enable bit error rate tests using the specified pattern at the T1 over T3 layer.
- Unlike other configuration commands, **path ds3 t1 bert** is not stored in NVRAM.
- Specify one of the following options:
  - **2^11**—Pseudorandom test pattern, 2047 bits in length
  - **2^15**—Pseudorandom test pattern, 32,767 bits in length
  - **2^20-O153**—Pseudorandom test pattern, 1,048,575 bits in length
- Specify the duration of the test in the range 1–1440 minutes.
- Optionally, specify the **unframed** keyword to overwrite the framing bits.
- Example

  host1(config-controll)#**path 12 ds3 2 t1 14 bert pattern 2^11 interval 10 unframed**

- Use the **no** version to stop the test that is running.

Receiving BERT Patterns

The router can receive BERT patterns from a remote device at the T1/E1 over SONET/SDH VT and T1/E1 over T3 layers. To receive BERT patterns, configure the interface on the router for network payload loopback and the remote interface to use the line clock. Inaccurate results might occur if you use other loopback modes or clock sources.

When the router is synchronized with and receiving BERT patterns from a remote device, the router records the number of bit errors and the number of bits received. To view these statistics, issue the **show controllers sonet** command.

Enabling Local or Network Loopback

You can enable loopback tests on the router at the following layers in the interface stack:

- SONET/SDH section layer
- T1/E1 over SONET/SDH VT layer
- T3 layer
- T1/E1 over T3 layer

See *Interface Stack* on page 105 for a description of the layers.

To enable local or network loopback:

1. Select a controller.
2. Configure local or network loopback at the desired layers in the interface.

loopback

- Use to configure the type of loopback at the SONET/SDH section layer.
- Specify one of the following options:
  - **local**—Loops the data back toward the router; on supported line modules, also sends an alarm indication signal (AIS) out toward the network.
  - **network**—Loops the data toward the network before the data reaches the frame.
- Example

  host1(config)#**controller sonet 4/0**
  host1(config-controller)#**loopback network**

- Use the **no** version to disable loopback.

path ds1|e1 loopback

- Use to configure a loopback at the T1/E1 over SONET/SDH VT layer.
- Specify one of the following options:
  - **local**—Loops the router output data back toward the router at the T1/E1 framer; on supported line modules, also sends an alarm indication signal (AIS) out toward the network.
  - **network { line | payload }**
    - Specify the **line** keyword to loop the data back toward the network before the T1/E1 framer and automatically set a local loopback at the HDLC controllers.
    - Specify the **payload** keyword to loop the payload data back toward the network at the T1/E1 framer and automatically set a local loopback at the HDLC controllers.
- Example

  host1(config-controll)#**path 12 ds1 1/3/4 loopback network line**

- Use the **no** version to clear the local loopback configuration.

path ds3 loopback

- Use to configure a loopback at the T3 layer.
- Specify one of the following options:
  - **local**—Loops the data back toward the router; on supported line modules, also sends an alarm indication signal (AIS) out toward the network.
  - **network { line | payload }**
    - Specify the **line** keyword to loop the data toward the network before the data reaches the framer.
    - Specify the **payload** keyword to loop the data toward the network after the framer has processed the data.

- Example

  host1(config-controll)#**controller sonet 5/0**
  host1(config-controll)#**path 12 ds3 1 loopback local**

- Use the **no** version to turn off the loopback.

path ds3 t1 loopback

- Use to configure a loopback at the T1 over T3 layer.
- Specify one of the following options:
  - **local**—Loops the router output data back toward the router at the T1 framer; on supported line modules, also sends an alarm indication signal (AIS) out toward the network.
  - **network { line | payload }**
    - Specify the **line** keyword to loop the data back toward the network before the T1 framer and automatically set a local loopback at the HDLC controllers.
    - Specify the **payload** keyword to loop the payload data back toward the network at the T1 framer and automatically set a local loopback at the HDLC controllers.
- Example

  host1(config-controll)#**path 12 ds3 2 t1 14 loopback network line**

- Use the **no** version to clear the local loopback configuration.

Enabling Remote Loopback Testing

You can configure the router to request that compatible devices connected at the following layers enter into a loopback:

- T1 over SONET/SDH VT layer
- T1 over T3 layer
- T3 layer

You can also configure the router to start loopback testing when it receives an appropriate signal from a devices connected at any of these layers.

For a list of the modules that support remote loopback, see *ERX Module Guide, Appendix A, Module Protocol Support*.

NOTE: There is no protocol that allows remote loopback on E1 links.

To enable remote loopback:

1. Select a controller.
2. Configure remote loopback at the desired layers in the interface.

path ds1|e1 loopback remote

- Use to place a remote device, connected at the T1 over SONET/SDH VT layer, in loopback.
- Specify one of the following options:
  - **line fdl ansi** (T1 only)—Sends a repeating 16-bit ESF data link code word (00001110 11111111) to the remote end requesting that it enter into a network line loopback. Specify the **ansi** keyword to enable the remote line facilities data link (FDL) ANSI bit loopback on the T1 line, according to the ANSI T1.403 specification.
  - **line fdl bellcore** (T1 only)—Sends a repeating 16-bit ESF data link code word (00010010 11111111) to the remote end requesting that it enter into a network line loopback. Specify the **bellcore** keyword to enable the remote line FDL Bellcore bit loopback on the T1 line, according to the Bellcore TR-TSY-000312 specification.
  - **payload** [**fdl**] [**ansi**] (T1 only)—Sends a repeating 16-bit ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 line. You can optionally specify **fdl** and **ansi**.
- Example

  host1(config-controll)#**path 12 ds1 1/3/4 loopback remote line fdl ansi**

- Use the **no** version to send the 16-bit ESF data link code word to deactivate the loopback at the remote end, depending on the last activate request sent to the remote end.

path ds1 remote-loopback

- Use to enable the router to accept remote loopback requests from a remote device connected at the T1 over SONET/SDH VT layer.
- Example

  host1(config-controll)#**path 12 ds1 1/3/4 remote-loopback**

- Use the **no** version to restore the default, which is to reject remote loopback requests.

path ds3 equipment loopback

- Use to enable or disable the router's ability to enter into a loopback initiated by a remote device connected at the T3 layer.

NOTE: Remote loopback is available only on frame-based T3 interfaces configured to use C-bit framing.

- Specify one of the following loopback options:
  - **customer**—Enables the router to enter into loopback when it receives an appropriate signal from the remote interface
  - **network**—Disables the router's ability to enter into loopback when it receives an appropriate signal from the remote interface; this is the default behavior

- Examples

  host1(config-controll)#**path 12 ds3 2 equipment customer loopback**
  host1(config-controll)#**path 12 ds3 2 equipment network loopback**

- Use the **no** version to restore the default behavior, which disables the router's ability to be placed in loopback by a remote device. Using the **no** version has the same effect as issuing the command with the network keyword.

path ds3 loopback remote

- Use to place a remote device, connected at the T3 layer, in loopback.
- Specify the **remote** keyword to send a far end alarm code in the C-bit framing, as defined in ANSI T1.404, to notify the remote end to activate or (when you use the **no** version) deactivate the line loopback.

NOTE: Remote loopback is available only on frame-based T3 interfaces configured to use C-bit framing.

- Example

  host1(config)#**controller sonet 5/0**
  host1(config-controll)#**path 12 ds3 1 loopback remote**

- Use the **no** version to turn off the loopback.

path ds3 t1 loopback remote

- Use to place a remote device, connected at the T1 over T3 layer, in loopback.
- Specify one of the following options:
  - **line fdl ansi**—Sends a repeating 16-bit ESF data link code word (00001110 11111111) to the remote end requesting that it enter into a network line loopback. Specify the **ansi** keyword to enable the remote line FDL ANSI bit loopback on the T1 line, according to the ANSI T1.403 specification.
  - **line fdl bellcore**—Sends a repeating 16-bit ESF data link code word (00010010 11111111) to the remote end requesting that it enter into a network line loopback. Specify the **bellcore** keyword to enable the remote line FDL Bellcore bit loopback on the T1 line, according to the Bellcore TR-TSY-000312 specification.
  - **payload** [**fdl**] [**ansi**]—Sends a repeating 16-bit ESF data link code word (00010100 11111111) to the remote end requesting that it enter into a network payload loopback. Enables the remote payload FDL ANSI bit loopback on the T1 line. You can specify **fdl** or **ansi**.
- Example

  host1(config-controll)#**path 12 ds3 2 t1 14 loopback remote payload**

- Use the **no** version to send the 16-bit ESF data link code word to deactivate the loopback at the remote end, depending on the last activate request sent to the remote end.

path ds3 t1 remote-loopback

- Use to enable the router to accept remote loopback requests from a remote device connected at the T1 over T3 layer.
- Example

  host1(config-controll)#**path 12 ds3 2 t1 14 remote-loopback**

- Use the **no** version to restore the default, which is to reject remote loopback requests.

Testing Connectivity

Use the **path overhead j1** command to check for connectivity between the router and a SONET/SDH device at the other end of the line. This command defines:

- A message that the router sends from the specified interface to the SONET/SDH device at the other end of the line.
- A message that the router expects to receive on the specified interface from the SONET/SDH device at the other end of the line.

When you define a message that the interface sends, you must monitor receipt of that message at the remote end.

When you define a message that the interface expects to receive, you should configure the remote device to transmit the same message to the interface. You can then use the **show controllers sonet** command to compare the expected and received messages.

path overhead j1

- Use to define messages that the router sends to or expects to receive from a SONET/SDH device connected to a cOCx/STMx interface.
- Specify a path identifier between 1 and 2,147,483,648 for a cOCx/STMx interface.
- Specify the keyword **msg** for a message that the router transmits for this path.
- Specify the keyword **exp-msg** to define a message that the router expects to receive on this path.
- Define a message of up to 62 characters for SONET or up to 15 characters for SDH.
- Configure the remote device to send the same message that the router expects to receive on this path. You can then compare the expected and received messages in the display of the **show controllers sonet** command.
- Example for cOCx/STMx interface:

  host1(config-controller)#**path 2 overhead j1 exp-msg goodbye**

- Use the **no** version to restore the default situation, in which all the characters in the transmitted or expected message are zeros.

Monitoring Interfaces

To display statistics for channelized SONET and SDH interfaces, use the **show controllers sonet** command. The following section describes some of the options for the command and shows some sample displays.

From User Exec mode, use the following **show** commands to monitor and display the T3, T1/E1, and HDLC serial data channel information:

- Display E1 or T1 statistics for E1 or T1 over a VT.

  host1#**show controllers sonet 2/0 e1**

- Display T3 statistics.

  host1#**show controllers sonet 2/1 ds3**

- Display statistics for the section, line, path, and tributary layers.

  host1#**show controllers sonet 2/1 section**

- Display the configuration for channelized SONET and SDH interfaces.

  host1#**show controllers sonet 2/0 configuration**

- Display statistics for serial interfaces.

  host1#**show interfaces serial 2/0:1/1/1/1/1**

Setting a Baseline

You can set statistics baselines for serial interfaces, subinterfaces, and circuits using the **baseline interface serial** command. You can also set statistics baselines for the section, line, and path layers using the **baseline interface sonet** command. Use the **delta** options with the **show** commands to display statistics with the baseline subtracted.

Output Filtering

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*, for details.

baseline interface serial

- Use to set a statistics baseline for serial interfaces.
- The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **delta** keyword with the **show interfaces serial** command to view the baseline statistics.

- Example

  host1#**baseline interface serial 2/0:1/1**

- There is no **no** version.

baseline line interface sonet

- Use to set a statistics baseline for the SONET/SDH line layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet line** command to view the baseline statistics.
- Example

  host1#**baseline line interface sonet 2/0**

- There is no **no** version.

baseline path interface sonet

- Use to set a statistics baseline for the SONET/SDH path layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet path** command to view the baseline statistics.
- Example

  host1#**baseline path interface sonet 2/0:1**

- There is no **no** version.

baseline section interface sonet

- Use to set a statistics baseline for the SONET/SDH section layer.
- The router implements the baseline by reading and storing the MIB statistics at the time the baseline is set and then subtracting this baseline whenever baseline-relative statistics are retrieved.
- Use the **total** [**delta**] keywords with the **show controllers sonet section** command to view the baseline statistics.
- Example

  host1#**baseline section interface sonet 2/0**

- There is no **no** version.

show controllers sonet configuration

- Use to display the configuration for channelized SONET and SDH interfaces.
- Specify an interface in *slot/port* format.
- To view information for a controller and all layers above that controller, specify a controller. For example, to view all controllers on interface 3/0, use **show controllers sonet 3/0 configuration**. To view information for path 1 only, use **show controllers sonet 3/0:1 configuration**.
- Field descriptions
  - Interface specifier in slot/port format
  - channelized—Number of channels and speed for the interface
  - ifAdminStatus—Configured status of the interface: up or down
  - description—Configured description of the controller
  - snmp trap link-status—State of SNMP link status processing for the section and line layers of the interface: enabled or disabled
  - alarms used for operational status calculation—Types of defects that the router uses to determine the operational status of the interface at the section and line layers
  - defect trigger soaking delay—Time that the router waits to set an alarm when the router records a defect at the section or line layer
  - Operational Status—Physical state of the interface:
    - up—Interface is operational
    - down, failure alarm—Interface is not operational; type of defect that caused failure is specified
    - time since last status change—Time since the line module was rebooted
  - Loopback State—Type of loopback configured at this layer in the interface, or none
  - Last Remote Loopback Request Sent
  - BERT test—Number of current test and total number of tests
    - Test interval—Length of the BERT test
    - status—Sync (controller is synchronized with remote device) or NoSync (controller is not synchronized with remote device
    - Sync count—Number of times the pattern detector synchronized with the incoming data pattern
    - Received bit count—Number of bits received
    - Error bit count—Number of bits with errors
  - Mode—Type of interface: SONET or SDH
  - Timing source—Type of clock source configured for the channel:
    - internal module—Internal clock is from the line module itself
    - chassis—Internal clock is from the configured router clock

- Current section alarms—Number of suspect bit patterns found in several consecutive frames in section layer, or none
- Current line alarms—Number of suspect bit patterns found in several consecutive frames in line layer
- Channel configuration—Parameters for specific controllers; the actual parameters depend on the controller.
- ifAdminStatus—State of the controller in the software configuration: up or down
- ifOperStatus—Physical state of the controller: up or down
- Time since last status change—Time the controller has been up or down
- Alarms—Number of suspect bit patterns found in several consecutive frames
- snmp trap link-status—State of SNMP link status processing for the controller: enabled or disabled
- alarms used for operational status calculation—Types of defects that the router uses to determine the operational status of the interface at the path layer
- defect trigger soaking delay—Time that the router waits to set an alarm when the router records a defect at the path layer
- c2 byte—Setting of path signal byte: set by upper interface type (automatic setting) or configured value
- Operational Status—Physical state of this layer: up, down, or lowerLayerDown
  - time since last status change—Time since the line module was rebooted
- Framing—Type of framing configured for the controller:
  - c-bit parity framing (for T3 interfaces)
  - M23 multiplexer framing (for T3 interfaces)
  - crc4—Cyclic redundancy check (for E1 interfaces)
  - no-crc4—No cyclic redundancy check (for E1 interfaces)
  - esf—Extended superframe (for T1 interfaces)
  - sf—Superframe (for T1 interfaces)
- Line Code—Type of line coding the router assigned to the controller: B8ZS or AMI
- Clock source—Type of clock source configured for the channel:
  - module—Internal clock is from the line module itself
  - chassis—Internal clock is from the configured router clock
- J1 transmit trace message—Trace message sent to the remote device
- J1 expected trace message—Trace message expected from the remote device
- J1 received trace message—Trace message received from the remote device

- Example 1

```
host1#show controllers sonet 3/0 configuration
oc12 3/0
non channelized
ifAdminStatus: up
description: link1
snmp trap link-status: enabled
alarms used for operational status calculation: LOS LOF AIS RDI
defect trigger soaking delay: 2500 milliseconds
Operational Status: up
      time since last status change: 00:03:30
Loopback State: none
Mode: sonet
Timing source: internal module
Receive FIFO Overruns: 0, Reconfigurations: 0
Current section defects: none
Current line    defects: none

Channel configuration:
channel = 0, path = oc12, hierarchy = 1/1/0/0, current path defects: none
 ifAdminStatus: up
 snmp trap link-status: disabled
 alarms used for operational status calculation: LOP AIS
 defect trigger soaking delay: 2500 milliseconds
 c2 byte override 20
 Operational Status: up
       time since last status change: 00:03:30
 J1 transmit trace message: sonet3/0
 J1 expected trace message: sonet4/0
 J1 received trace message: sonet4/0
```

- Example 2—If you do not specify the layer in the interface, the router shows the configuration for all layers, whether or not you specify the keyword **configuration**.

```
host1#show controllers sonet 2/1
oc3 2/1
channelized (3 channels, oc1 minimum speed)
ifAdminStatus: up
description: link1
snmp trap link-status: enabled
alarms used for operational status calculation: LOS LOF AIS RDI
defect trigger soaking delay: 2500 milliseconds
Operational Status: up
      time since last status change: 00:03:30
Operational Status: up
      time since last status change: 00:06:49
Loopback State: none
Mode: sonet
Timing source: internal module
Current section alarms: none
Current line alarms   : none

Channel configuration:
channel = 1, path = oc1, hierarchy = 1/1/1/1, current path alarms: none
 ifAdminStatus: up
 snmp trap link-status: disabled
 alarms used for operational status calculation: LOP AIS
 defect trigger soaking delay: 2500 milliseconds
 c2 byte override 20
```

```
Operational Status: up
       time since last status change: 00:06:49
Ds3 1, unchannelized
 ifOperStatus =  ifOperUp
 snmp trap link-status = disabled
 Framing is C-BIT, Line Code is B3ZS, Clock Source is Internal - Module
```

- Example 3—This example displays the configuration for T3 1/1 on slot 2, port 1.

```
host1#show controllers sonet 2/1:1/1
oc3 2/1
channelized (3 channels, oc1 minimum speed)
ifAdminStatus: up
description: link1
snmp trap link-status: enabled
alarms used for operational status calculation: LOS LOF AIS RDI
defect trigger soaking delay: 2500 milliseconds
Operational Status: up
      time since last status change: 00:03:30
Loopback State: none
Mode: sonet
Timing source: internal module
Current section alarms: none
Current line alarms   : none

Channel configuration:
channel = 1, path = oc1, hierarchy = 1/1/1/1, current path alarms: none
 ifAdminStatus: up
 snmp trap link-status: disabled
 alarms used for operational status calculation: LOP AIS
 defect trigger soaking delay: 2500 milliseconds
 c2 byte override 20
Operational Status: up
       time since last status change: 00:05:37
Ds3 1, unchannelized
 ifOperStatus =  ifOperUp
 snmp trap link-status = disabled
 Framing is C-BIT, Line Code is B3ZS, Clock Source is Internal - Module
```

show controllers sonet ds1|e1

- Use to display E1 or T1 (DS1) statistics for the different layers in channelized SONET and SDH interfaces. Figure 8 on page 105 shows the layers in the interface.
- For definitions of the MIB statistics, see RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999).
- Specify an interface in *slot/port* format.
- To view information for a specific controller in a layer, enter the specifier for the controller and the type for the controller. For example, to view the E1 controller 1/1/1 on path 1 on the interface 4/0, enter **show controllers sonet 4/0:1/1/1/1 e1**.
- To view information for all controllers above a particular layer, enter the specifier for the layer and the type for the controller. For example, to view all E1 controllers on the interface 4/0 path 1, enter **show controllers sonet 4/0:1 e1**.
- To view E1 or T1 statistics for a layer, specify the controller type, **e1** or **ds1**.

- To view the configuration for a controller or all controllers in a layer, omit the controller type.
- Field descriptions
  - Description—Text description or alias if configured for the interface
  - BERT test—Number of current test and total number of tests
    - Test interval—Length of the BERT test
    - status—Sync (controller is synchronized with remote device) or NoSync (controller is not synchronized with remote device
    - Sync count—Number of times the pattern detector synchronized with the incoming data pattern
    - Received bit count—Number of bits received
    - Error bit count—Number of bits with errors
  - Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
  - Time elapsed in current interval—Reported in 15-minute intervals
  - Errored seconds—Number of errored seconds encountered by a T1 or an E1 in the current interval
  - Severely errored seconds—Number of severely errored seconds encountered by a T1 or an E1 in the current interval
  - Severely errored frame seconds—Number of severely errored framing seconds encountered by a T1 or an E1 in the current interval
  - Unavailable seconds—Number of unavailable seconds encountered by a T1 or an E1 in the current interval
  - Clock slip seconds—Number of clock slips encountered by a T1 or an E1 in the current interval
  - Path code violations—Number of coding violations encountered by a T1 or an E1 in the current interval
  - Line errored seconds—Number of line errored seconds encountered by a T1 or an E1 in the current interval
  - Bursty errored seconds—Number of bursty errored seconds encountered by a T1 or an E1 in the current interval
  - Degraded minutes—Number of minutes that a T1 or an E1 line is degraded
  - Line code violations—Number of line code violations encountered by a T1 or an E1 in the current interval
- Example—This example displays statistics for all the E1 lines on the interface 2/0.

```
host1#show controllers sonet 2/0 e1
E1 1/1/1

Description: boston111 e1
BERT test - 2 in 11
Test Interval 1 minute(s), Running - Status is Sync
0 minute(s), 33 second(s) left in test interval
Sync count        = 1
```

```
Received bit count = 41472000
Error bit count    = 0

 Number of valid interval - 0
 Time elapse in current interval - 0

Current Interval Counters
Errored seconds                  = 0
Severely errored second          = 0
Severely errored frame seconds   = 0
Unavailable seconds              = 0
Clock slip seconds               = 0
Path code violations             = 0
Line errored seconds             = 0
Bursty errored seconds           = 0
Degraded minutes                 = 0
Line code violations             = 0

24 Hour Total Counters
Errored seconds                  = 0
Severely errored second          = 0
Severely errored frame seconds   = 0
Unavailable seconds              = 0
Clock slip seconds               = 0
Path code violations             = 0
Line errored seconds             = 0
Bursty errored seconds           = 0
Degraded minutes                 = 0
Line code violations             = 0
```

show controllers sonet ds3

- Use to display T3 statistics for the different layers in channelized SONET and SDH interfaces. Figure 8 on page 105 shows the layers in the interface.
- For definitions of the MIB statistics, see RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999).
- Specify an interface in *slot/port* format.
- To view information for a specific controller in a layer, enter the specifier for the controller and the type for the controller. For example, to view T3 controller 1 on path 1 on the interface 4/0, enter **show controllers sonet 4/0:1/1 ds3**.
- To view information for all controllers above a particular layer, enter the specifier for the layer and the type for the controller. For example, to view all DS3 controllers on the interface 4/0, enter **show controllers sonet 4/0 ds3**.
- To view T3 statistics for a layer, specify the controller type, **ds3**.
- To view the configuration for a controller or all controllers in a layer, omit the controller type.
- Field descriptions
  - Description—Text description or alias if configured for the interface
  - BERT test—Number of current test and total number of tests
    - Test interval—Length of the BERT test
    - status—Sync (controller is synchronized with remote device) or NoSync (controller is not synchronized with remote device

    - Sync count—Number of times the pattern detector synchronized with the incoming data pattern
    - Received bit count—Number of bits received
    - Error bit count—Number of bits with errors
  - Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
  - Time elapse in current interval—Time (seconds) passed in current interval
  - Current Interval Counters—Statistics for the current 15-minute interval
  - P-bit errored seconds—Number of errored seconds encountered by a T3
  - P-bit severely errored seconds—Number of severely errored seconds encountered by a T3
  - Severely errored frame seconds—Number of severely errored framing seconds encountered by a T3
  - Unavailable seconds—Number of unavailable seconds encountered by a T3
  - Line code violations—Number of line code violations encountered by a T3
  - P-bit coding violations—Number of coding violations encountered by a T3
  - Line errored seconds—Number of line errored seconds encountered by a T3
  - C-bit coding violations—Number of C-bit coding violations encountered by a T3
  - C-bit errored seconds—Number of C-bit errored seconds encountered by a T3
  - C-bit severely errored seconds—Number of C-bit severely errored seconds encountered by a T3
  - 24 Hour Total counters—Statistics for last 24 hours

- Example 1—This example shows all T3 controllers on the interface 2/1.

```
host1#show controllers sonet 2/1 ds3
Ds3 1
Description: ottawa211 ds3
 Number of valid interval - 0
 Time elapse in current interval - 696

Current Interval Counters
P-bit errored seconds          = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds            = 541
Line code violations           = 0
P-bit coding violations        = 0
Line errored seconds           = 0
C-bit coding violations        = 0
C-bit errored seconds          = 0
C-bit severely errored seconds = 0

24 Hour Total Counters
P-bit errored seconds          = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds            = 0
```

```
Line code violations          = 0
P-bit coding violations       = 0
Line errored seconds          = 0
C-bit coding violations       = 0
C-bit errored seconds         = 0
C-bit severely errored seconds = 0
```

- Example 2—This example shows statistics for the T3 controller 1/1 on interface 2/0.

```
host1#show controllers sonet 2/0:1/1 ds3
Ds3 1
Description: ottawa2011 ds3
Number of valid interval - 0
 Time elapse in current interval - 534

Current Interval Counters
P-bit errored seconds         = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds           = 117
Line code violations          = 0
P-bit coding violations       = 0
Line errored seconds          = 0
C-bit coding violations       = 0
C-bit errored seconds         = 0
C-bit severely errored seconds = 0

24 Hour Total Counters
P-bit errored seconds         = 0
P-bit severely errored seconds = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Line code violations          = 0
P-bit coding violations       = 0
Line errored seconds          = 0
C-bit coding violations       = 0
C-bit errored seconds         = 0
C-bit severely errored seconds = 0
```

show controllers sonet line | path | section | tributary

- Use to display statistics for the different layers in channelized SONET and SDH interfaces. Figure 8 on page 105 shows the layers in the interface.
- For definitions of the MIB statistics, see RFC 2558—Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999).
- Specify an interface in *slot/port* format.
- To view information for a specific controller in a layer, enter the specifier for the controller and the type for the controller. For example, to view tributary 1/1/1 on path 1 of interface 4/0, enter **show controllers sonet 4/0:1/1/1/1 tributary**.
- To view information for all controllers above a particular layer, enter the specifier for the layer and the type for the controller. For example, to view all tributaries on path 1 of interface 4/0, enter **show controllers sonet 4/0:1 tributary**.
- To view statistics for a layer, specify the type of layer.
- To view the configuration for a controller or all controllers in a layer, omit the controller type.

- To view all statistics for all sessions, specify the **total** keyword.
- To view baselined statistics for all intervals, specify the **delta total** keywords.
- Field descriptions
  - Current Interval Counters—Statistics for the current 15-minute interval
    - Errored seconds—Number of errored seconds encountered by a T1 or an E1 in an interval
    - Severly errored seconds—Number of severely errored seconds encountered in an interval
    - Severly errored framing seconds—Number of severely errored framing seconds encountered in an interval
    - Coding violations—Number of coding violations encountered in an interval
    - Unavailable seconds—Number of unavailable seconds encountered in an interval
  - Last Interval Counters—Statistics for the previous 15-minute interval
  - Current Far End Interval Counters—Statistics for the remote connection associated with the SONET/SDH path in the current 15-minute interval
  - Last Far End Interval Counters—Statistics for the remote connection associated with the SONET/SDH path in the previous 15-minute interval
  - Total interval counters—Shows the statistics for all intervals or baselined statistics
- Example 1—This example shows the MIB statistics for the section layer on interface 2/1.

```
host1#show controllers sonet 2/1 section
Current Section Interval Counters
Current status                   = No Defect
Errored seconds                  = 0
Severly errored seconds          = 0
Severely errored framing seconds = 0
Coding violations                = 0

Last Section Interval Counters
Errored seconds                  = 0
Severly errored seconds          = 0
Severely errored framing seconds = 0
Coding violations                = 0
```

- Example 2—This example illustrates the behavior of the **baseline section interface sonet** command. The examples show the MIB statistics of the section layer before and after the command is issued.

```
host1#show controllers sonet 2/0 section total
Number of valid intervals - 0
 Time elapsed in current interval - 192

Current Section Interval Counters
Current status                   = No Defect
Errored seconds                  = 68
Severly errored seconds          = 68
Severely errored framing seconds = 2
Coding violations                = 4018
```

```
Total Section Counters
Errored seconds               = 68
Severly errored seconds       = 68
Severely errored framing seconds = 2
Coding violations             = 4018

host1#baseline section interface sonet 2/0

host1#show controllers sonet 2/0 section total delta
Number of valid intervals - 0
 Time elapsed in current interval - 209
Current Section Interval Counters
Current status                = No Defect
Errored seconds               = 68
Severly errored seconds       = 68
Severely errored framing seconds = 2
Coding violations             = 4018

Total Section Counters
Errored seconds               = 0
Severly errored seconds       = 0
Severely errored framing seconds = 0
Coding violations             = 0
```

- Example 3—This example shows the MIB statistics for the line layer on interface 2/1.

```
host1#show controllers sonet 2/1 line
Current Line Interval Counters
Current status                = No Defect
Errored seconds               = 0
Severly errored seconds       = 0
Coding violations             = 0
Unavailable seconds           = 190
Last Line Interval Counters
Errored seconds               = 0
Severly errored seconds       = 0
Coding violations             = 0
Unavailable seconds           = 900

Current Far End Line Interval Counters
Errored seconds               = 0
Severly errored seconds       = 0
Coding violations             = 0
Unavailable seconds           = 0

Far End Last Line Interval Counters
Errored seconds               = 0
Severly errored seconds       = 0
Coding violations             = 0
Unavailable seconds           = 0
```

- Example 4—This example shows the MIB statistics for the path layer on interface 2/1.

```
host1#show controllers sonet 2/1 path
Channel number 1
Current Path Interval Counters
Current status                = No Defect
Errored seconds               = 0
Severly errored seconds       = 0
Coding violations             = 0
Unavailable seconds           = 248
```

```
Last Path Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
Current Far End Path Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 248

Far End Last Path Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
```

- Example 5—This example displays the tributary statistics for all tributaries on interface 4/0, path 1.

```
host1#show controllers sonet 4/0:1 tributary
Tributary 1/1/1
Current Tributary Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
Last Tributary Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
Current Far End Path Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
Far End Last Tributary Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
```

- Example 6—This example displays the tributary statistics for the tributary 1/1/1 on path 1 on slot 4, port 0.

```
host1#show controllers sonet 4/0:1/1/1/1 tributary
Tributary 1/1/1
Current Tributary Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
Last Tributary Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
Current Far End Path Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
```

```
Unavailable seconds            = 0
Far End Last Tributary Interval Counters
Errored seconds                = 0
Severly errored seconds        = 0
Coding violations              = 0
Unavailable seconds            = 0
```

show controllers sonet remote

- Use to display MIB statistics for the remote end of a channelized T3 interface configured for MDL or for the remote end of a T1 channel configured for FDL.
- Specify the **all** option to display detailed information for all 15-minute intervals.
- For definitions of the MIB statistics for a T3 connections, see RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999).
- For definitions of the MIB statistics for a T1 connections, see RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999).
- Field descriptions for a T3 interface
  - Far End MDL Carrier bit—Status of MDL configuration on remote device connected to T3 interface
    - set—MDL is configured for carrier mode
    - not set—MDL is not configured for carrier mode
  - Far End Equipment Identification Code—eic string sent by remote device for MDL
  - Far End Line Identification Code—lic string sent by remote device for MDL
  - Far End Frame Identification Code—fic string sent by remote device for MDL
  - Far End Unit Identification Code—unit string sent by remote device for MDL
  - Far End Facility Identification Code—pfi string sent by remote device for MDL
  - Far End Generator Number—generator string sent by remote device for MDL
  - Far End Port Number—port string sent by remote device for MDL
  - Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
  - Time elapse in current interval—Number of seconds that have passed in the 15-minute (900-second) interval
  - C-bit errored seconds—Number of C-bit errored seconds encountered by a T3 in the current interval
  - C-bit severely errored seconds—Number of C-bit severely errored seconds encountered by a T3 in the current interval
  - C-bit coding violations—Number of C-bit coding violations encountered by a T3 in the current interval

- Unavailable seconds—Number of unavailable seconds encountered by a T3 in the current interval
- Invalid seconds—Number of seconds when statistics were not collected

- Field descriptions for a T1 channel
  - DS1—Identifier of T1 channel
  - Number of valid intervals—Number of 15-minute intervals since the line module was last powered on or reset
  - Time elapse in current interval—Number of seconds that have passed in the 15-minute (900-second) interval
  - Far End FDL Carrier bit—Status of FDL configuration on remote device connected to T1 channel
    - set—FDL is configured for carrier mode
    - not set—FDL is not configured for carrier mode
  - Far End Equipment Identification Code—eic string sent by remote device for FDL
  - Far End Line Identification Code—lic string sent by remote device for FDL
  - Far End Frame Identification Code—fic string sent by remote device for FDL
  - Far End Unit Identification Code—unit string sent by remote device for FDL
  - Far End Facility Identification Code—pfi string sent by remote device for FDL
  - Far End Generator Number—generator string sent by remote device for FDL
  - Far End Port Number—port string sent by remote device for FDL
  - Errored seconds—Number of errored seconds encountered by a T1 in the current interval
  - Severely errored seconds—Number of severely errored seconds encountered by a T1 in the current interval
  - Severely errored frame seconds—Number of severely errored framing seconds encountered by a T1 in the current interval
  - Unavailable seconds—Number of unavailable seconds encountered by a T1 in the current interval
  - Clock slip seconds—Number of clock slips encountered by a T1 in the current interval
  - Path code violations—Number of coding violations encountered by a T1 in the current interval
  - number of coding violations encountered by a T1 in the current interval
  - Line errored seconds—Number of line errored seconds encountered by a T1 in the current interval
  - Bursty errored seconds—Number of bursty errored seconds encountered by a T1 in the current interval
  - Degraded minutes—Number of minutes that a T1 line is degraded

- Example 1—In this example, a T3 interface is specified.

```
host1#show controllers sonet 5/0:1/1 remote
Far End MDL Carrier bit is not set
Far End Equipment Identification Code is the null string
Far End Line Identification Code is the null string
Far End Frame Identification Code is the null string
Far End Unit Identification Code is the null string
Far End Facility Identification Code is the null string
Far End Generator Number is the null string
Far End Port Number is the null string

Number of valid interval - 3
Time elapse in current interval - 756

Ds3 Current Interval Counters
C-bit errored seconds          = 0
C-bit severely errored seconds = 0
C-bit coding violations        = 0
Unavailable seconds            = 0
Invalid seconds                = 0

Ds3 Last Interval Counters
C-bit errored seconds          = 0
C-bit severely errored seconds = 0
C-bit coding violations        = 0
Unavailable seconds            = 0
Invalid seconds                = 0
Ds3 24 Hour Total Counters
C-bit errored seconds          = 1
C-bit severely errored seconds = 1
C-bit coding violations        = 330
Unavailable seconds            = 0
Invalid seconds                = 0
```

- Example 2—In this example, a T1 channel on a T3 over channelized SONET interface is specified.

```
host1#show controllers sonet 5/0:1/1/1 remote
DS1 10/1:1
Number of valid interval - 0
Time elapse in current interval - 0

Far End FDL Carrier bit is not set
Far End Equipment Identification Code is the null string
Far End Line Identification Code is the null string
Far End Frame Identification Code is the null string
Far End Unit Identification Code is the null string
Far End Facility Identification Code is the null string
Far End Port Number is the null string
Far End Generator Number is the null string

DS1 Current Interval Counters
Errored seconds                = 0
Severely errored second        = 0
Severely errored frame seconds = 0
Unavailable seconds            = 0
Clock slip seconds             = 0
Path code violations           = 0
Line errored seconds           = 0
Bursty errored seconds         = 0
Degraded minutes               = 0
```

```
DS1 24 Hour Total Counters
Errored seconds               = 0
Severely errored second       = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Clock slip seconds            = 0
Path code violations          = 0
Line errored seconds          = 0
Bursty errored seconds        = 0
Degraded minutes              = 0
```

- Example 3—In this example, a T1 over channelized SONET interface is specified.

```
host1#show controllers sonet 5/0:1/1/1/2/2 remote
DS1 10/1:1
Number of valid interval - 0
Time elapse in current interval - 0

Far End FDL Carrier bit is not set
Far End Equipment Identification Code is the null string
Far End Line Identification Code is the null string
Far End Frame Identification Code is the null string
Far End Unit Identification Code is the null string
Far End Facility Identification Code is the null string
Far End Port Number is the null string
Far End Generator Number is the null string

DS1 Current Interval Counters
Errored seconds               = 0
Severely errored second       = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Clock slip seconds            = 0
Path code violations          = 0
Line errored seconds          = 0
Bursty errored seconds        = 0
Degraded minutes              = 0

DS1 24 Hour Total Counters
Errored seconds               = 0
Severely errored second       = 0
Severely errored frame seconds = 0
Unavailable seconds           = 0
Clock slip seconds            = 0
Path code violations          = 0
Line errored seconds          = 0
Bursty errored seconds        = 0
Degraded minutes              = 0
```

show interfaces serial

- Use to display information about the serial interfaces you specify.
- Field descriptions
  - Serial Interface—Location of the interface
  - Description—Text description or alias if configured for the interface

- ifOperStatus—Physical state of the interface
  - ifOperDown—Interface is not functioning
  - ifOperLowerLayerDown—Lower layer in the interface stack is not functioning
  - ifOperNotPresent—Module has been removed from the chassis
  - ifOperTesting—Interface is being tested
  - ifOperUp—Interface is functioning
- snmp trap link-status—Enabled or disabled
- Encapsulation—Layer 2 encapsulation display; options: ppp, frame-relay ietf, mlppp, mlframe-relay ietf, hdlc
- Crc type checking—Size of the CRC
- Hdlc mru—Current size of the MRU
- Hdlc mtu—Current size of the MTU
- Hdlc interface speed—Current line speed of the interface
- Hdlc idle-character—Current idle character
- Invert data disabled—Status of the data inversion feature
- Ds0 mode—Nx56 or Nx64
- 5 minute input rate—Data rates based on the traffic received in the last five minutes
- 5 minute output rate—Data rates based on the traffic sent in the last five minutes
- Interface Statistics
  - Packets received—Number of packets received on the interface
  - Bytes received—Number of bytes received on the interface
  - Errored packets received—Number of packets with errors received on the interface
  - Packets sent—Number of packets sent on the interface
  - Bytes sent—Number of bytes sent on the interface
  - Errored packets sent—Number of packets with errors sent from the interface

- Example

```
host1#show interfaces serial 2/0:1/1/1/1/1
Serial Interface at 2/0:1/1/1/1/1
Description: toronto20 hdlc channel
ifOperStatus = ifOperUp
snmp trap link-status = disabled
Encapsulation hdlc
Crc type checking - CRC16
Hdlc mru = 1600
Hdlc mtu = 1600
Hdlc interface speed = 1536000
Hdlc idle-character marks
Invert data disabled, Ds0 time slot map = 0xffffff
Ds0 mode = Nx64
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
Interface statistics
Packets received             100
Bytes received               1300
Errored packets received     1
Packets sent                 100
Bytes send                   1436
Errored packets sent         0
```

Monitoring APS/MSP

For information about monitoring APS/MSP, see *Monitoring APS/MSP* in *Chapter 3, Configuring Unchannelized OCx/STMx Interfaces*.

Chapter 5

Configuring Ethernet Interfaces

This chapter describes how to configure Ethernet interfaces on E-series routers.

Most of the procedures described here do not apply to the Fast Ethernet management port on the SRP module. You can, however, select and display statistics for that port by using commands described in this chapter. For information about managing the Fast Ethernet port on the SRP module, see *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

This chapter contains the following sections:

- Ethernet Overview on page 164
- Ethernet Interface Platform Considerations on page 165
- Fast Ethernet I/O Modules on page 167
- Gigabit Ethernet I/O Modules and IOAs on page 168
- 10-Gigabit Ethernet IOAs on page 177
- Ethernet References on page 180
- High-Density Ethernet on page 181
- Managing Port Redundancy on Gigabit Ethernet I/O Modules on page 181
- Configuration Tasks for Ethernet on page 183
- Configuring the Physical Interface on page 183
- Configuring VLANs on page 187
- Configuring S-VLANs on page 197
- Configuring 802.3ad Link Aggregation for Ethernet on page 205

- Configuring Ethernet Link Redundancy on page 214
- Configuring Higher-Level Protocols over Ethernet on page 225
- Disabling Ethernet Interfaces on page 230
- Monitoring Ethernet Interfaces on page 230

Ethernet Overview

Ethernet modules support the following Ethernet interfaces:

- Fast Ethernet
- Gigabit Ethernet
- 10-Gigabit Ethernet
- IEEE 802.3ad link aggregation group (LAG)

This section describes features that are available with Ethernet interfaces.

Ethernet modules use the Address Resolution Protocol (ARP) to obtain MAC addresses for outgoing Ethernet frames. For more information about ARP, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

NOTE: Read *Configuration Tasks for Ethernet* on page 183 before you begin to configure an Ethernet interface.

Features

Ethernet interfaces support the following features:

- Routing of IP packets.
- Quality of Service (QoS) classification.
- High-density Ethernet. (For information, see *High-Density Ethernet* on page 181.*)*
- Virtual LAN (VLAN) configurations. (For information, see *Configuring VLANs* on page 187.)
- Stacked Virtual LAN (S-VLAN) configurations. (For information, see *Configuring S-VLANs* on page 197.)
- Configurations with higher-level protocols. (For information, see *Configuring Higher-Level Protocols over Ethernet* on page 225.)
- Layer 2 Tunneling Protocol (L2TP. For information, see *L2TP* on page 165.)
- Multinetting. (For information, see *Multinetting* on page 165.)

L2TP

Most Ethernet interfaces support L2TP. To use L2TP, you must first create a PPP interface. See *JUNOSe Broadband Access Configuration Guide, Chapter 10, L2TP Overview* for information about configuring L2TP.

Multinetting

Ethernet interfaces, except for bridged Ethernet interfaces, support multinetting; that is, adding more than one IP address to an IP interface. If you want to add multiple IP addresses to a single IP interface, use the **ip address** command with the **secondary** keyword, which is described in *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

Ethernet Interface Platform Considerations

You can configure Ethernet interfaces on the following E-series routers:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

This section describes the line modules and I/O modules that support Ethernet interfaces.

For detailed information about the modules that support Fast Ethernet and Gigabit Ethernet interfaces on the ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed specifications of these modules.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that Ethernet modules support.

For detailed information about the modules that support Gigabit Ethernet and 10-Gigabit Ethernet interfaces on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed specifications of these modules.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the protocols and applications that Ethernet modules support.

Numbering Scheme

When configuring or managing an interface, you must know the numbering scheme for identifying an interface. The numbering scheme depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

Use the *slot/port* [.*subinterface*] format to identify Ethernet interfaces and subinterfaces.

- *slot*—Number of the slot in which the line module resides in the chassis.

  In ERX-7xx models, line module slots are numbered 2-6; slots 0 and 1 are reserved for SRP modules. In ERX-14xx models, line module slots are numbered 0–5 and 8–13; slots 6 and 7 are reserved for SRP modules. In an ERX-310 router, line module slots are numbered 1–2; slot 0 is reserved for the SRP module.

- *port*—Number of the port on the I/O module.

  On the OC3-2 GE APS I/O module, you can configure only a Gigabit Ethernet interface in port 2; ports 0 and 1 are reserved for OC3/STM1 ATM interfaces.

- *subinterface*—Subinterface number of the protocol or VLAN subinterface.

For information about installing line modules and I/O modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

E120 Router and E320 Router

Use the *slot/adapter/port* [.*subinterface*] format to identify Ethernet interfaces and subinterfaces.

- *slot*—Number of the slot in which the line module resides in the chassis.

  In the E120 router, line module slots are numbered 0–5. In the E320 router, line module slots are numbered 0–5 and 11–16. For both routers, slots 6 and 7 are reserved for SRP modules; slots 8–10 are reserved for switch fabric modules (SFMs).

- *adapter*—Number of the bay in which the I/O adapter (IOA) resides.

  This identifier applies to the E120 and E320 routers only. In the software, adapter 0 identifies the right IOA bay (E120 router) and the upper IOA bay (E320 router); adapter 1 identifies the left IOA bay (E120 router) and the lower IOA bay (E320 router).

- *port*—Number of the port on the IOA

- *subinterface*—Subinterface number of the protocol or VLAN subinterface

For information about installing line modules and IOAs in the E120 and E320 routers, see *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*.

Interface Specifier

The configuration task examples in this chapter use the format for ERX-7xx models, ERX-14xx models, and the ERX-310 router to specify an Ethernet interface. (The format is described in *Numbering Scheme* on page 166.)

For example, the following command specifies a Fast Ethernet interface on port 0 of an I/O module in slot 4.

host1(config)#**interface fastEthernet 4/0**

When you configure a Gigabit Ethernet interface or a 10-Gigabit Ethernet interface on E120 or E320 routers, you must include the adapter identifier as part of the interface specifier. For example, the following command specifies a Gigabit Ethernet interface on port 0 of the IOA installed in the upper adapter bay of slot 3.

host1(config)#**interface gigabitEthernet 3/0/0**

For more information about interface types and specifiers on E-series models, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

Fast Ethernet I/O Modules

Fast Ethernet interfaces are supported on two I/O modules: the FE-8 I/O module and the FE-8 SFP I/O module.

FE-8 I/O Module

ERX-7xx models, ERX-14xx models, and the ERX-310 router all support the FE-8 I/O module.

An FE-8 I/O module accepts up to eight RJ-45 connectors.

FE-8 SFP I/O Module

ERX-7xx models, ERX-14xx models, and the ERX-310 router all support the FE-8 SFP I/O module.

The FE-8 SFP I/O module uses a range of small form-factor pluggable transceivers (SFPs) to support different optical modes and cabling distances. The I/O module supports up to eight LC-style fiber-optic connectors.

Unlike all other Fast Ethernet and Gigabit Ethernet I/O modules, the FE-8 SFP I/O module does not support automatic negotiation of the line speed and duplex mode by the router. For more information, see **duplex** on page 184 and **speed** on page 187.

Gigabit Ethernet I/O Modules and IOAs

Gigabit Ethernet interfaces are supported on the following modules:

- GE I/O module
- GE-2 SFP I/O module
- GE-8 I/O module
- OC3-2 GE APS I/O module
- ES2-S1 GE-4 IOA
- ES2-S1 GE-8 IOA
- ES2-S3 GE-20 IOA

GE I/O Module

ERX-7xx models, ERX-14xx models, and the ERX-310 router all support the GE I/O module.

You can pair any of the following types of GE I/O modules with the GE/FE line module:

- The GE I/O SFP module uses a range of SFPs to support different optical modes and cabling distances. The I/O module accepts up to two pairs (Tx/Rx) of LC-style fiber-optic connectors that support different optical modes and cabling distances. Alternatively, the I/O module supports up to two pairs of copper SFPs.
- The GE I/O MULTI MODE module accepts up to two pairs (Tx/Rx) of SC-style fiber-optic connectors.
- The GE I/O SINGLE MODE module accepts up to two pairs (Tx/Rx) of SC-style fiber-optic connectors.

The GE I/O module has two ports: one port (port 0) is active (also known as *primary*), and the other port (port 0R) is redundant. If the active port fails, the redundant port automatically becomes active.

You can configure only port 0 for a Gigabit Ethernet interface; you cannot configure redundant port 0R. Cabling both ports provides a redundant path to the Gigabit Ethernet interface.

GE-2 SFP I/O Module

The ERX-1440 router and the ERX-310 router both support the GE-2 SFP I/O module. Other E-series routers do not support the GE-2 SFP I/O module. The GE-2 SFP I/O module was previously called the 2XGE APS I/O module.

The GE-2 SFP I/O module pairs with the GE-2 line module and the GE-HDE line module. You can install the GE-2 line module or the GE-HDE line module and its corresponding GE-2 SFP I/O module in slot 1 or slot 2 of an ERX-310 router or in any slot of an ERX-1440 router.

The GE-2 SFP I/O module can use either fiber-optic or copper SFPs. The I/O module accepts up to two pairs (Tx/Rx) of LC-style fiber-optic connectors that support different optical modes and cabling distances. Alternatively, the I/O module supports up to two pairs of copper SFPs.

Ports on GE-2 SFP I/O Module

The GE-2 SFP I/O module has four ports: two ports (port 0 and port 1) are active (also known as *primary*), and the other two ports (port 0R and port 1R) are redundant. If an active port fails, its corresponding redundant port automatically becomes active.

You can configure only port 0 and port 1 for a Gigabit Ethernet interface; you cannot configure redundant ports 0R and 1R. Cabling an active port and its corresponding redundant port (that is, port 0 and port 0R, or port 1 and port 1R) provides a redundant path to the Gigabit Ethernet interface.

Bandwidth and Line Rate Considerations

When the GE-2 line module or the GE-HDE line module is installed in the ERX-1440 router, it delivers full bandwidth of 2 GB per port only when installed in slot 2 or slot 4, and when the SRP-40G+ module is used in the router. When the module is installed in any other ERX-1440 slot, it delivers a maximum bandwidth of 2 GB per line module (1 GB maximum at the ingress and 1 GB maximum at the egress). Therefore, of the maximum 24 possible ports for the module in an ERX-1440 chassis (that is, two ports in each of 12 slots), full bandwidth is delivered only on a maximum of four ports (those in slots 2 and 4).

When the GE-2 line module or the GE-HDE line module is installed in either the ERX-1440 router or the ERX-310 router and both ports are active, line rate performance is achieved only with packets that are 174 bytes or larger. The module might not achieve line rate with packets that are smaller than 174 bytes.

GE-8 I/O Module

The ERX-1440 router and the ERX-310 router both support the GE-8 I/O module. Other E-series routers do not support the GE-8 I/O module.

The GE-8 I/O module pairs with the GE-HDE line module to provide Gigabit Ethernet operation through eight line interfaces.

NOTE: The GE-8 I/O module has a logical port, numbered port 8, that is reserved for the hardware multicast packet replication feature. For more information, see *JUNOSe Multicast Routing Configuration Guide, Chapter 1, Configuring IPv4 Multicast* and *JUNOSe Multicast Routing Configuration Guide, Chapter 5, Configuring IPv6 Multicast*.

You can install the GE-HDE line module and its corresponding GE-8 I/O module in slot 1 or slot 2 of an ERX-310 router or in any slot of an ERX-1440 router.

The GE-8 I/O module can use either fiber-optic or copper SFPs. The I/O module accepts up to eight pairs (Tx/Rx) of LC-style fiber-optic connectors that support different optical modes and cabling distances. Alternatively, the I/O module supports up to eight pairs of copper SFPs.

Bandwidth and Line Rate Considerations

When the GE-HDE line module is installed in the ERX-1440 router, it delivers full bandwidth of 4 GB per line module (2 GB at the ingress and 2 GB at the egress) only when installed in slot 2 or slot 4, and when the SRP-40G+ module is used in the router. When the module is installed in any other ERX-1440 slot, it delivers a maximum bandwidth of 2 GB per line module (1 GB maximum at the ingress and 1 GB maximum at the egress). Therefore, of the maximum 96 possible ports for the module in an ERX-1440 chassis (that is, eight ports in each of 12 slots), full bandwidth is delivered only on a maximum of 16 ports (those in slots 2 and 4).

When the GE-HDE line module is installed in either the ERX-1440 router or the ERX-310 router and all ports are active, line rate performance is achieved only with packets that are 174 bytes or larger. The module might not achieve line rate with packets that are smaller than 174 bytes.

Table 15 lists the average data rate on the GE-HDE line module and GE-8 I/O module combination when installed in an ERX-310 router or in slots 2 or 4 of an ERX-1440 router.

Table 15: Average Data Rate for ERX-310 Router or in Slots 2 or 4 of an ERX-1440 Router

Port Combination	Average Data Rate per GE-8 I/O Module (> 174 Byte Packets)	Average Data Rate per GE-HDE Line Module
Ports 1–8	250 Mbps per port	250 Mbps per port
Any four ports	500 Mbps per port	500 Mbps per port
Any two ports	1 Gbps per port	1 Gbps per port

Table 16 lists the average data rate on the GE-HDE line module and GE-8 I/O module combination when installed in all other slots on the ERX-1440.

Table 16: Average Data Rate When Installed in All Other Slots on an ERX-1440 Router

Port Combination	Average Data Rate per GE-8 I/O Module (> 174 Byte Packets)	Average Data Rate per GE-HDE Line Module
Ports 1–8	125 Mbps per port	125 Mbps per port
Any four ports	250 Mbps per port	250 Mbps per port
Any two ports	500 Mbps per port	500 Mbps per port

Managing High-Density Ethernet

The overall data rate for the GE-HDE line module is 2 Gbps; therefore, the I/O module becomes highly oversubscribed because of the wire rate of the line module. The data rate of the GE-8 I/O module is limited with larger frames, and the packet rate is limited with smaller frames.

Currently, flow control using MAC pause frames is disabled on the GE-8 I/O module. The I/O module does not transmit or receive pause frames.

For more information about high-density Ethernet, see *High-Density Ethernet* on page 181.

OC3-2 GE APS I/O Module

ERX-7xx models, ERX-14xx models, and the ERX-310 router all support the OC3-2 GE APS I/O module.

The OC3-2 GE APS I/O module pairs with the OC3/STM1 GE/FE line module to provide Gigabit Ethernet operation through one line interface and OC3 STM1 ATM operation through two line interfaces.

The OC3-2 GE APS I/O module uses a range of SFPs to support different optical modes and cabling distances, and accepts up to three LC-style fiber-optic or copper SFPs. You can configure only port 2 for Gigabit Ethernet interfaces; port 0 and port 1 are reserved for OC3/STM1 ATM interfaces.

For more information about configuring OC3/STM-1 ATM interfaces on this I/O module, see *OC3/STM1 GE/FE Line Module* on page 73.

NOTE: The OC3-2 GE APS I/O module does not support APS in the current release.

ES2-S1 GE-4 IOA

The E120 router and the E320 router support the ES2-S1 GE-4 IOA. Other E-series routers do not support the ES2-S1 GE-4 IOA.

The ES2-S1 GE-4 IOA pairs with the ES2 4G line module (LM). For more information about the ES2 4G LM, see *ES2 4G Line Module* on page 74.

The ES2-S1 GE-4 IOA is offered in a half-height size that enables you to configure it in one of two IOA bays that are available for each slot. You can install the ES2-S1 GE-4 IOA in only one of the IOA bays per slot.For more information about installing IOAs, see the *E120 and E320 Hardware Guide*.

The ES2-S1 GE-4 IOA has four ports. The IOA can use either fiber-optic or copper SFPs. The IOA accepts up to four pairs (Tx/Rx) of LC-style fiber-optic connectors that support different optical modes and cabling distances. Alternatively, the IOA supports up to eight pairs of copper SFPs.

The ES2-S1 GE-4 IOA does not support port redundancy.

ES2-S1 GE-8 IOA

The E120 router and the E320 router support the ES2-S1 GE-8 IOA. Other E-series routers do not support the ES2-S1 GE-8 IOA.

The ES2-S1 GE-8 IOA is offered in a half-height size that enables you to configure it in either of the two IOA bays that are available for each slot. You can install the ES2-S1 GE-8 IOA in both IOA bays. For more information about installing IOAs, see the *E120 and E320 Hardware Guide*.

The ES2-S1 GE-8 IOA has eight ports. The IOA can use either fiber-optic or copper SFPs. The IOA accepts up to four pairs (Tx/Rx) of LC-style fiber-optic connectors that support different optical modes and cabling distances. Alternatively, the IOA supports up to eight pairs of copper SFPs.

NOTE: The ES2-S1 GE-8 IOA has a logical port, numbered port 8, that is reserved for the hardware multicast packet replication feature. For more information, see *JUNOSe Multicast Routing Configuration Guide, Chapter 1, Configuring IPv4 Multicast* and *JUNOSe Multicast Routing Configuration Guide, Chapter 5, Configuring IPv6 Multicast*.

The ES2-S1 GE-8 IOA pairs with either the ES2 4G line module (LM) and the ES2 10G LM to provide access services.

ES2 4G LM Combination

For more information about the ES2 4G LM, see *ES2 4G Line Module* on page 74.

When paired with the ES2 4G LM, you can combine the ES2-S1 GE-8 IOA in a slot with one of the following IOA types:

- ES2-S1 OC3-8 ATM IOA
- ES2-S1 OC12-2 ATM IOA
- ES2-S1 OC12-2 POS IOA

Bandwidth and Line Rate Considerations

Table 17 lists the average data rate on the ES2-S1 GE-8 IOA when installed in E120 and E320 routers with one ES2 4G LM installed.

Table 17: Average Data Rate for One ES2-S1 GE-8 IOA Installed with an ES2 4G LM

	100 Gbps Configuration (E320 Router)		120 Gbps and 320 Gbps Configurations (E120 and E320 Routers)	
Port Combination	Average Data Rate per GE-8 IOA (> 128 Byte Packets)	Average Data Rate per ES2 4G LM	Average Data Rate per GE-8 IOA (> 128 Byte Packets)	Average Data Rate per ES2 4G LM
All eight ports	412.5 Mbps per port	412.5 Mbps per port	475 Mbps per port	475 Mbps per port
Any four ports	825 Mbps per port	825 Mbps per port	950 Mbps per port	950 Mbps per port
Any two ports	1 Gbps per port	1 Gbps per port	1 Gbps per port	1 Gbps per port

Table 18 lists the average data rate on two ES2-S1 GE-8 IOAs when installed in E120 and E320 routers with one ES2 4G LM installed.

Table 18: Average Data Rate for Two ES2-S1 GE-8 IOAs Installed with an ES2 4G LM

	100 Gbps Configuration (E320 Router)		120 Gbps and 320 Gbps Configurations (E120 and E320 Routers)	
Port Combination	**Average Data Rate per GE-8 IOA (> 128 Byte Packets)**	**Average Data Rate per ES2 4G LM**	**Average Data Rate per GE-8 IOA (> 128 Byte Packets)**	**Average Data Rate per ES2 4G LM**
All sixteen ports	206.25 Mbps per port	206.25 Mbps per port	237.5 Mbps per port	237.5 Mbps per port
Any eight ports	412.5 Mbps per port	412.5 Mbps per port	475 Mbps per port	475 Mbps per port
Any four ports	825 Mbps per port	825 Mbps per port	950 Mbps per port	950 Mbps per port
Any two ports	1 Gbps per port	1 Gbps per port	1 Gbps per port	1 Gbps per port

Table 19 lists the average data rate when combining an ES2-S1 GE-8 IOA in one adapter bay with the ES2-S1 OC3-8 ATM IOA, or the ES2-S1 OC12-2 ATM IOA, or the ES2-S1 OC12-2 POS IOA in another adapter bay. Because the OC3/STM1 and OC12/STM4 IOAs use less than half of the full bandwidth of the ES2 4G LM, the router allocates these IOAs as much bandwidth as they can use. The ES2-S1 GE-8 IOA uses any remaining bandwidth.

Each OC12/STM4 port has a maximum theoretical bandwidth of 622 Mbps. Each OC3/STM1 port has a maximum theoretical bandwidth of 155 Mbps. Therefore, the OC12/STM4 IOAs have a maximum theoretical bandwidth of 1.244 Gbps and the OC3/STM1 IOA has an maximum theoretical bandwidth of 1.244 Gbps.

Table 19: Average Data Rate for ES2-S1 GE-8 IOA Combined with Other IOA Types in Same Slot

		100 Gbps Configuration (E320 Router)	120 Gbps and 320 Gbps Configurations (E120 and E320 Routers)
Average Data Rate per GE-8 IOA (> 128 Byte Packets)	**Average Data Rate per OC12/STM4 IOA**	**Average Data Rate per ES2 4G LM**	**Average Data Rate per ES2 4G LM**
257 Mbps per port (Ports 0–7)	622 Mbps per port (Ports 0 and 1)	GE-8 IOA—257 Mbps per port OC12/STM4—622 Mbps per port	GE-8 IOA—319.5 Mbps per port OC12/STM4—622 Mbps per port
334.75 Mbps per port (Ports 0–7)	622 Mbps (Port 1)	GE-8 IOA—334.75 Mbps per port OC12/STM4 IOA—622 Mbps for port 1	GE-8 IOA—397.25 Mbps per port OC12/STM4 IOA—622 Mbps for port 1
387.5 Mbps per port (Ports 0–7)	100 Mbps per port (Ports 0 and 1)	GE-8 IOA—387.5 Mbps per port OC12/STM4 IOA—100 Mbps per port	GE-8 IOA—450 Mbps per port OC12/STM4 IOA—100 Mbps per port

Managing High-Density Ethernet

With a 100 Gbps fabric configuration, the overall data rate for the ES2 4G LM with ES2-S1 GE-8 IOAs is 3.3 Gbps. With a 120 Gbps fabric configuration or a 320 Gbps fabric configuration, the overall data rate for the ES2 4G LM with ES2-S1 GE-8 IOAs is 3.8 Gbps. In both configurations, the line module becomes highly oversubscribed because of the IOA available wire rate. When paired with the ES2 4G LM, the data rate of the ES2-S1 GE-8 IOA is bandwidth limited with larger frames, and the packet rate is limited with smaller frames.

NOTE: The overall data rate of the ES2-S1 GE-8 IOA is 0.1 Gbps less than other IOAs that pair with the ES2 4G LM because of fair bandwidth allocation across the eight ports.

Currently, flow control using MAC pause frames is disabled on the ES2-S1 GE-8 IOA. The IOA does not transmit or receive pause frames.

For more information about high-density Ethernet on E-series routers, see *High-Density Ethernet* on page 181.

ES2 10G LM Combination

When paired with the ES2 10G LM, you can only combine the ES2-S1 GE-8 IOA in a slot with another ES2-S1 GE-8 IOA.

With a 100 Gbps fabric configuration, the E320 router can accommodate up to 2 combinations of ES2 10G LMs and ES2-S1 GE-8 IOAs. You must install a combination in either of the turbo slots (slot 2 or slot 4). The 100 Gbps allocates 10 Gbps of overall bandwidth to each of these slots.

With a 120 Gbps fabric configuration, the E120 router can accommodate up to 6 combinations of ES2 10G LMs and ES2-S1 GE-8 IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

With a 320 Gbps fabric configuration, the E320 router can accommodate up to 12 combinations of ES2 10G LMs and ES2-S1 GE-8 IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

Bandwidth and Line Rate Considerations

Each ES2-S1 GE-8 IOA is connected to the ES2 10G LM through a 5 Gbps bus. Therefore, the aggregate bandwidth of any IOA is limited to 5 Gbps.

Table 20 lists the average data rate on the ES2-S1 GE-8 IOA when installed in E120 and E320 routers with one ES2 10G LM installed.

Table 20: Average Data Rate for One ES2-S1 GE-8 IOA Installed with an ES2 10G LM

	100 Gbps, 120 Gbps, or 320 Gbps Configuration
Port Combination	**Average Data Rate per GE-8 IOA (> 128 Byte Packets)**
Any five ports	1 Gbps per port
All eight ports	625 Mbps per port

Table 21 lists the average data rate of two ES2-S1 GE-8 IOAs when installed in E120 and E320 routers with one ES2 10G LM installed.

Table 21: Average Data Rate for Two ES2-S1 GE-8 IOAs Installed with an ES2 10G LM

	100 Gbps, 120 Gbps, or 320 Gbps Configuration
Port Combination	**Average Data Rate per GE-8 IOA (> 128 Byte Packets)**
All sixteen ports	625 Mbps per port
Any five ports on each IOA	1 Gbps per port

Managing High-Density Ethernet

When installed in an E120 router or an E320 router with any SRP module combination, the overall data rate for the ES2 10G LM with one ES2-S1 GE-8 IOA is limited to 5 Gbps. The overall data rate for the ES2 10G LM with two ES2-S1 GE-8 IOAs is limited to 10 Gbps. In all configurations, the line module can become oversubscribed because of the IOA available wire rate (8 Gbps).

Currently, flow control using MAC pause frames is disabled on the ES2-S1 GE-8 IOA. The IOA does not transmit or receive pause frames.

For more information about high-density Ethernet on E-series routers, see *High-Density Ethernet* on page 181.

ES2-S3 GE-20 IOA

The E120 router and the E320 router support the ES2-S3 GE-20 IOA. Other E-series routers do not support the ES2-S3 GE-20 IOA.

The ES2-S3 GE-20 IOA pairs with the ES2 10G LM to provide Gigabit Ethernet operation through 20 line interfaces.

The ES2-S3 GE-20 IOA is offered in a full-height size that uses both adapter bays. The IOA is identified by the software as adapter bay 0. For more information about installing IOAs, see the *E120 and E320 Hardware Guide*.

The IOA can use either fiber-optic or copper SFPs. The IOA accepts up to four pairs (Tx/Rx) of LC-style fiber-optic connectors that support different optical modes and cabling distances.

The ES2-S3 GE-20 IOA does not support port redundancy.

ES2 10G LM Combination

With a 100 Gbps fabric configuration, the E320 router can accommodate up to 2 combinations of ES2 10G LMs and ES2-S3 GE-20 IOAs. You must install a combination in either of the turbo slots (slot 2 or slot 4). The 100 Gbps allocates 10 Gbps of overall bandwidth to each of these slots.

With a 120 Gbps fabric configuration, the E120 router can accommodate up to 6 combinations of ES2 10G LMs and ES2-S3 GE-20 IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

With a 320 Gbps fabric configuration, the E320 router can accommodate up to 12 combinations of ES2 10G LMs and ES2-S3 GE-20 IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

Bandwidth and Line Rate Considerations

Table 20 lists the average data rate on the ES2-S3 GE-20 IOA when installed in E120 and E320 routers with one ES2 10G LM installed.

Table 22: Average Data Rate for One ES2-S3 GE-20 IOA Installed with an ES2 10G LM

	100 Gbps, 120 Gbps, or 320 Gbps Configuration
Port Combination	**Average Data Rate per GE-20 IOA (> 128 Byte Packets)**
Any 10 ports	1 Gbps per port
All 20 ports	500 Mbps per port

Managing High-Density Ethernet

When installed in an E120 router or an E320 router with any SRP module combination, the overall data rate for the ES2 10G LM with one ES2-S3 GE-20 IOA is limited to 10 Gbps. The line module can become oversubscribed because of the IOA available wire rate (20 Gbps).

Currently, flow control using MAC pause frames is disabled on the ES2-S3 GE-20 IOA. The IOA does not transmit or receive pause frames.

For more information about high-density Ethernet on E-series routers, see *High-Density Ethernet* on page 181.

10-Gigabit Ethernet IOAs

10-Gigabit Ethernet interfaces are supported on the ES2-S1 10GE IOA and the ES2-S1 10GE PR IOA. For more information about 10-Gigabit Ethernet, see IEEE Standard 802.3ae.

ES2-S1 10GE IOA

The E120 router and the E320 router support the ES2-S1 10GE IOA. Other E-series routers do not support the ES2-S1 10GE IOA.

The ES2-S1 10GE IOA pairs with the ES2 4G LM to provide a 10-Gigabit Ethernet interface. For more information about the ES2 4G LM, see *ES2 4G Line Module* on page 74.

The ES2-S1 10GE IOA is offered in a full-height size that uses both adapter bays. The IOA is identified by the software as adapter bay 0. For more information about installing IOAs, see the *E120 and E320 Hardware Guide*.

The ES2-S1 10GE IOA has one port, uses a range of 10-gigabit small form-factor pluggable transceivers (XFPs) to support different optical modes and cabling distances, and accepts one LC-style fiber-optic connector.

Managing High-Density Ethernet

With a 100 Gbps fabric configuration, the overall data rate for the ES2 4G LM with the ES2-S1 10GE IOA is 3.4 Gbps for large packets. With a 120 Gbps or a 320 Gbps fabric configuration, the overall data rate for the ES2 4G LM with the ES2-S1 10GE IOA is 3.9 Gbps for large packets. In all configurations, the line module becomes highly oversubscribed because of the available wire rate on the IOA. When paired with the ES2 4G LM, the data rate of the ES2-S1 10GE IOA is bandwidth limited with larger frames, and the packet rate is limited with smaller frames.

Currently, flow control using MAC pause frames is disabled on the ES2-S1 10GE IOA. The IOA does not transmit or receive pause frames.

For more information about high-density Ethernet on E-series routers, see *High-Density Ethernet* on page 181.

ES2-S2 10GE PR IOA

The E120 router and the E320 router support the ES2-S2 10GE PR IOA. Other E-series routers do not support the ES2-S2 10GE PR IOA.

The ES2-S2 10GE PR IOA is offered in a full-height size that uses both adapter bays. The IOA is identified by the software as adapter bay 0. For more information about installing IOAs, see the *E120 and E320 Hardware Guide*.

The ES2-S2 10GE PR IOA has one port, uses a range of XFPs to support different optical modes and cabling distances, and accepts 10 LC-style fiber-optic connectors.

The single port on the ES2-S2 10GE PR IOA has a redundant port. If the active port fails, the redundant port automatically becomes active. You can configure only the active port for a 10-Gigabit Ethernet interface; you cannot configure the redundant port. Cabling both ports provides a redundant path to the 10-Gigabit Ethernet interface.

The ES2-S2 10GE PR IOA pairs with the ES2 10G Uplink LM to provide uplink services or the ES2 10G LM to provide access services.

ES2 10G Uplink LM Combination

With a 100 Gbps fabric configuration, the E320 router can accommodate up to 2 combinations of ES2 10G Uplink LMs and ES2-S2 10GE PR IOAs. You must install a combination in either of the turbo slots (slot 2 or slot 4). The 100 Gbps allocates 10 Gbps of overall bandwidth to each of these slots. With a 120 Gbps fabric configuration, the E120 router can accommodate up to 6 combinations of ES2 10G Uplink LMs and ES2-S2 10GE PR IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

With a 320 Gbps fabric configuration, the E320 router can accommodate up to 12 combinations of ES2 10G Uplink LMs and ES2-S2 10GE PR IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

Uplink Operation

The ES2 10G Uplink LM and ES2-S2 10GE PR IOA combination provides an uplink connection from the core network to the edge rather than traditional broadband access services such as PPPoE, transparent bridging, and subscriber interfaces.

The combination can receive and transmit full duplex line rate of 10 GB (10 GB at the ingress and 10 GB at the egress). The IOA can also support 9.6 Kbps jumbo packets at both the ingress and egress.

Multicast

The ES2 10G Uplink LM can receive multicast traffic, including all multicast control protocols. The ES2 10G Uplink LM can also transmit multicast control protocol frames and multicast data frames to perform multicast egress elaboration.

L2TP

An E-series router can be configured as either an L2TP access concentrator (LAC) or an L2TP network server (LNS). The ES2 10G Uplink LM and ES2-S2 10GE PR IOA combination supports an E-series router configured as a LAC only for traffic to or from an LNS. The ES2 10G Uplink LM and ES2-S2 10GE PR IOA combination supports both sides of the L2TP LNS function (LAC facing and core facing).

Flow Control and Policy

The ES2 10G Uplink LM and ES2-S2 10GE PR IOA combination does not support quality of service (QoS) functionality that is available on other ASIC-based Ethernet modules.

Although the ES2 10G Uplink LM does not support scheduling and shaping for egress traffic, the LM does account for the traffic class of packets through the fabric so that high priority packets are scheduled for transmission to the line module before lower priority packets. Packets that arrive at the line module are processed and transmitted using a flow-through scheme.

Currently, flow control using MAC pause frames is disabled on the ES2-S2 10GE PR IOA. The IOA does not transmit or receive pause frames. Instead, the system prioritizes control traffic over non-control traffic (that is, data). For a list of types of control traffic, see *High-Density Ethernet* on page 181.

For information about configuring policies on the ES2 10G Uplink LM and ES2-S2 10GE PR IOA, see *JUNOSe Policy Management Configuration Guide, Chapter 8, Policy Resources*.

ES2 10G LM Combination

With a 100 Gbps fabric configuration, the E320 router can accommodate up to 2 combinations of ES2 10G LMs and ES2-S2 10GE PR IOAs. You must install a combination in either of the turbo slots (slot 2 or slot 4). The 100 Gbps allocates 10 Gbps of overall bandwidth to each of these slots.

With a 120 Gbps fabric configuration, the E120 router can accommodate up to 6 combinations of ES2 10G LMs and ES2-S2 10GE PR IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

With a 320 Gbps fabric configuration, the E320 router can accommodate up to 12 combinations of ES2 10G LMs and ES2-S2 10GE PR IOAs. You can install a combination in any of the line module slots, each of which are allocated 10 Gbps of overall bandwidth.

Access Operation

The ES2 10G LM and ES2-S2 10GE PR IOA combination provides traditional broadband access services such as PPPoE and subscriber interfaces. It also supports both sides of the L2TP LNS and LAC function.

The combination can receive and transmit full duplex line rate of 10 GB (10 GB at the ingress and 10 GB at the egress). The IOA can also support 9.6 Kbps jumbo packets at both the ingress and egress.

Multicast

The ES2 10G LM can receive multicast traffic, including all multicast control protocols. The ES2 10G LM can also transmit multicast control protocol frames and multicast data frames to perform multicast egress elaboration.

Flow Control and Policy

The ES2 10G LM and ES2-S2 10GE PR IOA combination supports QoS functionality that is available on other ASIC-based Ethernet modules.

Currently, flow control using MAC pause frames is disabled on the ES2-S2 10GE PR IOA. The IOA does not transmit or receive pause frames. Instead, the system prioritizes control traffic over non-control traffic (that is, data). For a list of types of control traffic, see *High-Density Ethernet* on page 181.

For information about configuring policies on the ES2 10G LM and ES2-S2 10GE PR IOA, see *JUNOSe Policy Management Configuration Guide, Chapter 1, Managing Policies on the E-series Router*.

Ethernet References

For more information about Ethernet implementations, consult the following resources:

- IEEE 802.1q (Virtual LANs)
- IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)
- IEEE 802.3 (Fast Ethernet and Gigabit Ethernet)
- IEEE 802.3u (Fast Ethernet only)
- IEEE 802.3z (Gigabit Ethernet only)
- IEEE 802.3ae (10-Gigabit Ethernet only)
- IEEE 802.3ad (Link Aggregation)
- RFC 826—An Ethernet Address Resolution Protocol (November 1982)
- RFC 894—A Standard for the Transmission of IP Datagrams over Ethernet Networks (April 1984)
- RFC 1042—A Standard for the Transmission of IP Datagrams over IEEE 802 Networks (February 1988)
- RFC 1112—Host Extensions for IP Multicasting (August 1989)
- RFC 2516—Method for Transmitting PPP over Ethernet (PPPoE) (February 1998)

For more information about MIB support for Ethernet interfaces, consult the following resources:

- RFC 2863—The Interfaces Group MIB (June 2000)
- RFC 2668—Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs) (August 1999)
- RFC 2665—Definitions of Managed Objects for the Ethernet-like Interface Types (August 1998)

High-Density Ethernet

The following modules support high-density Ethernet:

- GE-HDE line module and GE-8 I/O module combination
- ES2 4G LM and ES2-S1 10GE IOA module combination
- ES2 4G LM and ES2-S1 GE-8 IOA module combination

In the current release, you cannot configure port parameters for high-density Ethernet. Instead, JUNOSe contains a packet classifier that enables the module to *intelligently drop* certain packets when the module becomes oversubscribed. The packet classifier inspects each incoming packet to determine whether to classify it as control traffic. To enhance network stability, the packet classifier prioritizes control traffic over non-control traffic (that is, data). The packet classifier randomly drops non-control packets when the interface is oversubscribed.

When the I/O module or IOA is oversubscribed, the packet classifier prioritizes the following types of control traffic:

- PPP discovery or PPP session
- Address Resolution Protocol (ARP)
- 802.3ad (link aggregation)
- 802.3 Spanning Tree Protocol (STP)
- IPv4 and IPv6 DHCP server
- IPv4 and IPv6 DHCP host
- IPv6 Neighbor Discovery
- IPv4 virtual router alert
- IPv4 and IPv6 Internet Group Management Protocol (IGMP)
- IPv4 packets with a type of service (ToS) precedence value set to Internetwork Control (C0)
- IPv6 packets with a traffic class precedence value set to Internetwork Control (C0)

Managing Port Redundancy on Gigabit Ethernet I/O Modules

By default, the software manages port redundancy on GE I/O modules automatically. However, you can manage redundancy on GE I/O modules as follows:

- Specify the time that the router waits for a port on a GE I/O module to become active before the router switches to the redundant port.

- Force a GE I/O module to switch operation from one port to the other.
- Disable port redundancy by specifying operation on one port only.

If you manage port redundancy manually, the router retains the manual configuration after the module reboots.

You can monitor the port redundancy configuration with the **show interfaces gigabitEthernet** command.

NOTE: The router manages failover in the same way for the GE I/O Modules and the GE-2 SFP I/O module.

link failover force

- Use to force a GE I/O module to switch operation from one port to the other.
- Select an interface on the GE I/O module before you issue this command.
- Example

  host1(config)#**interface gigabitEthernet 5/0**
  host1(config-if)#**link failover force**

- There is no **no** version.

link failover timeout

- Use to specify the time that the router waits for a port on a GE I/O module to become active before the router switches to the redundant port.
- Select an interface on the GE I/O module before you issue this command.
- Specify a time in the range 100–10,000 ms.
- Example

  host1(config)#**interface gigabitEthernet 5/0**
  host1(config-if)#**link failover timeout 1000**

- Use the **no** version to restore the default situation in which the router sets this time automatically.

link selection

- Use to disable redundancy on a GE I/O module by allowing operation on the specified port only.
- Select an interface on the GE I/O module before you issue this command.
- Example

  host1(config)#**interface gigabitEthernet 5/0**
  host1(config-if)#**link selection secondary**

- Use the **no** version to restore the default situation in which port redundancy is enabled.

Configuration Tasks for Ethernet

This section describes the options for configuring Ethernet interfaces.

You configure an Ethernet interface based on the requirements for your router configuration and the protocols you plan to route on the interface. Because you can configure an interface in different ways, Ethernet configuration tasks are divided into three primary areas. These areas are further described in separate sections in this chapter.

- Configuring the physical interface—You must perform basic configuration steps for all interfaces. This task begins with selecting an Ethernet interface and setting parameters such as line speed and MTU.
- Configuring VLANs and stacked VLANs (S-VLANs)—After you configure the physical interface, you must decide whether to configure the Ethernet interface with or without VLANs or S-VLANs. VLANs and S-VLANs enable you to multiplex multiple IP interfaces and PPPoE interfaces over a single physical Ethernet port. If you are not configuring with VLANs or S-VLANs, proceed to *Configuring Higher-Level Protocols over Ethernet* on page 225.
- Configuring higher-level protocols—You must determine which higher-level protocols, such as MPLS, to configure on the interface. This section focuses on non-VLAN configurations. You can configure some higher-level protocols, such as PPPoE, with or without VLANs.

Configuring the Physical Interface

This section describes how to complete the basic configuration for a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interface. CLI examples are provided with the individual command descriptions.

To configure an Ethernet interface:

1. Select an Ethernet interface.
2. (Optional) Specify the line speed and duplex mode.
3. (Optional) Specify the MTU.
4. (Optional) Set the time interval at which the router records bit and packet rates.
5. (Optional) Associate a name with the interface.
6. (Optional) Validate MAC addresses on a per interface basis.

duplex

- Use to specify the duplex mode.
- This command also works on the Fast Ethernet port on the SRP module on all E-series routers. For more information, see the *Managing the Ethernet Port on the SRP Module* in *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

NOTE: If you set either the line speed or duplex mode to automatically negotiate by using the **automatically negotiate** keyword, the router negotiates both parameters. You can specify different values to prevent the router from negotiating these parameters.

Automatic negotiation is not supported for the FE-8 SFP I/O module. For this I/O module, full duplex mode is the default.

- Example

  host1(config-if)#**duplex full**

- Use the **no** version to revert to the default, either automatically negotiate or full duplex (FE-8 SFP I/O module only)

ethernet description

- Use to associate a text description of up to 64 characters with an Ethernet interface.
- This command does not work for the Fast Ethernet port on the SRP module.
- The description is displayed in the output for **show configuration**, **show interfaces fastEthernet**, **show interfaces gigabitEthernet**, and **show interfaces tenGigabitEthernet** commands.
- Example

  host1(config-if)#**ethernet description abcd1234**

- Use the **no** version to remove the description from the interface.

interface fastEthernet

- Use to select a Fast Ethernet interface on a line module.
- You can also use it to select a Fast Ethernet management port on an SRP I/O module (ERX-7xx models, ERX-14xx models, and the ERX-310 router) or an SRP IOA (E120 and E320 routers). For information about managing the Fast Ethernet port on the SRP module, see *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.
- Use the *slot/port* [.*subinterface*] format for Fast Ethernet interfaces on ERX-7xx models, ERX-14xx models, and the ERX-310 router. Use the *slot/adapter/port* format for the SRP IOA on the E120 or E320 routers; the port on the SRP IOA is always identified by 0.
- Example 1—Selects a Fast Ethernet interface on ERX-7xx models, ERX-14xx models, or the ERX-310 router

  host1(config)#**interface fastEthernet 1/0**

- Example 2—Selects the Fast Ethernet management port on an E320 router

  host1(config)#**interface fastEthernet 6/0/0**

- Use the **no** version to remove IP from an interface or subinterface. You must issue the **no** version from the highest level down; you cannot remove an interface or subinterface if the one above it still exists.

interface gigabitEthernet

- Use to select a Gigabit Ethernet interface.

NOTE: On the GE I/O module, you can configure only the primary port, 0. The router automatically uses the redundant port, 0R, if the primary port fails.

On the GE-2 SFP I/O module, you can configure only the primary ports, 0 and 1. The router automatically uses the corresponding redundant port, 0R or 1R, if the primary port fails.

On the OC3-2 GE APS I/O module, you can configure only port 2. Ports 0 and 1 are reserved for OC3/STM1 ATM interfaces. This I/O module does not support redundant ports in the current release.

On the ES2-S1 GE-4 IOA, you can configure all four ports.

On the ES2-S1 GE-8 IOA, you can configure all eight ports.

- Use the *slot/port* [.*subinterface*] format for Gigabit Ethernet interfaces on ERX-7xx models, ERX-14xx models, or the ERX-310 router; use the *slot/adapter/port* format for Gigabit Ethernet interfaces on the E120 and E320 routers.
- Example 1—Selects a Gigabit Ethernet interface on ERX-7xx models, ERX-14xx models, and the ERX-310 router

  host1(config)#**interface gigabitEthernet 1/0**
  host1(config)#**interface gigabitEthernet 2/1**

- Example 2—Selects a Gigabit Ethernet interface on the E320 router

  host1(config)#**interface gigabitEthernet 4/0/1**

- Use the **no** version to remove IP from an interface. You must issue the **no** version from the highest level down; you cannot remove an interface or subinterface if the one above it still exists.

interface tenGigabitEthernet

- Use to select a 10-Gigabit Ethernet interface on the E120 router or the E320 router.

NOTE: On the ES2-S2 10GE PR IOA, you can configure only the primary port, 0. The router automatically uses the redundant port, 0R, if the primary port fails.

- Use the *slot/adapter/port* format.

- Example—Selects a 10-Gigabit Ethernet interface on the ES2-S1 10GE IOA

  host1(config)#**interface tenGigabitEthernet 4/0/1**

- Use the **no** version to remove IP from an interface. You must issue the **no** version from the highest level down; you cannot remove an interface or subinterface if the one above it still exists.

ip mac-validate

- Use to enable or disable MAC address validation on a per interface basis.
- Use the **strict** keyword to prevent transmission of IP packets that do not reside in the validation table.
- Use the **loose** keyword to enable IP packets to pass through even though the packets do not have entries in the validation table. Only packets that have matching IP–MAC pair entries in the table are validated.
- The default behavior is not to perform MAC address validation.
- Example

  host1(config)#**interface gigabitEthernet 2/0**
  host1(config-if)#**ip address 4.4.4.2 255.255.255.0**
  host1(config-if)#**ip mac-validate strict**
  host1(config-if)#**exit**

- Use the **no** version to disable the command.

NOTE: For additional information about MAC address validation, see the **arp validate** command description in *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

load-interval

- Use to set the time interval at which the router calculates bit and packet rate counters.
- This command does not work for the Fast Ethernet port on the SRP module.
- Specify a multiple of 30 seconds, in the range 30–300 seconds.
- The default value is 300 seconds.
- Example

  host1(config-if)#**load-interval 90**

- Use the **no** version to restore the default time interval, 300 seconds.

mtu

- Use to specify the MTU for an interface.
- Specify a value in the range 64–9188 bytes. The range for FE-8 I/O modules is 64–9042 bytes.
- This command does not work for the Fast Ethernet port on the SRP module.

- Example

  host1(config-if)#**mtu 9000**

- Use the **no** version to specify the default, 1518.

speed

- Use to specify the line speed.
- This command also works on the Fast Ethernet port on the SRP module on all E-series routers. For more information, see *Managing the Ethernet Port on the SRP Module* in *JUNOSe System Basics Configuration Guide, Chapter 6, Managing Modules*.

NOTE: If you set either the line speed or duplex mode to automatically negotiate by using the **automatically negotiate** keyword, the router negotiates both parameters. You can specify different values to prevent the router from negotiating these parameters.

Automatic negotiation is not supported for the FE-8 SFP I/O module. For this I/O module, the default speed is 100 Mbps.

- Example

  host1(config-if)#**speed 10**

- Use the **no** version to revert to the default, either automatically negotiate or 100 Mbps (FE-8 SFP I/O module only).

Configuring VLANs

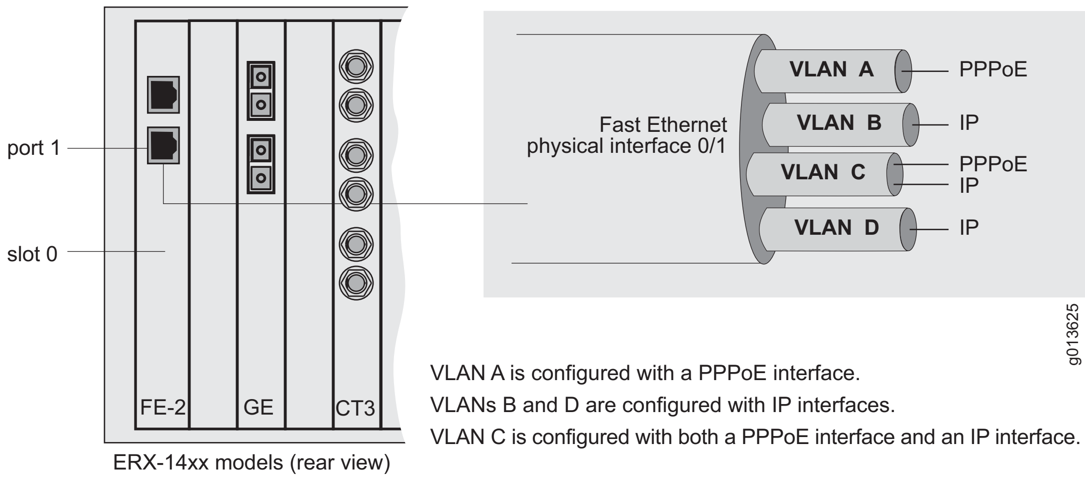
A virtual LAN (VLAN) enables multiplexing multiple IP and PPPoE interfaces and MPLS interfaces over a single physical Ethernet port. This multiplexing is accomplished through VLAN subinterfaces. Ethernet interfaces support the 802.1q-1998 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks, which the router uses as its standardized format for frame tagging.

The Ethernet V2 frame format enables multiplexing of different protocols over a single physical link. IEEE 802.1q compatibility extends the frame format by adding a tag that contains a VLAN ID. This feature enables multiplexing of different channels (VLANs) over the physical link; each channel is able to multiplex different protocols.

This capability works very much like ATM encapsulation as described in RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5 (September 1999). This encapsulation type enables multiplexing of multiple protocols over a single ATM virtual circuit (VC).

As shown in Figure 13, VLANs are similar to ATM VCs, with the VLAN ID serving the same function as the virtual path identifier (VPI) and virtual channel identifier (VCI) to multiplex the different channels over the physical link. The Ethernet protocol type serves the same function within a VLAN as the logical link control (LLC) subnetwork attachment point (SNAP) within a VC, to multiplex the different protocols over the channel.

Figure 13: Use of VLANs to Multiplex Different Protocols over a Single Physical Link



In a VLAN configuration, the router can send VLAN 0 *tagged* or *untagged frames*.

All VLAN subinterfaces use the MAC address of the Ethernet interface over which they are configured. However, some configurations, such as multiple IP over VLAN subinterfaces, require that you connect many VLAN subinterfaces to a single device. In these cases, the device uses the MAC address to identify and select the correct VLAN to use. When the MAC address is the same for all VLANs, uneven load balancing of traffic occurs. To ensure proper load balancing, you must assign unique MAC addresses to the individual VLAN subinterfaces that are connected to the device. Any ARP requests and responses generated for the IP address assigned to a VLAN subinterface use this MAC address.

You must assign the MAC address when you configure the VLAN ID. If you change the MAC address of the VLAN subinterface after you configure it, system errors can occur. To change the MAC address, you must first remove the VLAN subinterface and then reconfigure it.

For more information, see:

- *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*
- *JUNOSe Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol over Ethernet*

Creating a VLAN Major Interface

To use VLANs, you must first configure the Ethernet interface for VLAN encapsulation. This creates the VLAN major interface. For example:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/0**

2. Specify VLAN as the encapsulation method.

   host1(config-if)#**encapsulation vlan**

   The router creates the VLAN major interface.

You can now create multiple VLAN subinterfaces to carry higher-level protocols. For examples, see *Common VLAN Configurations*, next.

Common VLAN Configurations

Ethernet interfaces support IP, PPPoE, MPLS, or both IP and PPPoE on each VLAN. In addition to a VLAN major interface level, a VLAN subinterface level distinguishes the VLAN.

This section describes how to create the following common VLAN configurations, which you can configure on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces:

- IP over VLAN
- PPPoE over VLAN
- MPLS over VLAN
- IP over VLAN and PPPoE over VLAN

NOTE: You cannot configure VLANs on the Fast Ethernet port of the SRP module.

Configuring IP over VLAN

To configure IP over VLAN over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/0**

2. Specify VLAN as the encapsulation method.

   host1(config-if)#**encapsulation vlan**

   The VLAN major interface is added.

3. Create a VLAN subinterface by adding a subinterface number to the interface identification command.

   host1(config-if)#**interface fastEthernet 4/0.3**

4. Do one of the following:

   a. Assign a VLAN ID for the subinterface.

      host1(config-if)#**vlan id 201**

   b. Assign a VLAN ID and the optional unique MAC address for the subinterface.

      host1(config-if)#**vlan id 201 mac-address 0090.1a01.1234**

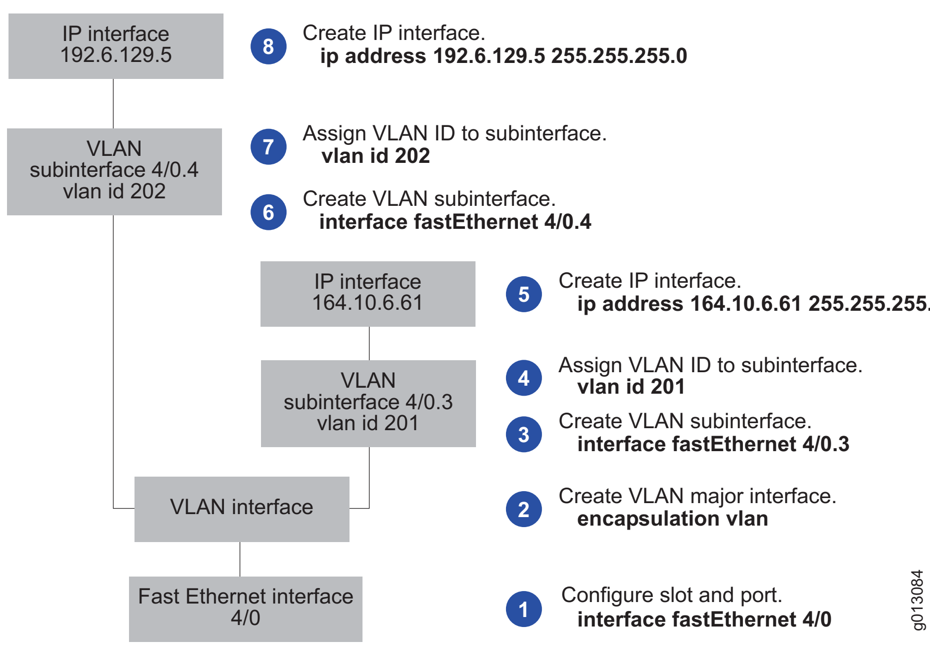
5. Assign an IP address and mask.

   host1(config-if)#**ip address 192.6.129.5 255.255.255.0**

6. (Optional) Configure additional VLAN subinterfaces by completing Steps 3 through 5.

Figure 14 illustrates the IP/VLAN/Fast Ethernet stacking, showing two separate VLAN subinterfaces. Configure one VLAN subinterface entirely; then configure the next VLAN subinterface.

Figure 14: Example of IP/VLAN/Fast Ethernet Stacking Configuration Steps



Configuring PPPoE over VLAN

To configure PPPoE over VLAN over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/1**

2. Specify VLAN as the encapsulation method.

   host1(config-if)#**encapsulation vlan**

   The VLAN major interface is added.

3. Create a VLAN subinterface by adding a subinterface number to the interface identification command.

   host1(config-if)#**interface fastEthernet 4/1.1**

4. Do one of the following:

   - Assign a VLAN ID for the subinterface.

     host1(config-if)#**vlan id 201**

   - Assign a VLAN ID and the optional unique MAC address for the subinterface.

     host1(config-if)#**vlan id 201 mac-address 0090.1a01.1234**

5. Specify PPPoE as the encapsulation method on the interface.

   host1(config-if)#**pppoe**

6. Create a PPPoE subinterface.

   host1(config-if)#**pppoe subinterface fastEthernet 4/1.1.1**

7. Specify PPP as the encapsulation method on the interface.

   host1(config-if)#**encapsulation ppp**

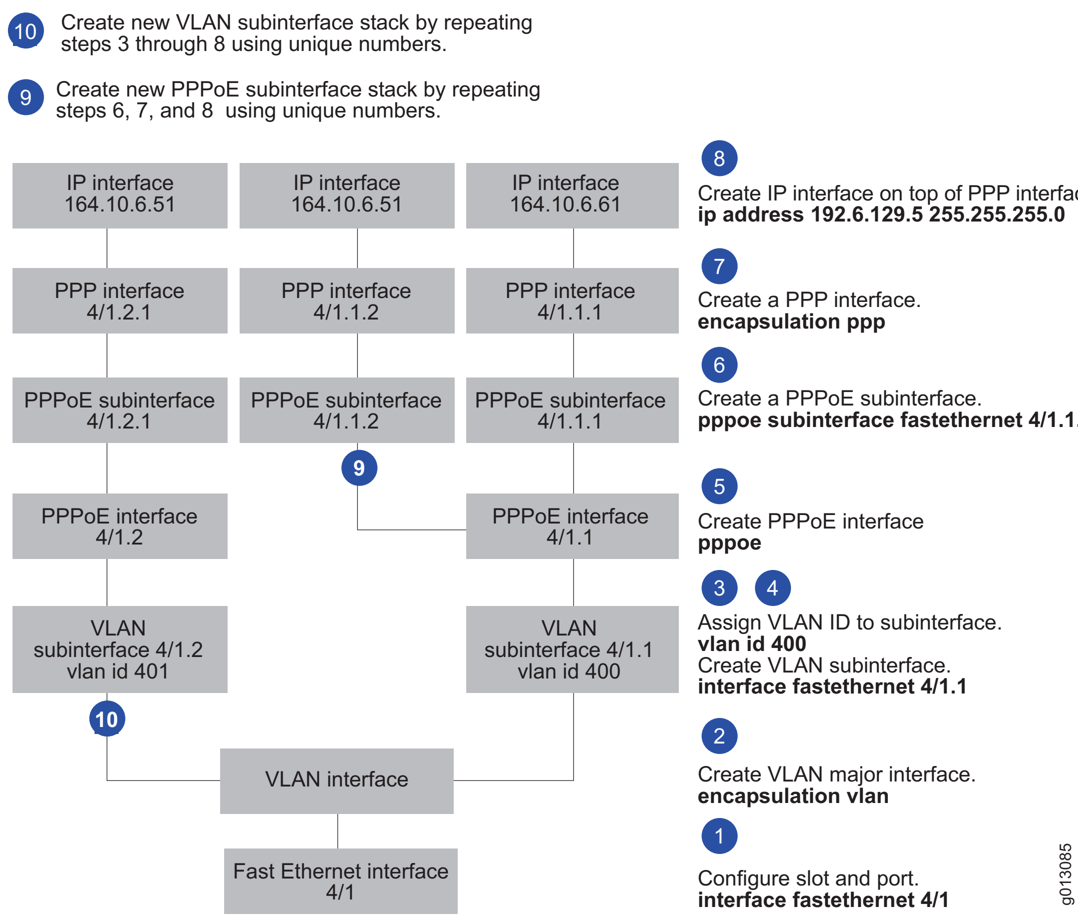
8. Assign an IP address and mask.

   host1(config-if)#**ip address 192.6.129.5 255.255.255.0**

9. (Optional) Configure additional VLAN subinterfaces by completing Steps 3 through 8.

Figure 15 on page 192 illustrates the PPPoE/VLAN/Fast Ethernet stacking, showing two separate VLAN subinterfaces. One VLAN subinterface has two PPPoE subinterfaces, and one VLAN subinterface has one PPPoE subinterface.

Figure 15: Example of PPPoE/VLAN/Fast Ethernet Stacking Configuration Steps



Configuring MPLS over VLAN

To configure MPLS over VLAN over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/0**

2. Specify VLAN as the encapsulation method.

   host1(config-if)#**encapsulation vlan**

   The VLAN major interface is added.

3. Create a VLAN subinterface by adding a subinterface number to the interface identification command.

   host1(config-if)#**interface fastEthernet 4/1.1**

4. Do one of the following:

   - Assign a VLAN ID for the subinterface.

     host1(config-if)#**vlan id 400**

   - Assign a VLAN ID and the optional unique MAC address for the subinterface.

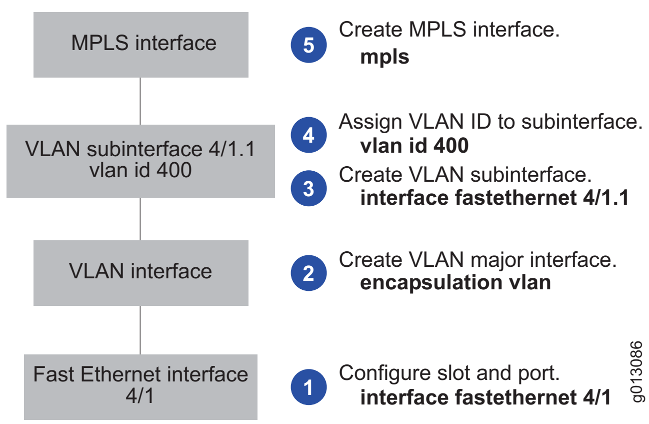
     host1(config-if)#**vlan id 400 mac-address 0090.1a01.1234**

5. Enable MPLS on the interface.

   host1(config-if)#**mpls**

Figure 16 illustrates the MPLS/VLAN/Fast Ethernet stacking, showing one VLAN subinterface.

Figure 16: Example of MPLS/VLAN/Fast Ethernet Stacking Configuration Steps



Configuring IP over VLAN and PPPoE over VLAN

To configure IP over VLAN with PPPoE over the same VLAN over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/1**

2. Specify VLAN as the encapsulation method.

   host1(config-if)#**encapsulation vlan**

   The VLAN major interface is added.

3. Create a VLAN subinterface by adding a subinterface number to the interface identification command.

   host1(config-if)#**interface fastEthernet 4/1.1**

4. Do one of the following:
   - Assign a VLAN ID for the subinterface.

     host1(config-if)#**vlan id 400**

   - Assign a VLAN ID and the optional unique MAC address for the subinterface.

     host1(config-if)#**vlan id 400 mac-address 0090.1a01.1234**

5. Create an IP interface on the same VLAN as the PPPoE interface.

   host1(config-if)#**ip address 164.10.6.71 255.255.255.0**

6. Specify PPPoE as the encapsulation method on the interface.

   host1(config-if)#**pppoe**

7. Create a PPPoE subinterface.

   host1(config-if)#**pppoe subinterface fastEthernet 4/1.1.1**

8. Specify PPP as the encapsulation method on the interface.

   host1(config-if)#**encapsulation ppp**

9. Assign an IP address and mask.

   host1(config-if)#**ip address 192.6.129.5 255.255.255.0**

10. (Optional) Configure additional PPPoE subinterfaces by completing Steps 7 through 9 using unique numbering.

To configure additional IP interfaces over the VLAN major interface:

1. Create a new VLAN subinterface by adding a unique subinterface number to the interface identification command.

   host1(config-if)#**interface fastEthernet 4/1.2**

2. Assign a VLAN ID for the subinterface.

   host1(config-if)#**vlan id 401**

3. Assign an IP address and mask.

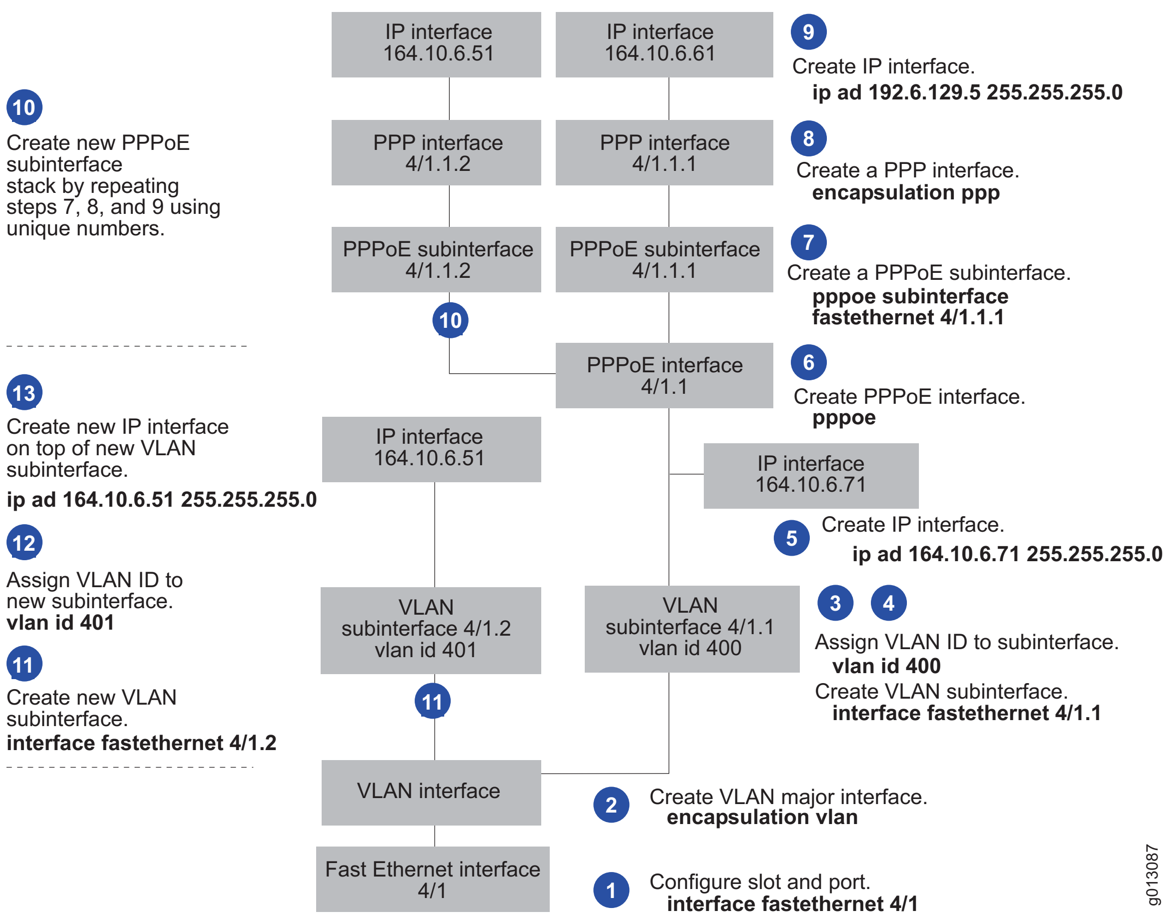
   host1(config-if)#**ip address 164.10.6.51 255.255.255.0**

Figure 17 illustrates the configuration steps for two VLAN subinterfaces. In this example:

- VLAN subinterface 4/1.1 has an IP interface, a PPPoE interface, and multiple PPPoE subinterface stacks.
- VLAN subinterface 4/1.2 has only an IP interface.

NOTE: Before you can remove a VLAN subinterface, you must remove the upper-layer interface stack.

Figure 17: Example of PPPoE over VLAN with IP over VLAN Stacking Configuration Steps



encapsulation ppp

- Use to configure PPP as the encapsulation method for the interface.
- Example

  host1(config-if)#**encapsulation ppp**
- Use the **no** version to disable PPP on the interface.

encapsulation vlan

- Use to configure VLAN as the encapsulation method for the interface.
- Example

  host1(config-if)#**encapsulation vlan**

- Use the **no** version to disable VLAN on an interface.

ip address

- Use to set a primary or secondary IP address for an interface or subinterface.
- Specify the layer 2 encapsulation before you set the IP address.
- Example

  host1(config-if)#**ip address 192.6.129.5 255.255.255.0**

- Use the **no** version to remove an IP address or disable IP processing.

pppoe

- Use to configure PPPoE as the encapsulation method on the interface.
- Example

  host1(config-if)#**pppoe**

- Use the **no** version to disable PPPoE on the interface.

pppoe subinterface fastEthernet

- Use to create a PPPoE subinterface on a Fast Ethernet interface.
- Example

  host1(config-if)#**pppoe subinterface fastEthernet 4/1.1.1**

- Use the **no** version to remove a PPPoE subinterface on a Fast Ethernet interface.

pppoe subinterface gigabitEthernet
pppoe subinterface tenGigabitEthernet

- Use to create a PPPoE subinterface on a Gigabit Ethernet interface or on a 10-Gigabit Ethernet interface.
- Example 1—Creates a PPPoE subinterface on an ERX-7xx model, ERX-14xx model, or the ERX-310 router

  host1(config-if)#**pppoe subinterface gigabitEthernet 4/2.1.1**

- Example 2—Creates a PPPoE subinterface on the E320 router

  host1(config-if)#**pppoe subinterface tenGigabitEthernet 4/0/2.1.1**

- Use the **no** version to remove a PPPoE subinterface on a Gigabit Ethernet interface or on a 10-Gigabit Ethernet interface.

vlan description

- Use to assign an alias or description to a VLAN subinterface.
- You can use a maximum of 64 characters for the description or to name the alias.
- Example

  host1(config-if)#**vlan description randolph56a**

- Use the **no** version to remove the VLAN description.

vlan id

- Use to specify the VLAN ID.
- Use a VLAN ID that is in the range 0–4095 and is unique within the Ethernet interface.
- Issue the **vlan id** command before any upper bindings are made, such as IP or PPPoE.
- Use the **mac-address** keyword to specify a unique MAC address for the VLAN subinterface. When you do not specify a unique MAC address, the VLAN uses the MAC address of the Ethernet interface.
- Use the optional keyword **untagged** to specify that frames be sent untagged. The keyword is valid only for VLAN ID 0. Tagged frames can be received, but untagged frames are sent.
- Examples

  host1(config-if)#**vlan id 400**
  host1(config-if)#**vlan id 4 255 mac-address 0090.1a01.1234**

- There is no **no** version.

Configuring S-VLANs

As described in *Configuring VLANs* on page 187, VLANs permit multiplexing multiple IP interfaces and PPPoE interfaces over a single physical Ethernet port by creating VLAN subinterfaces. As specified in IEEE Standard 802.1q, the 12-bit VLAN identifier's tagged frames enables the construction of a maximum of 4096 distinct VLANs. In an Ethernet B-RAS application environment, however, this VLAN limit is inadequate. A stacked VLAN (S-VLAN) provides a two-level VLAN tag structure, which extends the VLAN ID space to more than 16 million VLANs.

Creating an S-VLAN requires the use of a second encapsulation tag. The router performs decapsulation twice, once to get the S-VLAN tag and once to get the VLAN tag. This *double tagging* approach enables more than 16 million address possibilities, which more than satisfies the scaling requirement for Ethernet B-RAS applications.

VLAN and S-VLAN subinterfaces can coexist over the same VLAN major interface. You configure S-VLANs in the same way that you configure VLANs, with the addition of certain commands.

NOTE: See *JUNOSe Release Notes*, *Appendix A*, *System Maximums* for S-VLAN limitations.

Like VLANs, all S-VLAN subinterfaces use the MAC address of the Ethernet interface over which they are configured. For more information about assigning unique MAC address to the S-VLAN subinterface when assigning VLAN or S-VLAN IDs, see *Configuring VLANs* on page 187.

Configuring PPPoE over S-VLAN

To configure PPPoE over an S-VLAN over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/0**

2. Specify VLAN as the encapsulation method.

   host1(config-if)#**encapsulation vlan**

   The VLAN major interface is added.

3. Create a VLAN subinterface by adding a subinterface number to the interface identification command.

   host1(config-if)#**interface fastEthernet 4/1.1**

4. Assign an S-VLAN ID and a VLAN ID for the subinterface.

   host1(config-if)#**svlan id 4 255**

5. Assign an S-VLAN Ethertype.

   host1(config-if)#**svlan ethertype 88a8**

6. Specify PPPoE as the encapsulation method on the interface.

   host1(config-if)#**pppoe**

7. Create a PPPoE subinterface.

   host1(config-if)#**pppoe subinterface fastEthernet 4/1.1.1**

8. Specify PPP as the encapsulation method on the interface.

   host1(config-if)#**encapsulation ppp**

9. Assign an IP address and mask.

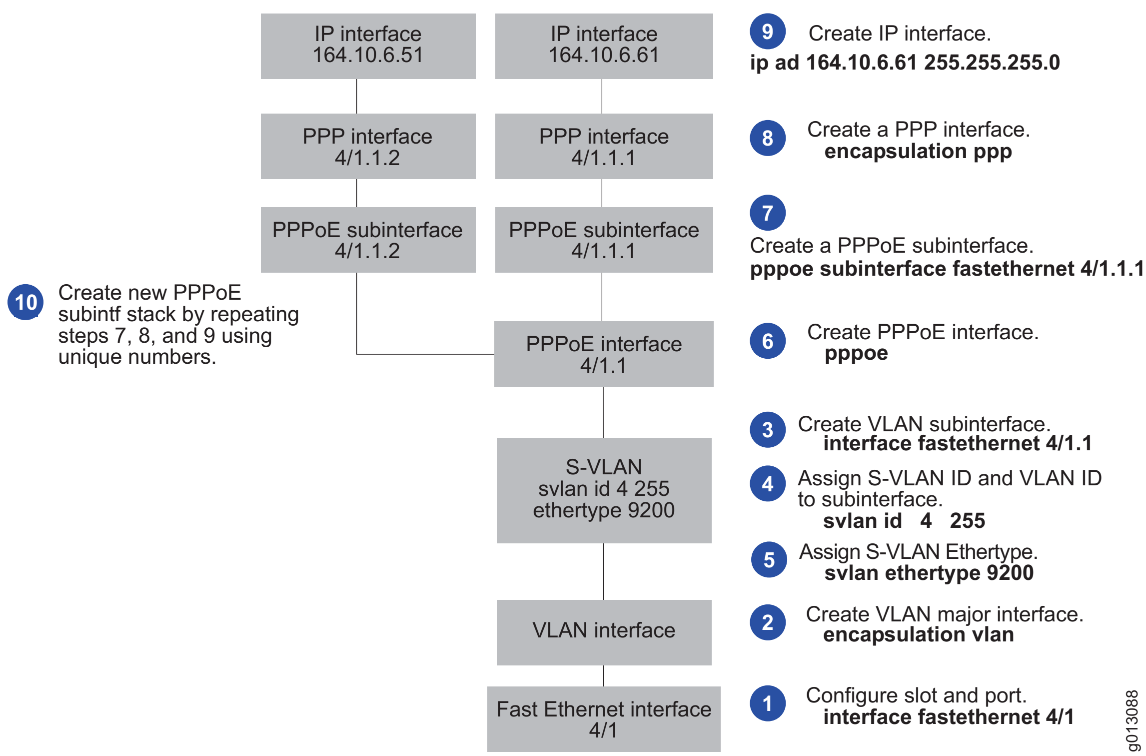
   host1(config-if)#**ip address 164.10.6.61 255.255.255.0**

10. (Optional) Configure additional PPPoE subinterfaces by completing Steps 7 through 9 using unique numbering.

Figure 18 shows one S-VLAN subinterface with multiple PPPoE subinterface stacks.

NOTE: Before you can remove an S-VLAN/VLAN subinterface, you must remove the upper-layer interface stack.

Figure 18: Example of PPPoE over S-VLAN Stacking Configuration Steps



encapsulation ppp

- Use to configure PPP as the encapsulation method for the interface.
- Use the **no** version to remove PPP as the encapsulation method on the interface.

encapsulation vlan

- Use to configure VLAN as the encapsulation method for the interface.
- Use the **no** version to remove VLAN as the encapsulation method on the interface.

ip address

- Use to set a primary or secondary IP address for an interface or subinterface.
- Specify the layer 2 encapsulation before you set the IP address.
- Use the **no** version to remove an IP address or disable IP processing.

pppoe

- Use to configure PPPoE as the encapsulation method on the interface.
- Use the **no** version to disable PPPoE on the interface.

pppoe subinterface fastEthernet

- Use to create a PPPoE subinterface on a Fast Ethernet interface.
- Use the **no** version to remove a PPPoE subinterface on a Fast Ethernet interface.

pppoe subinterface gigabitEthernet
pppoe subinterface tenGigabitEthernet

- Use to create a PPPoE subinterface on a Gigabit Ethernet interface or on a 10-Gigabit Ethernet interface.
- Use the **no** version to remove a PPPoE subinterface on a Gigabit Ethernet interface or on a 10-Gigabit Ethernet interface.

svlan ethertype

- Use to assign an Ethertype value for the S-VLAN subinterface.
- Choose one of the following Ethertype values:
  - 8100—Specifies Ethertype value 0x8100, as defined in IEEE Standard 802.1q
  - 88a8—Specifies Ethertype value 0x88a8, as defined in draft IEEE Standard 802.1ad
  - 9100—Specifies Ethertype value 0x9100, which is the default
- Use an Ethertype value that matches the Ethertype value set on the customer premises equipment (CPE) to which your router connects.
- Example

  host1(config-if)#**svlan ethertype 8100**

- Use the **no** version to restore the default value, 9100.

svlan id

- Use to assign S-VLAN IDs and VLAN IDs to VLAN subinterfaces.
- Use S-VLAN ID and VLAN ID numbers that are in the range 0–4095 and that are unique within the Ethernet interface.
- Use the **mac-address** keyword to specify a unique MAC address for the VLAN subinterface. When you do not specify a unique MAC address, the VLAN uses the MAC address of the Ethernet interface.
- Examples

  host1(config-if)#**svlan id 4 255**
  host1(config-if)#**svlan id 4 255 mac-address 0090.1a01.1234**

- Issue the **svlan id** command before any upper bindings are made, such as IP or PPPoE.
- There is no **no** version.

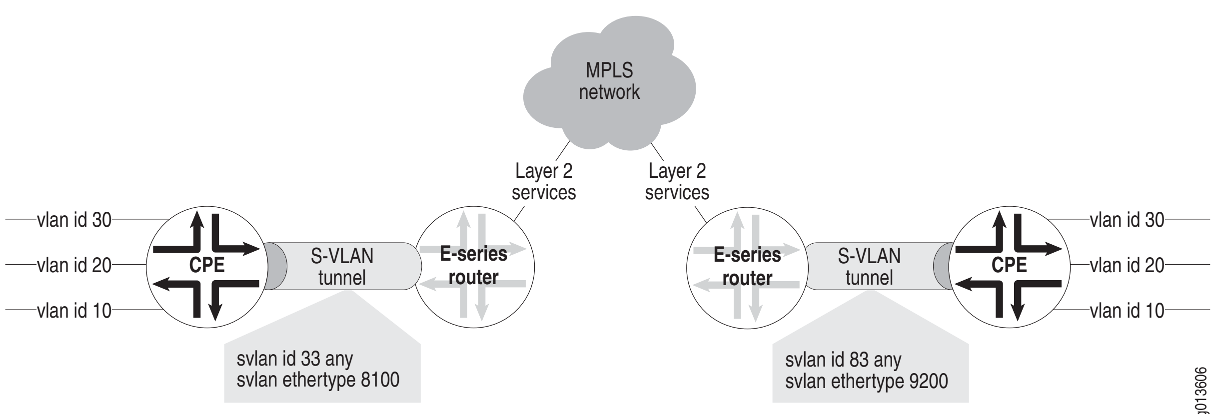
Configuring S-VLAN Tunnels for Layer 2 Services over MPLS

When you configure Ethernet layer 2 services over MPLS, you can create a special type of S-VLAN called an S-VLAN tunnel that uses a single interface to tunnel traffic from multiple VLANs across an MPLS network. The S-VLAN tunnel enables multiple VLANs, each configured with a unique VLAN ID tag, to share a common S-VLAN ID tag when they traverse an MPLS network.

Advantages

Using S-VLAN tunnels provides an easier and faster way to configure Ethernet layer 2 services over MPLS than using standard S-VLANs. For example, consider the network configuration shown in Figure 19.

Figure 19: S-VLAN Tunnels for Ethernet Layer 2 Services over MPLS



In this example, traffic from three VLAN subinterfaces must traverse the MPLS network. To accomplish this using standard S-VLANs, you issue the following commands to configure three separate S-VLANs with the same S-VLAN ID value and different VLAN IDs, as follows:

host1(config-if)#**svlan id 33 10**
host1(config-if)#**svlan id 33 20**
host1(config-if)#**svlan id 33 30**

By contrast, using an S-VLAN tunnel achieves the same result, but requires you to issue only a single **svlan id** command with the keyword **any** in place of the VLAN ID value. For example, the following command creates a single interface that tunnels traffic from VLANs configured with an S-VLAN ID of 33 and *any* VLAN ID to the same destination across the MPLS network. In effect, this command tunnels traffic from all three VLANs shown in Figure 19 on page 201.

host1(config-if)#**svlan id 33 any**

Interface Stacking

When you configure Ethernet layer 2 services over MPLS using S-VLAN tunnels, the only interface that you can stack over an S-VLAN tunnel is an MPLS tunnel, which you configure using the MPLS tunneling command (**mpls-relay** or **route interface**) that is appropriate for your configuration. Attempting to configure any other interface type—such as IP, MPLS (nontunnel), or PPPoE—over the S-VLAN tunnel causes the router to generate an error and reject the configuration as invalid.

For details about configuring MPLS and layer 2 services over MPLS, see:

- *JUNOSe BGP and MPLS Configuration Guide, Chapter 2, Configuring MPLS*
- *JUNOSe BGP and MPLS Configuration Guide, Chapter 4, Configuring Layer 2 Services over MPLS*

Configuration Example

This section uses the sample network topology shown in Figure 19 on page 201 to illustrate the steps for configuring S-VLAN tunnels for Ethernet layer 2 services over MPLS.

To configure S-VLAN tunnels for Ethernet layer 2 services over MPLS:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/0**

2. Specify VLAN as the encapsulation method to create the VLAN major interface.

   host1(config-if)#**encapsulation vlan**

3. Create a VLAN subinterface.

   host1(config-if)#**interface fastEthernet 8/1.1**

4. Create the S-VLAN tunnel. This interface tunnels traffic from VLANs configured with an S-VLAN ID of 33 and any VLAN ID to the same destination across the MPLS network.

   host1(config-if)#**svlan id 33 any**

5. Assign an S-VLAN Ethertype.

   host1(config-if)#**svlan ethertype 8100**

6. Create the MPLS tunnel interface using the appropriate MPLS tunneling command for your configuration. For example:

   host1(config-if)#**route interface tunnel mpls:tunnel3 45**

   For complete instructions on configuring the MPLS tunnel, see *JUNOSe BGP and MPLS Configuration Guide, Chapter 4, Configuring Layer 2 Services over MPLS*.

7. Repeat Steps 1 through 6 using unique values to configure the S-VLAN tunnel and MPLS tunnel interfaces on the remote E-series router. For example:

   host2(config)#**interface fastEthernet 3/1**
   host2(config-if)#**encapsulation vlan**
   host2(config-if)#**interface fastEthernet 3/1.1**
   host2(config-if)#**svlan id 83 any**
   host2(config-if)#**svlan ethertype 88a8**
   host2(config-if)#**route interface tunnel mpls:tunnel2 45**

encapsulation vlan

- Use to configure VLAN as the encapsulation method for the interface.
- Use the **no** version to disable VLAN on an interface.

interface fastEthernet

- Use to select a Fast Ethernet interface on a line module.
- Example

  host1(config)#**interface fastEthernet 3/1**

- Use the **no** version to remove the interface or subinterface. You must issue the **no** version from the highest level down; you cannot remove an interface or subinterface if the one above it still exists.

route interface

- Use to route layer 2 traffic on a specific tunnel interface.
- Use the **no** version to negate this command.

NOTE: For details on the use of this command, see *JUNOSe BGP and MPLS Configuration Guide, Chapter 4, Configuring Layer 2 Services over MPLS*.

svlan ethertype

- Use to assign an Ethertype value for the S-VLAN tunnel interface.
- Choose one of the following Ethertype values:
  - 8100—Specifies Ethertype value 0x8100, as defined in IEEE Standard 802.1q
  - 88a8—Specifies Ethertype value 0x88a8, as defined in draft IEEE Standard 802.1ad
  - 9100—Specifies Ethertype value 0x9100, which is the default
- Use an Ethertype value that matches the Ethertype value set on the customer premises equipment (CPE) to which your router connects.
- Example

  host1(config-if)#**svlan ethertype 8100**

- Use the **no** version to restore the default value, 9100.

svlan id

- Use to create an S-VLAN tunnel interface for configuring Ethernet layer 2 services over MPLS.
- Assign an S-VLAN ID value in the range 0–4095 that is unique within the Ethernet interface.
- Use the **any** keyword to tunnel traffic from VLANs configured with the specified S-VLAN ID and any VLAN ID to the same destination across an MPLS network.
- Issue the **svlan id** command with the **any** keyword before you configure the upper binding, which must be an MPLS tunnel interface. Attempting to configure any other interface type over the S-VLAN tunnel causes an error.
- Example

  host1(config-if)#**svlan id 1000 any**

- There is no **no** version.

S-VLAN Oversubscription

When you configure S-VLAN subinterfaces over Ethernet interfaces to support dynamic PPPoE subinterfaces, you can take advantage of S-VLAN oversubscription.

The following module combinations support S-VLAN oversubscription:

- GE/FE line module and all of its associated I/O modules
- GE-2 line module and the GE-2 SFP I/O module
- GE-HDE line module and its associated I/O modules
- OC3/STM1 GE/FE line module and the OC3-2 GE APS I/O module
- ES2 4G LM and its associated Gigabit Ethernet and 10-Gigabit Ethernet IOAs
- ES2 10G LM and its associated Gigabit Ethernet and 10-Gigabit Ethernet IOAs

The maximum number of S-VLANs that you can create per I/O module with PPPoE major interfaces stacked over them is greater than the maximum number of dynamic PPPoE subinterfaces. The maximum number of PPP interfaces supported per line module is directly proportional to the maximum number of PPPoE subinterfaces.

As a result, you can oversubscribe S-VLANs by configuring up to the maximum number of S-VLANs supported on these I/O modules, knowing that no more than the maximum number of supported PPP sessions can be connected to the router at any one time.

For configuration instructions, see *Configuring Dynamic PPPoE over Static PPPoE with Ethernet and S-VLAN Interface Columns* in *JUNOSe Link Layer Configuration Guide, Chapter 12, Configuring Dynamic Interfaces*.

For specific information about the maximum number of S-VLANs supported per I/O module and the maximum number of PPP interfaces and PPPoE subinterfaces supported per line module, see *JUNOSe Release Notes*, *Appendix A*, *System Maximums*.

NOTE: The E120 and E320 routers can support up to two IOAs per line module. This maximum number of S-VLANs per line module does not change if one or two IOAs are installed.

Configuring 802.3ad Link Aggregation for Ethernet

IEEE 802.3ad link aggregation enables you to group Ethernet interfaces at the physical layer to form a single link layer interface, also known as a link aggregation group (LAG) or bundle. For more information, see IEEE Standard 802.3ad, Link Aggregation.

Some users require more bandwidth in their network than a single Fast Ethernet link can provide, but cannot afford the expense or do not need the bandwidth of a higher-speed Gigabit Ethernet link. Using IEEE 802.3ad link aggregation in this situation provides increased port density and bandwidth at lower cost. For example, if you need 450 Mbps of bandwidth to transmit data and have only a 100-Mbps Fast Ethernet link, creating a LAG bundle containing five 100-Mbps Fast Ethernet links is more cost effective than purchasing a single Gigabit Ethernet link.

For information about the modules that support link aggregation, see *ERX Module Guide, Appendix A, Module Protocol Support* and *E120 and E320 Module Guide, Appendix A, IOA Protocol Support*.

LACP

The Link Aggregation Control Protocol (LACP) is a mechanism for exchanging port and system information to create and maintain LAG bundles. The LAG bundle distributes MAC clients across the link layer interface and collects traffic from the links to present to the MAC clients of the LAG bundle.

To create the links in the LAG bundles, you can add one or more Ethernet physical interfaces to it. The LACP detects Ethernet interfaces as links if they are configured on the same line module and have the same physical layer characteristics. The LACP also assigns to the LAG bundle the same MAC address of the Ethernet link with the highest port priority, which is the lowest value.

The LACP also controls the exchange of LACP protocol data units (PDUs) between the Ethernet links in the LAG bundle. The PDUs contain information about each link and enable the LAG bundle to maintain them.

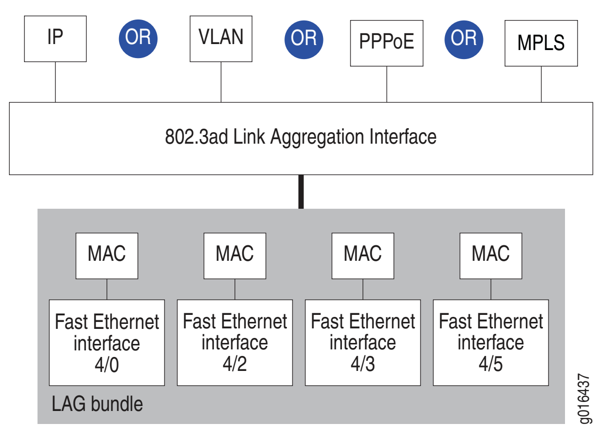
By default, Ethernet links do not exchange PDUs, which contain information about the state of the link. You can configure Ethernet links to actively transmit PDUs, or passively transmit them, sending out LACP PDUs only when it receives them from another link. The transmitting link is known as the *Actor* and the receiving link is known as the *Partner*.

Higher-Level Protocols

After you configure the LAG bundle, you can route IP traffic over it, create a VLAN over it, route PPPoE traffic over it, or route MPLS traffic over it.

Figure 20 displays the interface stack for 802.3ad link aggregation.

Figure 20: Interface Stack for 802.3ad Link Aggregation



For information about configuring higher-level protocols over VLANs, see *Common VLAN Configurations* on page 189.

Load Balancing and QoS

You can configure load balancing across 802.3ad links to provide quality of service (QoS). To ensure that QoS is symmetrically applied to all the links, the router periodically rebalances the traffic on the LAG. When you attach a QoS profile to the LAG, the load balancing properties that are configured are applied to the LAG, and determines how traffic is distributed.

For example, if VLANs are configured, IP queues are provisioned over the VLANs. In this case, the default behavior is per-VLAN load balancing.

For more information, see *JUNOSe Quality of Service Configuration Guide, Chapter 20, Configuring QoS for Gigabit Ethernet Interfaces and VLAN Subinterfaces*.

Configuration Tasks for 802.3ad Link Aggregation

To configure link aggregation on Ethernet interfaces, you must configure the Ethernet interface, create the LAG bundle, and add the Ethernet interface as a member link in the LAG bundle. Optionally, you can then configure IP, a VLAN subinterface, a PPPoE subinterface, or MPLS for the LAG bundle.

For more information about specifying LAG interfaces and subinterfaces on E-series routers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

Configuring an Ethernet Physical Interface

To configure a member link, perform the following steps:

1. Specify a Fast Ethernet or Gigabit Ethernet interface for which you want to create a member link.

   host1(config)#**interface gigabitEthernet 2/0**

2. Configure LACP in passive or active mode.

   host1(config-if)#**lacp active**

3. Specify the speed and the duplex mode for the Ethernet interface.

   host1(config-if)#**speed 100**
   host1(config-if)#**duplex full**

4. To configure additional member links, repeat steps 1 to 3.

NOTE: All of the member links that you configure must have the same physical layer characteristics, such as speed and duplex mode.

Configuring a LAG Bundle

To configure a LAG bundle and add member links, perform the following steps:

1. Create the LAG bundle.

   host1(config)#**interface lag bundleBoston**

2. Add a member link to the LAG bundle.

   host1(config-if)#**member–interface gigabitEthernet 2/0**

Configuring IP for a LAG Bundle

To configure IP for a LAG bundle, perform the following steps:

1. Specify the LAG bundle.

   host1(config)#**interface lag bundleBoston**

2. Assign an IP address and mask.

   host1(config-if)#**ip address 192.5.127.8 255.255.255.0**

Configuring a VLAN Subinterface for a LAG Bundle

To configure a VLAN subinterface for the LAG bundle, perform the following steps:

1. Specify VLAN as the encapsulation method.

   host1(config-if)#**encapsulation vlan**

2. Specify the VLAN subinterface for the LAG bundle by adding a unique subinterface number to the LAG interface identification command.

   host1(config)# **interface lag bundleBoston.1**

3. Assign a VLAN ID for the subinterface.

   host1(config-if)#**vlan id 203**

4. Assign an IP address and mask.

   host1(config-if)#**ip address 192.168.1.1 255.255.0.0**

Configuring a PPPoE Subinterface for a LAG Bundle

To configure a PPPoE subinterface for the LAG bundle, perform the following steps:

1. Specify PPPoE as the encapsulation method.

   host1(config-if)#**encapsulation pppoe**

2. Specify the PPPoE subinterface for the LAG bundle in either of the following ways:

- Use the **interface lag** command to add a unique subinterface number to the LAG bundle name.

  host1(config)#**interface lag bundleBoston.2**

- Use the **pppoe subinterface lag** command to add a unique subinterface number to the LAG bundle name.

  host1(config)#**pppoe subinterface lag bundleBoston.2**

3. Specify PPP as the encapsulation method on the PPPoE subinterface.

   host1(config-if)#**encapsulation ppp**

4. Assign an IP address and mask.

   host1(config-if)#**ip address 192.168.1.2 255.255.0.0**

You can also configure a PPPoE subinterface over a VLAN subinterface over a LAG bundle. For an example of this configuration, see *Example: Configuring a PPPoE Subinterface over a VLAN for a LAG Bundle* on page 211.

Configuring MPLS for a LAG Bundle

To configure MPLS for a LAG bundle, perform the following steps:

1. Specify the LAG bundle.

   host1(config)#**interface lag bundleBoston**

2. Create an MPLS interface.

   host1(config-if)#**mpls**

802.3ad Link Aggregation Configuration Examples

This section provides examples for the following 802.3ad link aggregation configurations:

- IP interface over a LAG bundle
- PPPoE subinterface over a LAG bundle
- PPPoE subinterface over a VLAN subinterface over a LAG bundle
- MPLS over a LAG bundle
- MPLS over a VLAN subinterface over a LAG bundle

Example: Configuring an IP Interface for a LAG Bundle

The following example displays configuration of LACP for two Fast Ethernet interfaces in slot 0. The interfaces are enabled for active LACP. The speed and duplex characteristics are the same for both interfaces.

```
host1(config)#interface fastEthernet 0/0
host1(config-if)#speed 100
host1(config-if)#duplex full
host1(config-if)#lacp active
host1(config-if)#interface fastEthernet 0/5
host1(config-if)#speed 100
host1(config-if)#duplex full
host1(config-if)#lacp active
```

The following commands create a virtual router, add the Ethernet physical interfaces to a LAG bundle named bundleBoston, and assign an IP address and mask to the bundle.

```
host1(config)#virtual-router boston
host1:boston(config)#interface lag boston
host1:boston(config-if)#member-interface fastEthernet 0/0
host1:boston(config-if)#member-interface fastEthernet 0/5
host1:boston(config-if)#ip address 1.1.1.1 255.255.255.0
```

Example: Configuring a PPPoE Subinterface for a LAG Bundle

The following example displays LACP configuration for two Fast Ethernet interfaces in slot 4. The interfaces are enabled for passive LACP. The speed and duplex characteristics are the same for both interfaces.

```
host1(config)#interface fastEthernet 4/0
host1(config-if)#speed 100
host1(config-if)#duplex full
host1(config-if)#lacp passive
host1(config-if)#interface fastEthernet 4/3
host1(config-if)#speed 100
host1(config-if)#duplex full
host1(config-if)#lacp passive
```

The following commands add the Ethernet physical interfaces to a LAG bundle named chicago.

```
host1(config)#interface lag chicago
host1(config-if)#member-interface fastEthernet 4/0
host1(config-if)#member-interface fastEthernet 4/3
```

The following commands configure a PPPoE subinterface for the LAG bundle named chicago. In the LAG interface identification command (**interface lag chicago.1**), the number 1 represents the subinterface number for the PPPoE subinterface.

```
host1(config-if)#encapsulation pppoe
host1(config)#interface lag chicago.1
host1(config-if)#encapsulation ppp
host1(config-if)#ip address 10.10.1.1 255.255.0.0
```

As an alternative to using the command **interface lag chicago.1** to configure the PPPoE subinterface in this example, you can also use the command **pppoe subinterface lag chicago.1** to achieve the same result. For more information, see **pppoe subinterface lag** on page 214.

Example: Configuring a PPPoE Subinterface over a VLAN for a LAG Bundle

The following example displays LACP configuration for two Fast Ethernet interfaces in slot 3. The interfaces are enabled for active LACP. The speed and duplex characteristics are the same for both interfaces.

```
host1(config)#interface fastEthernet 3/0
host1(config-if)#speed 100
host1(config-if)#duplex full
host1(config-if)#lacp active
host1(config-if)#interface fastEthernet 3/1
host1(config-if)#speed 100
host1(config-if)#duplex full
host1(config-if)#lacp active
```

The following commands add the Ethernet physical interfaces to a LAG bundle named sunnyvale.

```
host1(config)#interface lag sunnyvale
host1(config-if)#member-interface fastEthernet 3/0
host1(config-if)#member-interface fastEthernet 3/1
```

The following commands configure a VLAN subinterface for the LAG bundle named sunnyvale. In the LAG interface identification command (**interface lag sunnyvale.1**), the number 1 represents the subinterface number for the VLAN subinterface.

```
host1(config-if)#encapsulation vlan
host1(config)#interface lag sunnyvale.1
host1(config-if)#vlan id 100
```

The following commands configure a PPPoE subinterface over the VLAN subinterface for the LAG bundle named sunnyvale. In the LAG interface identification command (**interface lag sunnyvale.1.2**), the number 2 represents the subinterface number for the PPPoE subinterface.

```
host1(config-if)#encapsulation pppoe
host1(config)#interface lag sunnyvale.1.2
host1(config-if)#encapsulation ppp
host1(config-if)#ip address 10.10.2.2 255.255.0.0
```

As an alternative to using the command **interface lag sunnyvale.1.2** to configure the PPPoE subinterface in this example, you can also use the command **pppoe subinterface lag sunnyvale.1.2** to achieve the same result. For more information, see **pppoe subinterface lag** on page 214.

Example: Configuring MPLS for a LAG Bundle

The following example displays configuration of LACP for two Fast Ethernet interfaces in slot 5. The interfaces are enabled for active LACP. The speed and duplex characteristics are the same for both interfaces.

host1(config)#**interface fastEthernet 5/0**
host1(config-if)#**speed 100**
host1(config-if)#**duplex full**
host1(config-if)#**lacp active**
host1(config-if)#**interface fastEthernet 5/1**
host1(config-if)#**speed 100**
host1(config-if)#**duplex full**
host1(config-if)#**lacp active**

The following commands create a virtual router, add the Ethernet physical interfaces to a LAG bundle named kanata, assign an IP address, and configure MPLS.

host1(config)#**virtual router kanata**
host1:kanata(config)#**interface lag kanata**
host1:kanata(config-if)#**member-interface fastEthernet 0/0**
host1:kanata(config-if)#**member-interface fastEthernet 0/5**
host1:kanata(config-if)#**ip address 1.1.1.1 255.255.255.0**
host1(config-if)#**mpls**

Example: Configuring MPLS over a VLAN for a LAG Bundle

The following example displays configuration of LACP for two Fast Ethernet interfaces in slot 5. The interfaces are enabled for active LACP. The speed and duplex characteristics are the same for both interfaces.

host1(config)#**interface fastEthernet 5/0**
host1(config-if)#**speed 100**
host1(config-if)#**duplex full**
host1(config-if)#**lacp active**
host1(config-if)#**interface fastEthernet 5/1**
host1(config-if)#**speed 100**
host1(config-if)#**duplex full**
host1(config-if)#**lacp active**

The following commands add the Ethernet physical interfaces to a LAG bundle named kanata.

host1(config)#**virtual router kanata**
host1:kanata(config)#**interface lag kanata**
host1:kanata(config-if)#**member-interface fastEthernet 5/0**
host1:kanata(config-if)#**member-interface fastEthernet 5/1**

The following commands configure a VLAN subinterface for the LAG bundle named kanata. In the LAG interface identification command (**interface lag kanata.1**), the number 1 represents the subinterface number for the VLAN subinterface.

host1:kanata(config-if)#**encapsulation vlan**
host1:kanata(config)#**interface lag kanata.1**
host1:kanata(config-if)#**vlan id 100**

The following command creates an MPLS interface.

host1:kanata(config)#**mpls**

interface lag

- Use to create an IEEE 802.3ad LAG interface, also known as an LAG bundle, or a subinterface for the LAG bundle.
- Examples

  host1(config)#**interface lag boston**
  host1(config)#**interface lag boston.2**
  host1(config)#**interface lag boston.2.1**

- Use the **no** version to delete the LAG bundle.

lacp

- Use to configure whether an Ethernet link in a LAG bundle participates actively or passively in the LACP.
- Use the **active** keyword to indicate that the Ethernet link participates in the protocol regardless of whether its Partner member link is set to active or passive LACP PDU participation.
- Use the **passive** keyword to indicate that the Ethernet link to transmit LACP PDUs only when it receives LACP PDUs from its Partner member link.
- By default, Ethernet links in a LAG bundle do not send LACP PDUs.
- Example

  host1(config-if)#**lacp active**

- Use the **no** version to restore the default behavior.

lacp port-priority

- Use to set the priority for an Ethernet link in a LAG bundle.
- The member with the lowest value has the highest priority, and is selected to join the LAG bundle first.
- Valid values are in the range 0–65535.
- Example

  host1(config-if)#**lacp port-priority 100**

- Use the **no** version to restore the default value of 32768.

member-interface

- Use to add a Fast Ethernet interface or Gigabit Ethernet interface, also known as a bundle member, to a LAG bundle.
- Example

  host1(config-if)#**member-interface fastEthernet 4/0**

- Use the **no** version to remove the specified Ethernet link from the bundle.

mpls

- Use to enable, disable, or delete MPLS on an interface. MPLS is disabled by default.
- Example

  host1(config)#**mpls**

- Use the **no** version to halt MPLS on the interface and delete the MPLS interface configuration.

pppoe subinterface lag

- Use to create a PPPoE subinterface on a LAG bundle.
- Example

  host1(config-if)#**pppoe subinterface lag boston.1**

- Use the **no** version to remove the PPPoE subinterface from the LAG bundle.

virtual-router

- From Global Configuration mode, use this command to create a virtual router or access the context of a previously created virtual router or a VRF.
- Example

  host1(config)#**virtual-router boston**

- Use the **no** version of the command only to delete the VR and return the router to the default VR.

Configuring Ethernet Link Redundancy

You can use 802.3ad Link Aggregation (LAG) to configure Ethernet link redundancy for Fast Ethernet and Gigabit Ethernet interfaces. Ethernet link redundancy enables you to protect against physical link failure and account for network topology changes that redirect network traffic to redundant ports.

The following configurations are available:

- LAG to LAG—Provides redundancy capabilities for two or more ports that are assigned to a LAG. One member link is configured as the backup interface for all other ports in the LAG bundle (1:N). Traffic is not forwarded over the backup member interface; it is disabled until it takes over for an active member interface.

- LAG to non-LAG—Provides redundancy capabilities when redundant ports are connected to a bridged network that has Rapid Spanning Tree Protocol (RSTP) controlling the topology. This configuration supports only two links in the LAG.

For information about the modules that support link aggregation, see *ERX Module Guide, Appendix A, Module Protocol Support* and *E120 and E320 Module Guide, Appendix A, IOA Protocol Support*.

Ethernet Link Redundancy Configuration Models

The link connections determine the configuration model for link redundancy. The following connection types are available:

- Single-homed—Connections are between the local Ethernet interface and a single remote device. When the peer is also configured with LAG, LACP can be used to control link access.

- Dual-homed—Connections are between two separate, uncoordinated remote devices. The remote interfaces can be on the same module or on separate hardware. If LAG is not configured on the peers, LACP cannot be used to select ports; other protocols such as RSTP can be used.

The type of hardware used for connections further characterizes the single-homed and dual-homed configuration models. The following hardware types are available:

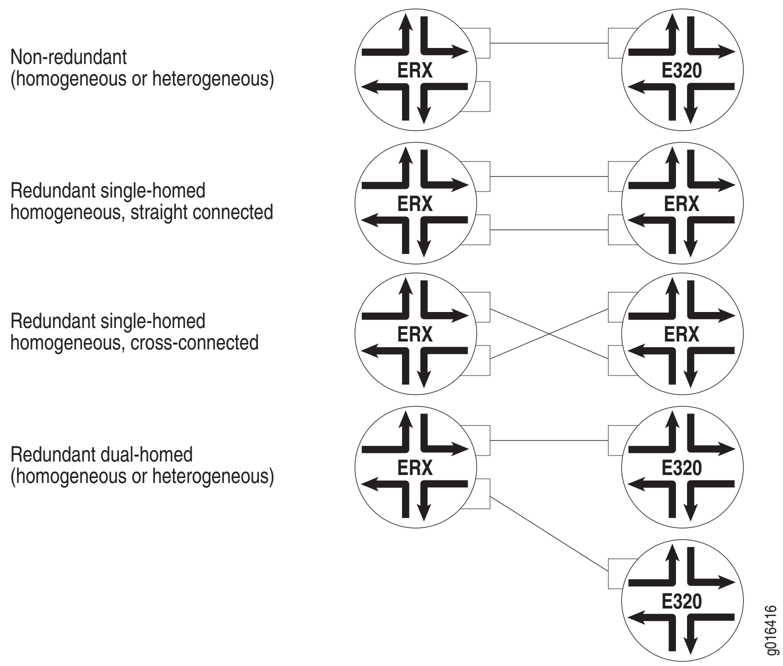
- Homogeneous—Remote interface is on another Fast Ethernet or Gigabit Ethernet port in a back-to-back router configuration of identical hardware and JUNOSe software versions. Both interfaces support the same redundant cabling and algorithm. The interfaces can be cabled on the same ports (port 0–port 0, port 1–port 1) or cross-cabled (port 0–port 1, port 1–port 0).

- Heterogeneous—Remote interface is on a different type of hardware that might or might not support redundant cabling, or on the same type of equipment with different software versions. For example, a heterogeneous configuration can include an ES2-S1 GE-4 IOA and an ES2-S1 GE-8 IOA on the E320 router, or an E-series router operating JUNOSe software connected to another vendor's router and software.

NOTE: You cannot configure link redundancy across different types of line modules in a router. You also cannot configure link redundancy across two GE-4 IOAs on the E120 router or the E320 router.

Figure 21 illustrates the configuration models for Ethernet link redundancy.

Figure 21: Ethernet Link Redundancy Configuration Models



Ethernet Link Redundancy Configuration Diagrams

The diagrams in this section illustrate examples of Ethernet link redundancy configurations. The diagrams display adjacent ports bundled in a LAG.

GE-2 Line Module Configurations

These diagrams compare physical port redundancy and link redundancy on a GE-2 line module.

Figure 22 displays a GE-2 line module with physical port redundancy on both ports.

Figure 22: GE-2 Line Module Using Physical Port Redundancy

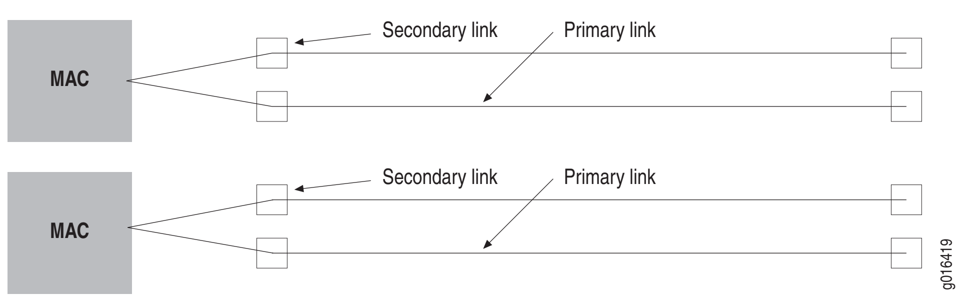
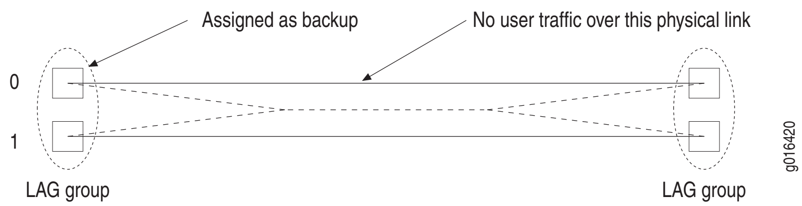


Figure 23 displays a single-homed configuration with port 0 backing up port 1 on a GE-2 line module.

Figure 23: Single-Homed GE-2 Line Module Configuration



FE-8 Line Module Configurations

Figure 24 displays an FE-8 line module with a link failure in a 1:N single-homed configuration.

Figure 24: Single-Homed FE-8 Line Module Configuration (1:N)

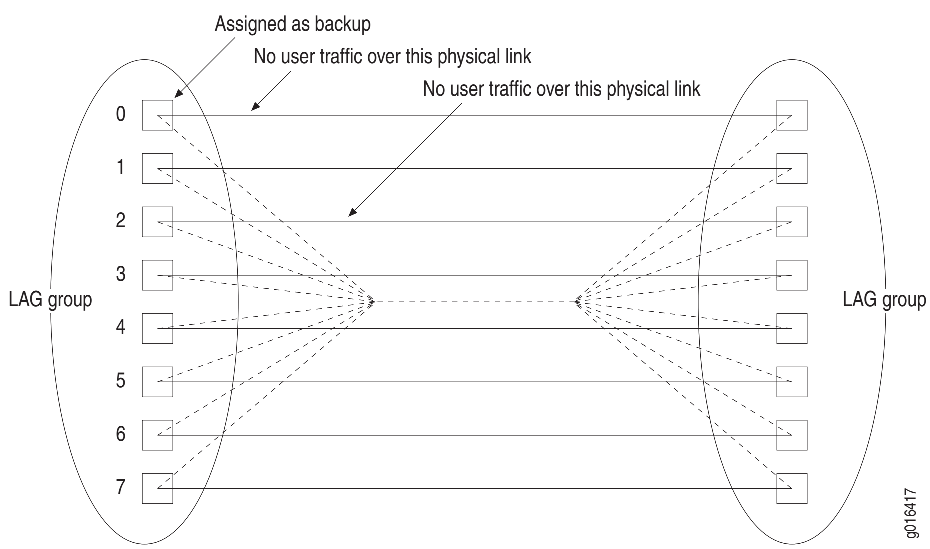
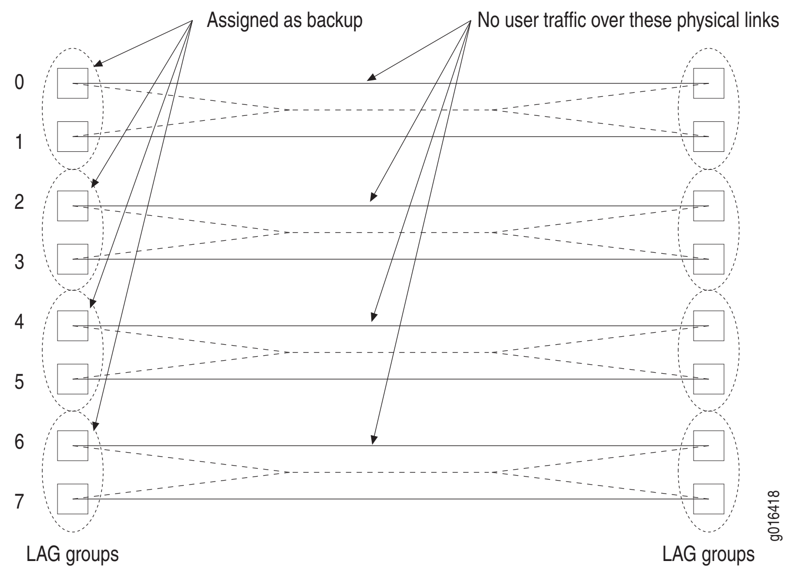


Figure 25 displays an FE-8 line module with four redundant Ethernet links in a 1:1 configuration.

Figure 25: FE-8 Line Module with 4 Redundant Ethernet Links (1:1)



E120 and E320 Router Configurations

Figure 26 and Figure 27 display link redundancy configurations on the E120 and E320 routers.

Figure 26 displays a single-homed 1:4 configuration on an E120 router.

Figure 26: Single-Homed GE-4 IOA Configuration (1:4)

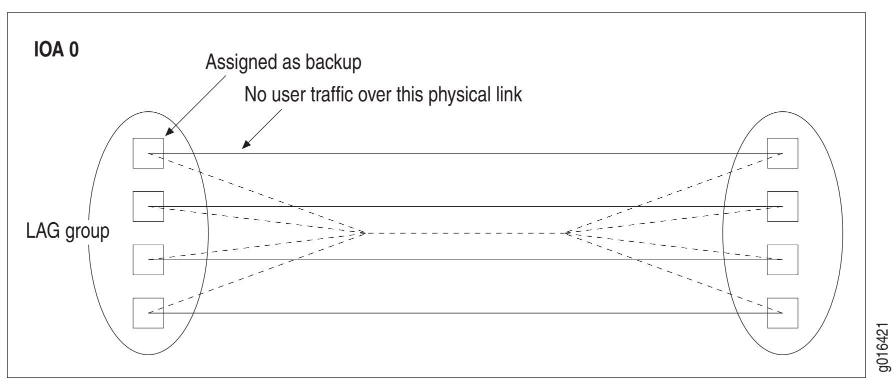
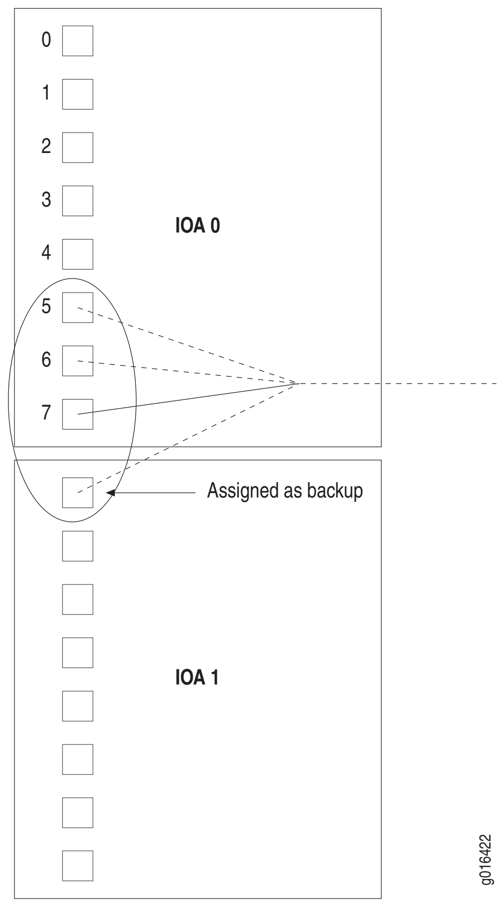


Figure 27 displays an E320 router with 1:N configuration across IOAs.

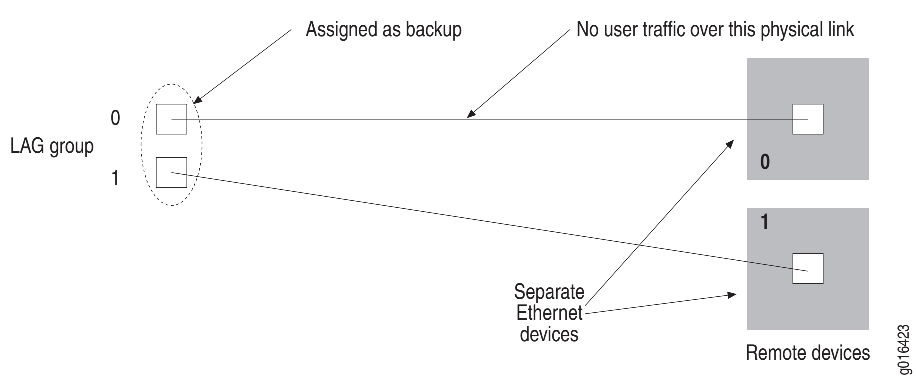
Figure 27: GE-8 IOA Configuration Across IOAs (1:N)



Dual-Homed Configurations with LAG Disabled

Figure 28 displays how you can configure Ethernet link redundancy with LACP disabled locally using a dual-homed configuration. LACP is disabled because there is no LAG at the peer.

Figure 28: Dual-Homed Configuration (1:1)



Ethernet Link Redundancy Behavior

When you create a LAG bundle, you can configure LACP with the Disabled, Passive, or Active states. For more information about these states, see *LACP* on page 206.

The following sections describe link redundancy behavior when the:

- Configuration and status of LACP changes during link failure and acquisition.
- Configuration of the endpoints of the member links is different.
- Configuration is LAG to non-LAG in an RSTP network.

Link Failure and Acquisition

Link failure on the local system occurs when the active link is no longer active. Failures can be characterized as physical link failure or virtual link failure.

Each type of link failure has different requirements for detection, failover, and link acquisition. In all cases, you configure the link to fail over when it fails by issuing the **redundant-port** command. Optionally, you can force the failover automatically by issuing the **redundant-port force-failover** command.

Protecting Against Physical Link Failure

Physical link failures can occur when a cable is cut.

To protect against physical link failure, issue the **transmitter** keyword with the **redundant-port** command to enable or disable the local redundant link. When the redundant link needs to be down, the link behavior in failure detection and failover follows a similar port redundancy scheme available with line modules such as the GE-2 line module.

When the transmitter on the remote end is enabled on the redundant link before it fails over, the local system considers the redundant link to be viable and enables the transmitter if it is disabled. If the remote end is disabled, the local end must enable the transmitter and wait for the remote end to enable.

Protecting Against Virtual Link Failure

A virtual link failure can occur when the active link is no longer used by the network because of topology changes caused by physical failure in the network. Topology changes can occur when, for example, a link is blocked because of network protocols such as RSTP blocking the port leading to selection of the redundant port connected to the receiver.

To protect against virtual link failure in conjunction with network protocols, use the **packet-sampling** keyword with the **redundant-port** command to detect link the viability. For example, when there is a network protocol decision that changes the topology and blocks a link to compensate for failures in the network, the system monitors the traffic to detect the change in network topology and fails over to the redundant port if necessary. It also determines whether the failover is successful. For more information, see *Member Link with Non-LAG Partner* on page 222.

Reverting After a Failover

When you specify the **auto-revert** keyword with the **redundant-port** command, the redundant link reverts back to redundant mode when the failed link becomes active again.

The system uses the following process when you issue the **auto-revert on** and **auto-revert off** keywords:

auto-revert on

1. An active link fails and a redundant link becomes active.
2. The original active link becomes active.
3. The original redundant link fails over to the original active link.
4. The redundant link can fail over to any other active link again.

auto-revert off

1. An active link fails and a redundant link becomes active.
2. The original active link becomes active.
3. The original redundant link remains the active link.
4. You can force the link to fail over by issuing the **redundant-port force-failover** command.

LACP Configuration and Member Link Behavior

By default, when a redundant member link is configured, the system disables LACP and the transmitter on that link.

When a member link is administratively down, the link state is operationally down at the local and remote ends, which means it does not transmit or receive PDUs.

The active link does not fail over when:

- An active link goes down and you set the redundant member link to administratively down.
- An active link is set to administratively down.

LACP configurations affect member link behavior based on the local or remote endpoint. For a remote end to include a member link in link aggregation, the two member links that are connected must have LACP configured.

Table 23 lists the acceptable configurations that enable redundant behavior for LACP modes at local and remote endpoints.

Table 23: Behavior of Member Links Using Local and Remote LACP Modes

		Remote LACP Mode		
		Disabled	**Passive**	**Active**
Local LACP Mode	Disabled	✔	✔	–
	Passive	✔	✔	✔
	Active	–	✔	✔

Member Link with Non-LAG Partner

When a member link has a non-LAG partner, there are two separate links in a 1:1 configuration. To successfully configure this, you must disable LACP.

When a failover occurs and LACP is active, the partner might receive a new LAG ID and the LACP PDUs receive a new MAC address; therefore, the member links are not aggregated or the bundle is disabled, terminating the sessions above it.

The partner that is connected to the redundant link must not be forwarding network traffic; that is, it is either blocked through a protocol such as RSTP, or MAC address learning has selected the active port. The redundant link must not transmit over the redundant link to that MAC. The behavior of the redundant link depends on the failure detection method that is controlled by the network protocol that is blocking the port.

Ethernet Link Redundancy and RSTP

In a LAG to non-LAG configuration, you can configure redundancy capabilities when redundant ports are connected to a bridged network that has RSTP controlling the topology.

On external devices, we recommend that you configure RSTP-enabled bridged ports that are connected to the LAG interfaces as edge ports to enable the ports to transition quickly to forwarding state upon reconfiguration, and to avoid the listening and learning states required by the spanning tree protocol. The edge port designation instructs the local bridge that bridge loops do not exist through the interface, enabling it to skip the listening and learning states.

Figure 29: Dual-Homed Heterogeneous Configuration in an RSTP Network

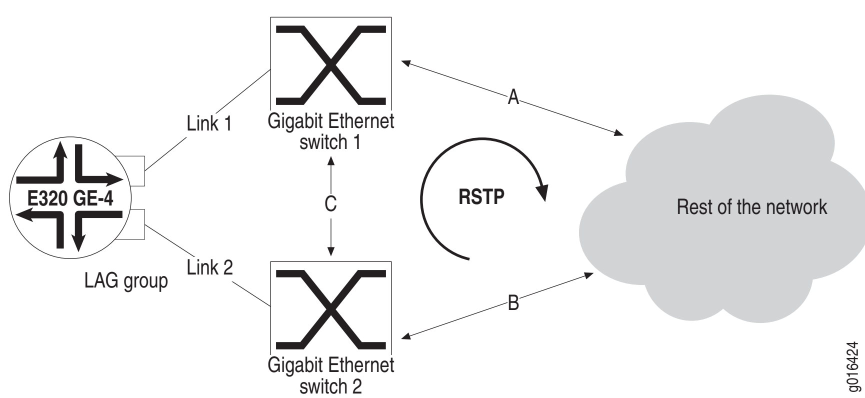


Figure 29 displays a network with RSTP enabled on Gigabit Ethernet switches 1 and 2. The local port receives bridge PDUs (BPDU), Ethernet broadcasts, and flooded unicast packets. If Link 1 is initially active and Link 2 is the backup, initial traffic destined for the LAG can be Ethernet broadcasts, PPPoE PDUs, or flooded Ethernet unicasts. The responses are only sent on the active link; in this case, Link 1.

The Ethernet network topology that is managed by RSTP learns that the MAC for the LAG group is through Link 1. Broadcasts and flooded packets are still sent on Link 2. If Link 1 is no longer viable, but has not suffered a physical failure, then that address ages out of the bridge databases and any packets directed to the LAG are flooded. The LAG detects traffic on Link 2 after the minimum delay time and then fails over.

Acquiring Initial Links

In an RSTP network, the system uses the following process for acquiring new links:

1. Based on the configuration, the system selects a link as active and the other as redundant.

2. The spanning tree converges on a topology.

3. When convergence occurs and the status of the spanning tree ports change to forwarding, network traffic appears on the links.

4. The local port detects the traffic and confirms the active member as active and the other as the redundant port. Because the initial traffic is broadcast or flooded, both ports receive the packets. However, because of the timing difference, the selected active port remains active.

Detecting Failures

In an RSTP network, the system uses the following process for detecting when the link has switched over due to topology changes:

1. BPDUs are ignored on the redundant port and system time is not retrieved. Because MAC learning forces non-flooded unicast packets to the active link, traffic to the redundant link does not receive non-flooded packets. The most recent system time is always retrieved when a network packet is received.

2. When the network cannot reach the active link because of topology changes, traffic appears on the redundant link. The redundant port detects the traffic and captures the latest timestamp. When the difference between the timestamp of the first non-bridged PDU and the time the last packet that was received on the active port is sufficiently large to account for the minimum spanning tree convergence time and latency for flooded and broadcast packets, then the port fails over.

Failing Over

In an RSTP network, the system uses the following process to fail over:

1. When the link has failed over, the system monitors the previously active port.

2. When a network packet is received on the redundant port, the system retrieves the timestamp. If the difference in timestamps between that one and the most recent on the current active port is more than the configured failover delay time, then the link fails over. If the difference is less than the delay time, the system ignores it but counts the event. If many of these transitions occur in a time period, then the system administratively brings the ports down. If no network traffic is received on either port, then failover does not occur.

Configuring Ethernet Link Redundancy

To configure Ethernet link redundancy:

1. Specify the Fast Ethernet or Gigabit Ethernet interface on which to configure a redundant link.

   host1(config)#**interface gigabitEthernet 1/1**

2. For LAG to non-LAG configurations only, specify that LACP is disabled on the port.

   host1(config-if)#**no lacp**

3. Configure a backup interface and disable LACP on it.

   host1(config)#**interface gigabitEthernet 1/0**
   host1(config-if)#**no lacp**

4. Configure a LAG interface and assign a member link to the backup interface.

   host1(config)#**interface lag myBundle**
   host1(config-if)#**member-interface gigabitEthernet 1/0**

5. Do one of the following:

   - Configure link redundancy on the port you specified in step 1.

     host1(config-if)#**redundant-port gigabitEthernet 1/1**

   - Force the port you specified in step 1 to fail over.

     host1(config-if)#**redundant-port gigabitEthernet 1/1 force-failover**

redundant-port

- Use to specify a member link in a LAG bundle as redundant.
- Use the **failover timeout** keyword to configure the amount of time between the current link event leading to failover or reversion and the previous link failover or reversion.
- Use the **packet-sampling** keyword to configure redundancy on a LAG to non-LAG application where packet sampling is used for failover detection. Use the optional **delay** keyword to control the minimum time difference to force packets on the active and redundant port to fail over.
- Use the **transmitter** keyword to enable or disable the transmitter when in redundant mode.
- Use the **auto-revert** keyword to instruct the redundant link to revert back to redundant mode when the failed link becomes active again.
- Example 1—Specifies that the Gigabit Ethernet interface in slot 4, port 0 is a redundant member interface

  host1(config-if)#**redundant-port gigabitEthernet 4/0**

- Example 2—Specifies that the Gigabit Ethernet interface in slot 1, port 1 is a redundant member interface with a packet sampling delay of 500 ms

  host1(config-if)#**redundant-port gigabitEthernet 1/1 packet-sampling delay 500**

- Use the **no** version to disable the redundant status of the member interface or disable the specified redundancy setting for the member.

redundant-port force-failover

- Use to force the specified member interface to fail over when more than one active member exists.
- Example

  host1(config)#**redundant-port gigabitEthernet 4/0 force-failover**

- There is no **no** version.

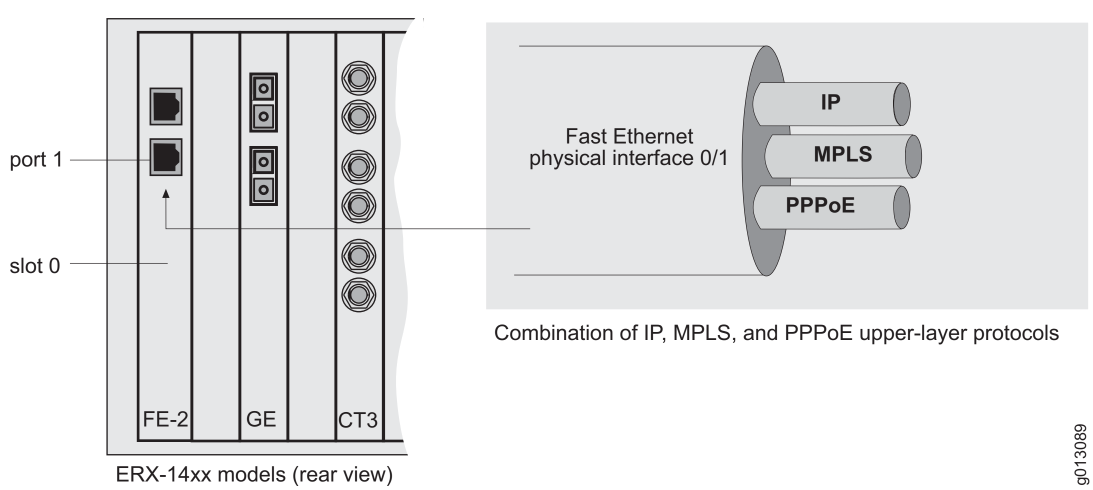
Configuring Higher-Level Protocols over Ethernet

You can configure one or more protocols over Ethernet with or without VLANs. This section focuses on non-VLAN configurations only. You can configure the following higher-level protocols on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces:

- IP
- Point-to-Point Protocol over Ethernet (PPPoE)
- Multiprotocol Label Switching (MPLS)

The Ethernet configuration examples in this section use combinations of these protocols. Figure 30 on page 225 illustrates how different protocols can be multiplexed over a single physical link without the use of VLANs.

Figure 30: Multiplexing Multiple Protocols over a Single Physical Link



The following sections describe how to create the following common non-VLAN configurations, which you can configure on Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet interfaces:

- IP over Ethernet
- PPPoE over Ethernet
- IP over Ethernet and MPLS over Ethernet
- IP over Ethernet, MPLS over Ethernet, and PPPoE over Ethernet

Configuring IP over Ethernet

To configure IP over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

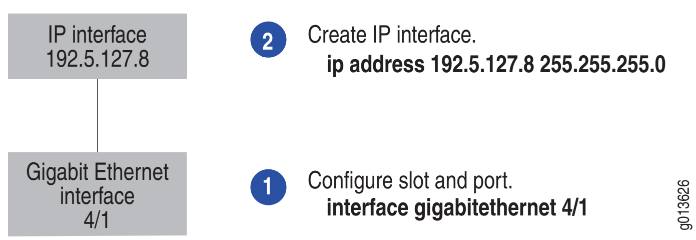
   host1(config)#**interface fastEthernet 4/1**

2. Create an IP interface.

   host1(config-if)#**ip address 192.5.127.8 255.255.255.0**

Figure 31 illustrates this configuration.

Figure 31: Example of IP over Ethernet Stacking Configuration Steps



Configuring PPPoE over Ethernet

To configure PPPoE over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/1**

2. Specify PPPoE as the encapsulation method on the interface.

   host1(config-if)#**pppoe**

3. Create a PPPoE subinterface.

   host1(config-if)#**pppoe subinterface fastEthernet 4/1.1**

4. Specify PPP as the encapsulation method on the interface.

   host1(config-if)#**encapsulation ppp**

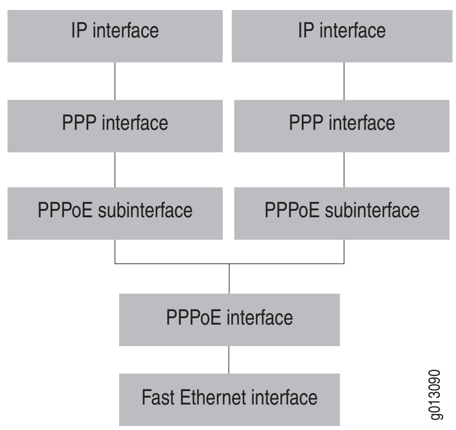
5. Assign an IP address and mask.

   host1(config-if)#**ip address 164.10.6.51 255.255.255.0**

6. (Optional) Configure additional PPPoE subinterfaces by completing Steps 3 through 5 using unique numbering.

Figure 32 illustrates this configuration.

Figure 32: Example of PPPoE Stacking Configuration Steps



Configuring IP and MPLS over Ethernet

To configure both IP and MPLS over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/0**

2. Create an IP interface.

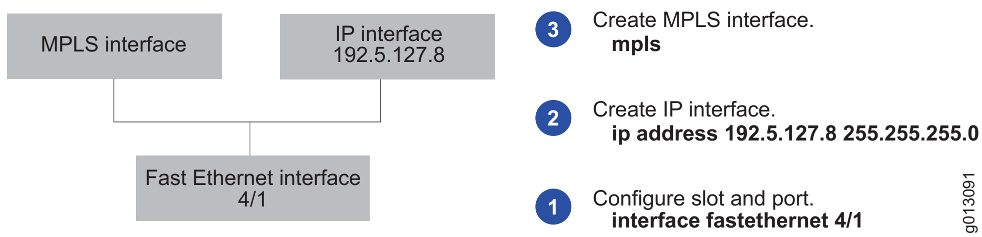
   host1(config-if)#**ip address 192.5.127.8 255.255.255.0**

3. Create an MPLS interface.

   host1(config-if)#**mpls**

Figure 33 illustrates this configuration.

Figure 33: Example of IP and MPLS Stacking Configuration Steps



Configuring IP, MPLS, and PPPoE over Ethernet

To configure IP, MPLS, and PPPoE over an Ethernet interface:

1. Specify a Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet port.

   host1(config)#**interface fastEthernet 4/0**

2. Create an IP interface.

   host1(config-if)#**ip address 192.5.127.8 255.255.255.0**

3. Create an MPLS interface.

   host1(config-if)#**mpls**

4. Create a PPPoE interface by specifying PPPoE as the encapsulation method on the interface.

   host1(config-if)#**pppoe**

5. Create a PPPoE subinterface.

   host1(config-if)#**pppoe subinterface fastEthernet 4/1.1**

6. Specify PPP as the encapsulation method on the interface.

   host1(config-if)#**encapsulation ppp**

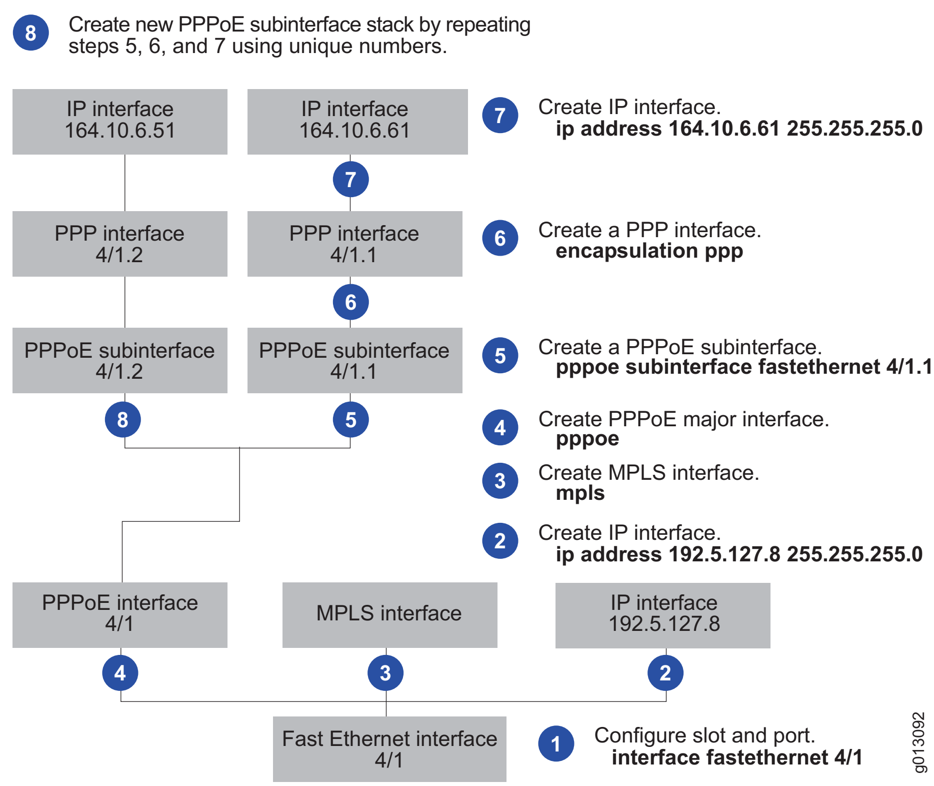
7. Assign an IP address and mask.

   host1(config-if)#**ip address 192.6.129.5 255.255.255.0**

8. (Optional) Configure additional PPPoE subinterfaces by completing Steps 5 through 7 using unique numbering.

Figure 34 illustrates this configuration.

Figure 34: Example of IP, MPLS, and PPPoE Stacking Configuration Steps



mpls

- Use to enable, disable, or delete MPLS on an interface. MPLS is disabled by default.
- Example

  host1(config)#**mpls**

- Use the **no** version to halt MPLS on the interface and delete the MPLS interface configuration.

Ethernet Link Aggregation and MPLS

CE-side load balancing in a Martini layer 2 transport environment enables an E-series router to interoperate with an 802.3ad switch in a topology designed for Ethernet link aggregation. See *JUNOSe BGP and MPLS Configuration Guide, Chapter 4, Configuring Layer 2 Services over MPLS* for more information.

Disabling Ethernet Interfaces

Use the **shutdown** command to disable an Ethernet interface.

shutdown

- Use to disable an Ethernet interface.
- Example

  host1(config-if)#**shutdown**
- Use the **no** version to restart a disabled Ethernet interface.

Monitoring Ethernet Interfaces

This section explains how to set a statistics baseline, display bit rate and packet rate statistics for VLAN subinterfaces, and use the **show** commands to display the physical characteristics and the configured settings for Ethernet interfaces.

NOTE: The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

Setting Statistics Baselines

The router stores statistics in counters that reset only when you reboot. However, you can establish a baseline for Ethernet statistics by setting a group of reference counters to zero.

baseline interface fastEthernet | gigabitEthernet | tenGigabitEthernet

- Use to establish a baseline for Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet statistics on a line module or an SRP module.
- Use the **delta** keyword with the **show interfaces fastEthernet**, the **show interfaces gigabitEthernet**, or the **show interfaces tenGigabitEthernet** command to display baselined statistics.

Displaying Interface Rate Statistics for VLAN Subinterfaces

You can use the **monitor vlan interface** command to display bit rate and packet rate statistics over a specified time interval for one or more VLAN subinterfaces configured on the router.

To display interface rate statistics for VLAN subinterfaces:

1. Log in to the router by using a local console session or a virtual terminal (vty) session (such as a Telnet session).

   While you are using the **monitor vlan interface** command, you must keep the console or terminal session open and you cannot issue any other commands at the session during this time.

   For information about logging in to the router, see *Accessing the CLI* in *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*.

2. Access User Exec mode or Privileged Exec mode.

   For information, see *Accessing Command Modes* in *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*.

3. Specify the interface identifier for each VLAN subinterface that you want to monitor.

   host1#**monitor vlan interface fastEthernet 0/0.1 fastEthernet 4/0.1 display-time-of-day**

   For information about specifying interface identifiers for VLAN subinterfaces configured over Ethernet interfaces, see *Configuring VLANs* on page 187. For information about specifying interface identifiers for VLAN subinterfaces configured over LAG bundles, see *Configuring a VLAN Subinterface for a LAG Bundle* on page 208.

   By default, the router uses a 5-second time interval between polls to calculate bit rates and packet rates for each specified VLAN subinterface. Optionally, you can use the **load-interval** keyword to specify a nondefault time interval in the range 5–30 seconds.

   You can also include the optional **display-time-of-day** keyword to show the time of day at which the router gathers statistics for each interval. Displaying the time of day enables you to monitor when a particular VLAN subinterface is underutilized or overutilized.

4. Review the command output.

```
host1#monitor vlan interface fastEthernet 0/0.1 fastEthernet 4/0.1
display-time-of-day
                       Seconds
                       between                                       Time
       Interface        polls    Input bps/pps   Output bps/pps   (UTC)
----------------------- -------- --------------- --------------- --------
FastEthernet 0/0.1             0           --/--           --/-- 10:50:07
FastEthernet 4/0.1             0           --/--           --/-- 10:50:07
FastEthernet 0/0.1             5      120240/100      120240/100 10:50:12
FastEthernet 4/0.1             5      120000/100      120000/100 10:50:12
FastEthernet 0/0.1             5      120240/100      120240/100 10:50:17
FastEthernet 4/0.1             5      120000/100      120000/100 10:50:17
```

The router polls each VLAN subinterface at the specified load interval (the default 5-second interval in this example) to calculate and display bit rate and packet rate statistics. The first line of output for each interface always displays 0 (zero) for the number of seconds between polls, and dashes (--/--) in the Input bps/pps and Output bps/pps columns. These values indicate that the router initially takes a baseline for each interface against which to measure subsequent statistics. The router continues to display subsequent lines of output for each interface at the specified load interval until you press Ctrl+c to stop the command.

For a description of each field in the **monitor vlan interface** command output, see **monitor vlan interface** on page 232.

5. When you are finished, press Ctrl+c to stop the **monitor vlan interface** command.

   host1#**^C**

monitor vlan interface

- Use to display bit rate and packet rate statistics over a specified time interval for one or more VLAN subinterfaces.
- You must use the **monitor vlan interface** command in a dedicated console or terminal session for the duration of the monitoring session.
- Specify the interface identifier for each VLAN subinterface that you want to monitor.
- To specify a nondefault time interval in the range 5–30 seconds at which the router calculates bit rate and packet rate statistics, use the optional **load-interval** keyword. The default time interval is 5 seconds.
- To display the time at which the router calculates bit rate and packet rate statistics for the current interval, use the optional **display-time-of-day** keyword.
- To stop the **monitor vlan interface** command, press Ctrl+c.
- Field descriptions
  - Interface—Interface identifier for the Ethernet or LAG interface on which the VLAN subinterface resides
  - Seconds between polls—Number of seconds at which the router calculates bit rate and packet rate statistics
  - Input bps/pps—Number of bits per second (bps) and packets per second (pps) received on this interface during the specified load interval
  - Output bps/pps—Number of bits per second (bps) and packets per second (pps) transmitted on this interface during the specified load interval
  - Time—Time of day, in hh:mm:ss format, at which the router calculates the bit rate and packet rate statistics for the current interval

- Example 1—Displays bit rate and packet rate statistics over the default (5-second) load interval for a single VLAN subinterface

```
host1#monitor vlan interface fastEthernet 0/0.1
                         Seconds
                         between
       Interface          polls    Input bps/pps   Output bps/pps
----------------------- -------- --------------- ---------------
FastEthernet 0/0.1             0           --/--           --/--
FastEthernet 0/0.1             5      120240/100      120240/100
FastEthernet 0/0.1             5      120000/100      120000/100
FastEthernet 0/0.1             5        92400/77        92400/77
FastEthernet 0/0.1             5        88800/74        88800/74
FastEthernet 0/0.1             5      120000/100      120000/100
host1#^C
```

- Example 2—Displays bit rate and packet rate statistics over a 10-second load interval for two VLAN subinterfaces, with the time of day that the statistics were calculated

```
host1#monitor vlan interface fastEthernet 0/0.1 fastEthernet 4/0.1
load-interval 10 display-time-of-day
                         Seconds
                         between                                     Time
       Interface          polls    Input bps/pps   Output bps/pps   (UTC)
----------------------- -------- --------------- --------------- --------
FastEthernet 0/0.1             0           --/--           --/-- 10:50:33
FastEthernet 4/0.1             0           --/--           --/-- 10:50:33
FastEthernet 0/0.1            10      120120/100      120120/100 10:50:43
FastEthernet 4/0.1            10      120000/100      120000/100 10:50:43
FastEthernet 0/0.1            10      120000/100      120000/100 10:50:53
FastEthernet 4/0.1            10      120000/100      120000/100 10:50:53
host1#^C
```

- There is no **no** version.

Using Ethernet show Commands

Use the **show** commands described in this section to display information about your Ethernet configuration and to monitor Ethernet interfaces.

show interfaces fastEthernet

- Use to display the status of Fast Ethernet interfaces, VLAN subinterfaces, or S-VLAN subinterfaces.
- You can specify the following keywords:
  - **delta**—Specifies that baselined statistics are to be shown
  - **brief**—Displays the operational status of all configured interfaces
- Field descriptions
  - FastEthernet *interfaceSpecifier*—Status of the hardware on this interface
    - up—Hardware is operational
    - down—Hardware is not operational

- Administrative status—Operational state that you configured for this interface
  - up—Interface is enabled
  - down—Interface is disabled
- Hardware—Type of MAC device on this interface
- Address—MAC address of the processor on this interface
- MAU—Type of medium attachment unit (MAU) on the physical port:
  - 10BASE-T (10 Mbps)
  - 100BASE-TX (100 Mbps)
  - 100BASE-FX-MM (100 Mbps) with the distance appearing after the type
  - 100BASE-LX-SM (100 Mbps)
  - SFP (Empty)—SFPs that are empty
  - SFP (Non-compliant Juniper Part)—SFPs that are installed in the FE-8 I/O module and do not have a Juniper Networks part number programmed
- MTU—Size of the MTU for this interface
  - Operational—Size of the largest packet processed
  - Administrative—Setting for MTU size that you specified
- Duplex Mode—Duplex option for this interface
  - Operational—Duplex option currently used
  - Administrative—Setting for duplex that you specified
- Speed—Line speed for this interface
  - Operational—Current rate at which packets are processed
  - Administrative—Setting for line speed
  - 5 minute input rate—Data rates based on traffic received in the last 5 minutes
  - 5 minute output rate—Data rates based on traffic sent in the last 5 minutes
- In—Analysis of inbound traffic on this interface
  - Bytes—Number of bytes received in error-free packets
  - Unicast—Number of unicast packets received
  - Multicast—Number of multicast packets received
  - Broadcast—Number of broadcast packets received
  - Errors—Total number of errors in all received packets; some packets might contain more than one error
  - Discards—Total number of discarded incoming packets
  - Mac Errors—Number of incoming packets discarded because of MAC sublayer failures
  - Alignment—Number of incomplete octets received

  - CRC—Number of packets discarded because the checksum the router computed from the data does not match the checksum generated by the originating devices
  - Too Longs—Number of packets discarded because the size exceeded the MTU
  - Symbol Errors—Number of symbols received that the router did not correctly decode
- Out—Analysis of outbound traffic on this interface
  - Bytes—Number of bytes sent
  - Unicast—Number of unicast packets sent
  - Multicast—Number of multicast packets sent
  - Broadcast—Number of broadcast packets sent
  - Errors—Total number of errors in all transmitted packets; some packets might contain more than one error
  - Discards—Total number of discarded outgoing packets
  - Mac Errors—Number of outgoing packets discarded because of MAC sublayer failures
  - Deferred—Number of packets that the router delayed sending because the line was busy. In half duplex mode, a high number of deferrals means the link is very busy with traffic from other stations. In full duplex mode, when the link is always available for transmission, this number is zero.
  - No Carrier—Number of packets sent when carrier sense was unavailable
- Collisions—Analysis of the collisions that occurred
  - Single—Number of packets sent after one collision
  - Multiple—Number of packets sent after multiple collisions
  - Late—Number of packets aborted during sending because of collisions after 64 bytes
  - Excessive—Number of packets not sent because of too many collisions
- ARP Statistics—Analysis of ARP traffic on this interface; In fields are for traffic received on the interface and Out fields are for traffic sent on the interface
  - ARP requests—Number of ARP requests
  - ARP responses—Number of ARP responses
  - Errors—Total number of errors in all ARP packets
  - Discards—Total number of discarded ARP packets
- queue—Hardware packet queue associated with the specified traffic class and interface
  - Queue length—Length of the queue, in bytes
  - Forwarded packets, bytes—Number of packets and bytes that were forwarded on this queue

    - Dropped committed packets, bytes—Number of committed packets and bytes that were dropped
    - Dropped conformed packets, bytes—Number of conformed packets and bytes that were dropped
    - Dropped exceeded packets, bytes—Number of exceeded packets and bytes that were dropped

- Field descriptions when you display the status of a Fast Ethernet VLAN or S-VLAN subinterface
  - *Subinterface number*—Location of the subinterface that carries the VLAN or S-VLAN traffic
  - Administrative status—Operational state that you configured for this interface; up or down
  - VLAN ID—Domain number of the VLAN
  - SVLAN ID—Domain number of the stacked VLAN
  - Ethertype—Ethertype assignment for the S-VLAN subinterface, 0x8100, 0x88a8, or 0x9100; 0x9100 is the default
  - In—Analysis of inbound traffic on this interface
    - Bytes—Number of bytes received on the VLAN or S-VLAN subinterface
    - Packets—Sum of all unicast, broadcast, and multicast packets received on the VLAN or S-VLAN subinterface
    - Multicast—Number of multicast packets received on the VLAN or S-VLAN subinterface
    - Broadcast—Number of broadcast packets received on the VLAN or S-VLAN subinterface
    - Errors—Total number of errors in all received packets; some packets might contain more than one error
    - Discards—Total number of discarded incoming packets
  - Out—Analysis of outbound traffic on this interface
    - Bytes—Number of bytes sent on the VLAN or S-VLAN subinterface
    - Packets—Number of packets sent on the VLAN or S-VLAN subinterface
    - Multicast—Number of multicast packets sent on the VLAN or S-VLAN subinterface
    - Broadcast—Number of broadcast packets sent on the VLAN or S-VLAN subinterface
    - Errors—Total number of errors in all transmitted packets; note that some packets might contain more than one error
    - Discards—Total number of discarded outgoing packets

- Example 1—Displays the status of a Fast Ethernet interface

```
host1:vr2#show interfaces fastEthernet 2/0
FastEthernet2/0 is Up, Administrative status is Up
  Hardware is Intel 21440, address is 0090.1a10.0552
  MAU is 10BASE-T
  MTU: Operational 1518, Administrative 1518
  Duplex Mode: Operational Full Duplex, Administrative Auto Negotiate
  Speed: Operational 100 Mbps, Administrative Auto Negotiate

  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

  In: Bytes 39256, Unicast 612
   Multicast 0, Broadcast 0
   Errors 0, Discards 0, Mac Errors 0, Alignment 0
   CRC 0, Too Longs 0, Symbol Errors 0
  Out: Bytes 4579036, Unicast 610
   Multicast 0, Broadcast 70932
   Errors 0, Discards 0, Mac Errors 0, Deferred 0, No Carrier 3
   Collisions: Single 0, Multiple 0, Late 0, Excessive 0
 ARP Statistics:
  In: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
Administrative qos-shaping-mode: none
Operational qos-shaping-mode: none

queue 0: traffic class control, bound to FastEthernet2/0
  Queue length 0 bytes
  Forwarded packets 1, bytes 46
  Dropped committed packets 0, bytes 0
  Dropped conformed packets 0, bytes 0
  Dropped exceeded packets 0, bytes 0
```

- Example 2—Displays the status of a Fast Ethernet VLAN subinterface

```
host1:vr2#show interfaces fastEthernet 8/3.1
FastEthernet8/3.1 is Up, Administrative status is Up
  VLAN ID: 10, address 0090.5e00.0001

In: Bytes 39256, Packets 612
   Multicast 0, Broadcast 0
   Errors 0, Discards 0
Out: Bytes 4536220, Packets 70873
   Multicast 0, Broadcast 70258
   Errors 0, Discards 0
ARP Statistics:
  In: ARP requests 1, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 1, ARP responses 0
   Errors 0, Discards 0
```

- Example 3—Displays the status of a Fast Ethernet S-VLAN subinterface

```
host1:vr2#show interfaces fastEthernet 0/0.1
FastEthernet0/0.1 is Up, Administrative status is Up
  SVLAN ID: 1, VLAN ID: 0, Ethertype 0x9100

  In: Bytes 39256, Packets 612
   Multicast 0, Broadcast 0
   Errors 0, Discards 0
  Out: Bytes 4536220, Packets 70873
   Multicast 0, Broadcast 70258
   Errors 0, Discards 0
ARP Statistics:
  In: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
```

show interfaces gigabitEthernet
show interfaces tenGigabitEthernet

- Use to display the status of Gigabit Ethernet interfaces, 10-Gigabit Ethernet interfaces, VLAN subinterfaces, or S-VLAN subinterfaces.
- You can specify the following keywords:
  - **delta**—Specifies that baselined statistics are to be shown
  - **brief**—Displays the operational status of all configured interfaces
- Field descriptions
  - GigabitEthernet or tenGigabitEthernet *interfaceSpecifier*—Status of the hardware on this interface
    - up—Hardware is operational
    - down—Hardware is not operational
  - Administrative status—Operational state that you configured for this interface
    - up—Interface is enabled
    - down—Interface is disabled
  - Hardware—Type of MAC device on this interface
  - Address—MAC address of the processor on this interface
  - MAU—Type of medium attachment unit (MAU) on the primary and secondary physical ports:
    - SFP—1000BASE-LH, 1000BASE-SX, 1000BASE-ZX; for SFPs that are empty, SFP (Empty) appears in this field; for SFPs that are installed in the OC3-2 GE APS I/O module and do not have a Juniper Networks part number programmed, SFP (GE Compliant) appears in this field
    - XFP—10GBASE-SR (10 Gbps), 10GBASE-LR (10 Gbps), 10GBASE-ER (10 Gbps); for XFPs that are empty, XFP (Empty) appears in this field

- MTU—Size of the MTU for this interface
  - Operational—Size of the largest packet processed
  - Administrative—Setting for MTU size that you specified
- Duplex Mode—Duplex option for this interface
  - Operational—Duplex option currently used
  - Administrative—Setting for duplex that you specified
- Speed—Line speed for this interface
  - Operational—Current rate at which packets are processed
  - Administrative—Setting for line speed that you specified
- Link —Link information for this interface
  - Operational Link Selected—Port that the I/O module is currently using: primary or secondary
  - Administrative link selected—Port that the I/O module is configured to use:
    - primary—Only primary port is configured to operate
    - secondary—Only redundant port is configured to operate
    - automatically—Software controls port redundancy automatically
- Primary link selected x times—Number of times that the I/O has used the primary port since the module was last rebooted
- Secondary link selected x times—Number of times that the I/O has used the secondary port since the module was last rebooted
- Primary/Secondary link signal detected, Primary/Secondary link signal not detected—Specifies the port (primary or secondary) on which the router detects a signal
- 5 minute input rate—Data rates based on the traffic received in the last 5 minutes
- 5 minute output rate—Data rates based on the traffic sent in the last 5 minutes
- In—Analysis of inbound traffic on this interface
  - Bytes—Number of bytes received in error-free packets
  - Unicast—Number of unicast packets received
  - Multicast—Number of multicast packets received
  - Broadcast—Number of broadcast packets received
  - Errors—Total number of errors in all received packets; some packets might contain more than one error
  - Discards—Total number of discarded incoming packets
  - Mac Errors—Number of incoming packets discarded because of MAC sublayer failures
  - Alignment—Number of incomplete octets received

  - CRC—Number of packets discarded because the checksum that the router computed from the data does not match the checksum generated by the originating devices
  - Too Longs—Number of packets discarded because the size exceeded the MTU
  - Symbol Errors—Number of symbols received that the router did not correctly decode
- Out—Analysis of outbound traffic on this interface
  - Bytes—Number of bytes sent
  - Unicast—Number of unicast packets sent
  - Multicast—Number of multicast packets sent
  - Broadcast—Number of broadcast packets sent
  - Errors—Total number of errors in all transmitted packets; note that some packets might contain more than one error
  - Discards—Total number of discarded outgoing packets
  - Mac Errors—Number of outgoing packets discarded because of MAC sublayer failures
  - Deferred—Number of packets that the router delayed sending because the line was busy. In half duplex mode, a high number of deferrals means the link is very busy with traffic from other stations. In full duplex mode, when the link is always available for transmission, this number is zero.
  - No Carrier—Number of packets sent when carrier sense was unavailable
- Collisions—Analysis of the collisions that occurred
  - Single—Number of packets sent after one collision
  - Multiple—Number of packets sent after multiple collisions
  - Late—Number of packets aborted during sending because of collisions after 64 bytes
  - Excessive—Number of packets not sent because of too many collisions
- ARP Statistics—Analysis of ARP traffic on this interface; In fields are for traffic received on the interface and Out fields are for traffic sent on the interface
  - ARP requests—Number of ARP requests
  - ARP responses—Number of ARP responses
  - Errors—Total number of errors in all ARP packets
  - Discards—Total number of discarded ARP packets
- queue—Hardware packet queue associated with the specified traffic class and interface
  - Queue length—Length of the queue, in bytes
  - Forwarded packets, bytes—Number of packets and bytes that were forwarded on this queue

    - Dropped committed packets, bytes—Number of committed packets and bytes that were dropped
    - Dropped conformed packets, bytes—Number of conformed packets and bytes that were dropped
    - Dropped exceeded packets, bytes—Number of exceeded packets and bytes that were dropped

- Field descriptions when you display the status of a Gigabit Ethernet or 10-Gigabit Ethernet VLAN or S-VLAN subinterface
  - *Subinterface number*—Location of the subinterface that carries the VLAN or S-VLAN traffic
  - Administrative status—Operational state that you configured for this interface; up or down
  - VLAN ID—Domain number of the VLAN
  - SVLAN ID—Domain number of the stacked VLAN
  - Ethertype—Ethertype assignment for the S-VLAN subinterface, 0x8100, 0x88a8, or 0x9100; 0x9100 is the default
  - In—Analysis of inbound traffic on this interface
    - Bytes—Number of bytes received on the VLAN or S-VLAN subinterface
    - Packets—Sum of all unicast, broadcast, and multicast packets received on the VLAN or S-VLAN subinterface
    - Multicast—Number of multicast packets received on the VLAN or S-VLAN subinterface
    - Broadcast—Number of broadcast packets received on the VLAN or S-VLAN subinterface
    - Errors—Total number of errors in all received packets; some packets might contain more than one error
    - Discards—Total number of discarded incoming packets
  - Out—Analysis of outbound traffic on this interface
    - Bytes—Number of bytes sent on the VLAN or S-VLAN subinterface
    - Packets—Number of packets sent on the VLAN or S-VLAN subinterface
    - Multicast—Number of multicast packets sent on the VLAN or S-VLAN subinterface
    - Broadcast—Number of broadcast packets sent on the VLAN or S-VLAN subinterface
    - Errors—Total number of errors in all transmitted packets; some packets might contain more than one error
    - Discards—Total number of discarded outgoing packets
- Example 1—Displays the status of a Gigabit Ethernet interface

```
host1:vr2#show interfaces gigabitEthernet 10/2
ERX-40-20-43#show int gigabitEthernet 10/2
GigabitEthernet10/2 is Down, Administrative status is Up
  Hardware is SEEQ 8101, address is 0090.1a01.0cc8
  Primary MAU is 1000BASE-SX, secondary MAU is SFP (Empty)
  MTU: Operational 1518, Administrative 1518
```

```
  Duplex Mode: Operational Full Duplex, Administrative Auto Negotiate
  Speed: Operational 1000 Mbps, Administrative Auto Negotiate
  Link: Operational Secondary Link Selected,
        Administrative Link Selected Automatically
  Link Failover Timeout: Operational 652 ms, Administrative default
  Primary link selected 6302 times, Secondary link selected 6302 times
  Primary link signal detected, Secondary link signal detected

  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

  In: Bytes 0, Unicast 0
   Multicast 0, Broadcast 0
   Errors 0, Discards 0, Mac Errors 0, Alignment 0
   CRC 0, Too Longs 0, Symbol Errors 0
  Out: Bytes 0, Unicast 0
   Multicast 0, Broadcast 0
   Errors 0, Discards 0, Mac Errors 0, Deferred 0, No Carrier 0
   Collisions: Single 0, Multiple 0, Late 0, Excessive 0
 ARP Statistics:
  In: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
Administrative qos-shaping-mode: none
Operational qos-shaping-mode: none

queue 0: traffic class control, bound to GigabitEthernet10/2
  Queue length 0 bytes
  Forwarded packets 0, bytes 0
  Dropped committed packets 0, bytes 0
  Dropped conformed packets 0, bytes 0
  Dropped exceeded packets 0, bytes 0
```

- Example 2—Displays the status of a Gigabit Ethernet VLAN subinterface

```
host1:vr2#show interfaces gigabitEthernet 2/0.1
GigabitEthernet2/0.1 is Up, Administrative status is Up
  VLAN ID: 10, address 0090.5e00.0001

  In: Bytes 2357, Packets 23
   Multicast 0, Broadcast 0
   Errors 0, Discards 0
  Out: Bytes 4872, Packets 57
   Multicast 0, Broadcast 0
   Errors 0, Discards 0
ARP Statistics:
  In: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
```

- Example 3—Displays the status of a Gigabit Ethernet S-VLAN subinterface

```
host1:vr2#show interfaces gigabitEthernet 2/0.2
GigabitEthernet2/0.2 is Up, Administrative status is Up
  SVLAN ID: 10, VLAN ID: 100, Ethertype 0x9100

  In: Bytes 2357, Packets 23
   Multicast 0, Broadcast 0
   Errors 0, Discards 0
  Out: Bytes 4872, Packets 57
   Multicast 0, Broadcast 57
```

```
ARP Statistics:
  In: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
```

show interfaces lag

- Use to display information about a specified Ethernet member link in an IEEE 802.3ad link aggregation group (LAG) bundle.
- Specify either the Fast Ethernet or Gigabit Ethernet interface type when issuing this command:

  host1(config):**show interfaces *interfaceType interfaceSpecifier* lag**

- Field descriptions
  - *interfaceSpecifier*—Status of the hardware on this interface
    - Up—Hardware is operational
    - Down—Hardware is not operational
  - Administrative status—Operational state that you configured for this interface
  - Member—Membership status of the Ethernet link
  - LACP—Status of LACP configuration for the Ethernet link
    - active—Ethernet link participates in the protocol regardless of whether its Partner member link is set to active or passive LACP PDU participation
    - passive—Ethernet link transmits LACP PDUs only when it receives LACP PDUs from its Partner member link
  - mux state—Status of collecting and distributing at the Mux state machine
    - collecting/distributing—Ethernet link is actively collecting incoming frames and distributing outgoing frames
    - detached—Ethernet link is detached from the LAG bundle due to protocol changes or system constraints
    - waiting—Ethernet link is waiting to attach to a LAG bundle
  - LACP state
    - active—Actor link actively particulates in LACP
    - passive—Actor link transmits LACP PDUs
    - timeout—Timeout control value; this value is not configurable and is set to long timeout (30 seconds)
    - aggregatable—Actor link can be aggregated
    - individual—Actor link cannot be aggregated; must operate as an individual link
    - in-sync—Actor link has joined the correct LAG bundle
    - out-of-sync—Actor link is unable to join the correct LAG bundle

  - collecting—Actor link is actively collecting incoming frames; if this field does not appear, the Actor link is not actively collecting incoming frames
  - distributing—Actor link is actively distributing outgoing frames; if this field does not appear, the Actor link is not actively distributing outgoing frames
  - defaulted—Actor link is using defaulted operational information about the Partner link that was administratively configured for Partner; if this field does not appear, the operational information about the Partner link has been received by the Actor link in an LACP PDU
  - expired—Actor link's receive machine is expired; if this field does not appear, the Actor link's receive machine is active
- port—Port number assigned to the Ethernet link by the Actor link
- priority—Priority assigned to this Ethernet link by the Actor link
- Key—Operational key value assigned to the Ethernet link by the Actor link
- System Priority—Priority assigned to the Ethernet link by the system
- System MAC Address—MAC address assigned to the Actor link
- Partner—Status of the Partner link
  - active— Partner link participates in the LACP
  - passive—Partner link transmits LACP PDUs
  - timeout—Timeout control value; short timeout or long timeout
  - aggregatable—Partner link can be aggregated
  - individual—Partner link cannot be aggregated
  - in-sync—Partner link has joined the correct LAG bundle
  - out-of-sync—Partner link has joined the incorrect LAG bundle
  - collecting—Partner link is actively collecting incoming frames; if this field does not appear, the Partner link is not actively collecting incoming frames
  - distributing—Partner link is actively distributing outgoing frames; if this field does not appear, the Partner link is not actively distributing outgoing frames
  - defaulted—Partner link is using defaulted operational information about the Partner link that was administratively configured for Partner; if this field does not appear, the operational information about the Partner link has been received by the Actor link in an LACP PDU
  - expired—Partner link's receive machine is expired; if this field does not appear, the Partner link's receive machine is active
  - port—Port number assigned to the Ethernet link by the Partner link
  - priority—Priority assigned to the Ethernet link by the Partner link
  - key—Operational key value assigned to the Ethernet link by the Partner link
  - age—Number of seconds since last LACP was received

        - System Priority—Priority assigned to the Ethernet link by the Partner link's system
        - System MAC Address—MAC address assigned to the Partner link by the system
    - LACP packets—Number of transmitted and received LACP packets
    - Marker Protocol request packets—Number of Marker Protocol packets requested to verify transmissions
    - Marker Protocol response packets—Number of Marker Protocol response packets that verified transmissions
    - Discarded—Number of invalid LACP packets
- Example

```
host1#show interfaces fastEthernet 4/0 lag
FastEthernet4/0 is Up, Administrative status is Up
 Member of Lag boston
 LACP passive, mux state collecting/distributing
 LACP state (0x3c) passive, long timeout, aggregatable, in-sync, collecting,
distributing
 port 0 priority 32768 key 8
 System Priority 32768 System MAC Address is 0090.1a40.2043
 Partner: state (0x3d) active, short timeout, aggregatable, in-sync,
collecting, distributing
  port 0 priority 32768 key 8 age 25
  System Priority 32768 System MAC Address is 0090.1a40.2043

 LACP packets: received 8, transmitted 7
 Marker Protocol request packets: received 0, transmitted 0
 Marker Protocol response packets: received 0, transmitted 0
 Discarded 0, unknown protocol received 0
```

show interfaces lag members

- Use to display information about the Ethernet member links in all IEEE 802.3ad link aggregation group (LAG) bundles configured on the router, or about the member links in a specified IEEE 802.3ad LAG bundle.
- Field descriptions
    - Lag—Name of the LAG bundle
    - Administrative status—Operational state that you configured for the LAG
    - Member-interface—Status of the member interface in the bundle
        - *Interface Specifier*—Status of the hardware on this interface (up or down)
        - LACP active—Ethernet link participates in the protocol regardless of whether its Partner member link is set to active or passive LACP PDU participation
        - LACP passive—Ethernet link transmits LACP PDUs only when it receives LACP PDUs from its Partner link

- collecting/distributing—Ethernet link is actively collecting incoming frames and distributing outgoing frames
- detached—Ethernet link is detached from the LAG bundle due to protocol changes or system constraints
- waiting—Ethernet link is waiting to attach to a LAG bundle

- Example

```
host1#show interfaces boston lag members

Lag bostonBundle is Up, Administrative status is Up
   Member-interface FastEthernet0/0 is Up
      (LACP active, state collecting/distributing)
   Member-interface FastEthernet0/5 is Up
      (LACP active, state collecting/distributing)

Lag actonBundle is Up, Administrative status is Up
   Member-interface FastEthernet4/0 is Up
      (LACP passive, state collecting/distributing)
   Member-interface FastEthernet4/6 is Up
      (LACP passive, state collecting/distributing)
2 lag interfaces found
```

show ip mac-validate interface

- Use to display the status of the MAC address validation on the physical interface.
- Field descriptions
  - FastEthernet *interfaceSpecifier*—On the ERX-14xx models, ERX-7xx models, and ERX-310 router, the Fast Ethernet or Gigabit Ethernet interface *slot/port*; on the E120 and E320 routers, the Gigabit Ethernet or 10-Gigabit Ethernet interface *slot/adapter/port*
  - Keyword assigned to interface—Options: Strict or Loose
  - Address—IP address of the entry
  - Hardware Addr—Physical (MAC) address of the entry
- Example

```
host1:boston#show ip mac-validate interface fastEthernet 11/0
FastEthernet11/0:  Strict

        Address     Hardware Addr
        3.3.3.3     0090.1a30.3365
        4.4.4.4     0090.1a30.3368
```

show vlan subinterface

- Use to display configuration and status information for a specified VLAN subinterface or for all VLAN subinterfaces configured on the router.
- Use the **summary** keyword to display only the counts of all VLAN subinterfaces and VLAN major interfaces configured on the router.
- Use the **mac-address** keyword to display information about the VLAN subinterfaces that were configured with unique MAC addresses.
- Use the **vlan** or **svlan** keywords to display information about specific S-VLAN IDs or VLAN IDs.

- Field descriptions
  - Interface—Type and specifier of the VLAN subinterface
  - Status—Status of the VLAN subinterface: up, down, dormant, lowerLayerDown, absent
  - MTU—Maximum allowable size (in bytes) of the maximum transmission unit (MTU) for the VLAN subinterface
  - Svlan Id—S-VLAN ID value, if configured
  - Vlan Id—VLAN ID value for the VLAN subinterface
  - Ethertype—S-VLAN Ethertype value, if configured
  - Type—Type of VLAN subinterface
    - Static—VLAN or S-VLAN subinterface was configured statically
    - Dynamic—VLAN or S-VLAN subinterface was configured dynamically
  - In—Analysis of inbound traffic on this interface
    - Bytes—Number of bytes received on the VLAN or S-VLAN subinterface
    - Packets—Sum of all unicast, broadcast, and multicast packets received on the VLAN or S-VLAN subinterface
    - Multicast—Number of multicast packets received on the VLAN or S-VLAN subinterface
    - Broadcast—Number of broadcast packets received on the VLAN or S-VLAN subinterface
    - Errors—Total number of errors in all received packets; some packets might contain more than one error
    - Discards—Total number of discarded incoming packets
  - Out—Analysis of outbound traffic on this interface
    - Bytes—Number of bytes sent on the VLAN or S-VLAN subinterface
    - Packets—Number of packets sent on the VLAN or S-VLAN subinterface
    - Multicast—Number of multicast packets received on the VLAN or S-VLAN subinterface
    - Broadcast—Number of broadcast packets received on the VLAN or S-VLAN subinterface
    - Errors—Total number of errors in all transmitted packets; some packets might contain more than one error
    - Discards—Total number of discarded outgoing packets

- ARP Statistics—Analysis of ARP traffic on this interface; In fields are for traffic received on the interface and Out fields are for traffic sent on the interface
  - ARP requests—Number of ARP requests
  - ARP responses—Number of ARP responses
  - Errors—Total number of errors in all ARP packets
  - Discards—Total number of discarded ARP packets
- Total VLAN interfaces—Total numbers of VLAN subinterfaces and VLAN major interfaces configured on the router; this is the only field that appears when you specify the **summary** keyword

- Example 1—Displays full status and configuration information for all VLAN subinterfaces configured on the router

```
host1#show vlan subinterface
        Interface          Status   MTU  Svlan Id Vlan Id  Ethertype  Type
------------------------- ---------- ---- -------- -------- --------- -------
ATM 3/0.1.2               Up         1522 ----     11       ----      Static
ATM 3/0.1.3               Up         1522 ----     12       ----      Static
ATM 3/1.1.1               Up         1522 ----     13       ----      Static
ATM 3/1.1.2               Up         1522 ----     14       ----      Static
ATM 3/2.1.1               Down       1526 4        255      0x9100    Static
FastEthernet 4/5.1        Up         1522 ----     1        ----      Dynamic
6 vlan subinterfaces found
```

- Example 2—Displays full status and configuration information for the specified VLAN subinterface

```
host1#show vlan subinterface fastEthernet 0/0.1
        Interface          Status   MTU  Svlan Id Vlan Id  Ethertype  Type
------------------------- ---------- ---- -------- -------- --------- -------
FastEthernet 0/0.1        Up         1526        1        0    0x9100 Static

In: Bytes 39256, Packets 612
   Multicast 0, Broadcast 0
   Errors 0, Discards 0
  Out: Bytes 4538652, Packets 70911
   Multicast 0, Broadcast 70296
   Errors 0, Discards 0
ARP Statistics:
  In: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
  Out: ARP requests 0, ARP responses 0
   Errors 0, Discards 0
```

- Example 3—Displays only brief summary information for all VLAN subinterfaces configured on the router

```
host1#show vlan subinterface summary
Total VLAN interfaces: 6 subinterfaces, 3 major interfaces
```

- Example 4—Displays full status and configuration information for all VLAN subinterfaces configured with a unique MAC address

```
host1#show vlan subinterface mac-address
        Interface          Svlan Id  Vlan Id    MAC Address
-------------------------  --------  --------  --------------
FastEthernet 4/0.25            ----        25  0090.dfad.2abd
FastEthernet 4/0.10050            1        50  0090.adad.0abd
2 vlan subinterfaces found
```

- Example 5—Displays full status and configuration information for a VLAN subinterface on a LAG bundle

```
host1#show vlan subinterface lag boston.1
        Interface           Status   MTU  Svlan Id Vlan Id  Ethertype  Type
------------------------- ---------- ---- -------- -------- --------- -------
lag boston.1              Up         1522 ----     1        ----      Static
```

- Example 6—Displays full status and configuration information for the specified S-VLAN ID

```
host1#show vlan subinterface svlan 100 53
        Interface           Status   MTU  Svlan Id Vlan Id  Ethertype  Type
------------------------- ---------- ---- -------- -------- --------- -------
FastEthernet 0/0.1        Up         1526 100      53       0x9100    Static
FastEthernet 4/6.1        Up         1526 100      53       0x9100    Dynamic
2 vlan subinterfaces found
```

Chapter 6

Managing Tunnel-Service and IPSec-Service Interfaces

This chapter describes how to configure tunnel-server ports, tunnel-service interfaces, and IPSec-service interfaces on E-series routers.

This chapter contains the following sections:

- Tunnel-Service and IPSec-Service Overview on page 251
- Tunnel-Service Interface Platform Considerations on page 253
- Redundancy and Interface Distribution of Tunnel-Service Interfaces on page 257
- Tunnel-Service Interface Considerations on page 260
- Configuring Tunnel-Server Ports and Tunnel-Service Interfaces on page 262
- Monitoring Tunnel-Service Interfaces on page 264

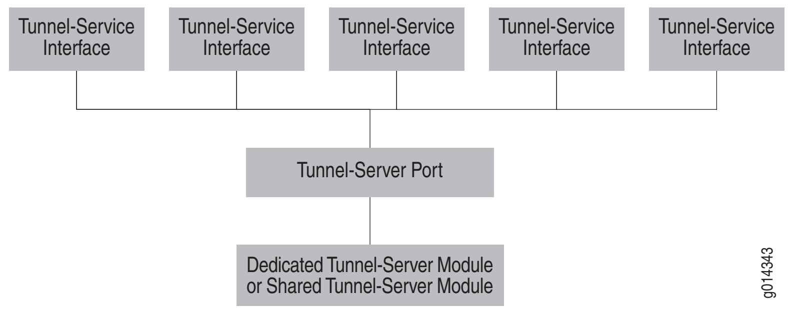
Tunnel-Service and IPSec-Service Overview

Tunnels provide a way of transporting datagrams between routers that do not support the same protocols. Often, these routers are separated by networks.

To configure tunneling, you must identify the tunnel-server ports that reside on modules that support tunnel services. You can then assign the tunnel-service interfaces that encapsulate protocols and enable them to be tunneled across the network.

Figure 35 displays the interface stacking for tunnel-service interfaces on a tunnel-server module.

Figure 35: Interface Stacking for Tunnel-Service Interfaces



This section describes the types of tunnel-server ports that you can configure on tunnel-server modules and the types of tunnel-service interfaces that you can run on these ports.

Types of Tunnel-Server Ports

E-series routers support two types of tunnel-server ports: *dedicated* tunnel-server ports and *shared* tunnel-server ports.

Dedicated Tunnel-Server Ports

Dedicated tunnel-server ports are virtual ports that are always present on dedicated tunnel-server modules. These modules offer only tunnel services; they do not offer access services.

Shared Tunnel-Server Ports

Shared tunnel-server ports are virtual ports that are always present on certain E-series line modules that provide tunnel services in addition to regular access services. You can configure the shared tunnel-server port to use a portion of the module's bandwidth to provide tunnel services.

Shared tunnel-server ports offer the following benefits:

- Greater flexibility in deploying tunnel servers

  You can use a shared tunnel-server module to provide tunnel services as an alternative to using a dedicated tunnel-server module.

- Cost savings

  If you have limited tunnel-server processing needs, you can provide tunnel services on a single available port of a shared tunnel-server module instead of having to allocate the entire bandwidth of a dedicated tunnel-server module for this purpose.

Types of Tunnel-Service Interfaces

You can configure the following types of tunnel-service interfaces using dedicated tunnel-server ports and shared tunnel-server ports:

- Static IP interfaces that you configure and delete

  Static IP interfaces include DVMRP and GRE tunnels. You must assign interfaces on other line modules to act as source endpoints for these tunnels. For information about configuring these tunnels, see *JUNOSe IP Services Configuration Guide, Chapter 10, Configuring IP Tunnels*.

- Dynamic interfaces associated with an L2TP LNS session

  The router establishes dynamic interfaces when required and removes the interfaces when they are not required. For information about applications that use these dynamic interfaces, see *JUNOSe Broadband Access Configuration Guide, Chapter 10, L2TP Overview*.

- Secure IP tunnels

  IPSec-service modules are associated with secure IP tunnels. You must configure and delete these interfaces statically; however, the router assigns tunnels to the interfaces dynamically. This mechanism means that you must manage the interfaces for tunnels manually: however, the router adds and removes tunnels when required. For information about configuring secure IP tunnels, see *JUNOSe IP Services Configuration Guide, Chapter 6, Configuring IPSec*.

Tunnel-Service Interface Platform Considerations

You can configure tunnel-service interfaces on the following E-series routers:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

This section describes the line modules, I/O modules, and I/O adapters (IOAs) that support tunnel-service interfaces.

For detailed information about the modules that support tunnel-service interfaces on the ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed specifications of these modules.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that tunnel-service modules support.

For detailed information about the modules that support tunnel-service interfaces on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed specifications of these modules.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the protocols and applications that tunnel-service modules support.

Supported Modules for Dedicated Tunnel-Server Ports

All E-series routers support dedicated tunnel-server ports; however, the supported modules depend on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

ERX-7xx models, ERX-14xx models, and the ERX-310 router all support Service Modules (SMs) and IPSec Service Modules (ISMs).

Unlike other line modules, SMs and ISMs do not pair with corresponding I/O modules that provide ingress and egress ports. Instead, they receive data from and transmit data to other line modules with ingress and egress ports.

See *JUNOSe Release Notes*, *Appendix A*, *System Maximums* for information about the number of tunnels and sessions that each module supports.

E120 Router and E320 Router

The E120 router and the E320 router support the ES2-S1 Service IOA and ES2 4G line module (LM) combination.

Unlike SMs and ISMs, you must install the ES2-S1 Service IOA with the ES2 4G LM to use dedicated tunnel-server ports. The ES2-S1 Service IOA does not have ingress and egress ports, but it conditions the ES2 4G LM to receive and transmit data to other line modules.

See *JUNOSe Release Notes*, *Appendix A*, *System Maximums* for information about the number of tunnels and sessions that the ES2-S1 Service IOA supports.

Supported Modules for Shared Tunnel-Server Ports

Most E-series routers support shared tunnel-server ports; however, the supported modules depend on the type of E-series router that you have.

See *JUNOSe Release Notes*, *Appendix A*, *System Maximums* for information about the number of tunnels and sessions that each module supports.

ERX-14xx Models and the ERX-310 Router

The ERX-1440 router and the ERX-310 router support line modules on which you can use shared tunnel-server ports. The following module combinations offer tunnel services in addition to regular access services:

- GE-2 line module with the GE-2 APS I/O module installed
- GE-HDE line module with the GE-2 SFP I/O module installed
- GE-HDE line module with the GE-8 I/O module installed

E120 Router and E320 Router

The E120 router and the E320 router support shared tunnel-server ports on the following line module and IOA combinations:

- ES2 4G LM with the ES2-S1 GE-4 IOA
- ES2 4G LM with the ES2-S1 GE-8 IOA
- ES2 4G LM with the ES2-S1 10GE IOA
- ES2 4G LM with OCx/STMx ATM IOAs
- ES2 4G LM with OCx/STMx POS IOAs

Numbering Scheme

When configuring or managing tunnel-server ports, you must know the numbering scheme for identifying the physical location of the port in the E-series router. The numbering scheme depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

Use the *slot/port* format to identify dedicated and shared tunnel-server ports.

- *slot*—Number of the slot in which the tunnel-server module resides in the chassis

  In ERX-7xx models, line module slots are numbered 2-6; slots 0 and 1 are reserved for SRP modules. In ERX-14xx models, line module slots are numbered 0–5 and 8–13; slots 6 and 7 are reserved for SRP modules. In an ERX-310 router, line module slots are numbered 1–2; slot 0 is reserved for the SRP module.

- *port*—Number of the port on the tunnel-server module

  For more information about identifying the port number on a tunnel-server port, see *Configuring Tunnel-Server Ports and Tunnel-Service Interfaces* on page 262.

For information about installing tunnel-server modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

E120 Router and E320 Router

Use the *slot/adapter/port* format to identify dedicated and shared tunnel-server ports.

- *slot*—Number of the slot in which the line module resides in the chassis

  In the E120 router, line module slots are numbered 0–5. In the E320 router, line module slots are numbered 0–5 and 11–16. For both routers, slots 6 and 7 are reserved for SRP modules; slots 8–10 are reserved for switch fabric modules (SFMs).

- *adapter*—Number of the bay in which the I/O adapter (IOA) resides

  This identifier applies to the E120 and E320 routers only. Dedicated tunnel-server ports are supported on the ES2-S1 Service IOA, which is a full-height IOA and is identified in the software as adapter 0. Shared tunnel-server ports reside on a virtual adapter that is identified in the software as adapter 2.

- *port*—Number of the port on the IOA

  For more information about identifying the port number on a tunnel-server port, see *Configuring Tunnel-Server Ports and Tunnel-Service Interfaces* on page 262.

For information about installing tunnel-server modules in the E120 and E320 routers, see *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*.

Interface Specifier

The configuration task examples in this chapter use the format for ERX-7xx models, ERX-14xx models, and the ERX-310 router to specify a tunnel-server port. (The format is described in *Numbering Scheme* on page 255.)

For example, the following command specifies a dedicated tunnel-server port on port 0 of a tunnel-server module in slot 4.

host1(config)#**tunnel-server 4/0**

When you configure a tunnel-server port on an E120 router or an E320 router, you must include the adapter identifier as part of the interface specifier. For example, the following command specifies a dedicated tunnel-server port on port 0 of an ES2-S1 Service IOA installed in both the upper and lower bays of slot 3. (When a full-height IOA is installed in the E120 router or the E320 router, it is identified in the software by the upper adapter bay 0.)

```
host1(config)#tunnel-server 3/0/0
```

For more information about interface types and specifiers on E-series models, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

Supported Applications for Dedicated and Shared Tunnel-Server Ports

Dedicated and shared tunnel-server ports provide support for some or all of the following applications and services, depending on the capabilities of the tunnel-server module on which the port resides:

- Distance Vector Multicast Routing Protocol (DVMRP) tunnels, also known as IP-in-IP tunnels
- Generic routing encapsulation (GRE) tunnels
- IPSec (on ISMs only)
- Layer 2 Tunneling Protocol (L2TP) network server (LNS) support
- IP packet reassembly for tunnels
- Network Address Translation (NAT)

NOTE: Support for IP reassembly and NAT services on shared tunnel-server ports depends on the capabilities of the module on which the shared tunnel-server port resides.

For a list of applications and services that dedicated and shared tunnel-server modules support on ERX-7xx models, ERX-14xx models, and the ERX-310 router, see *ERX Module Guide, Appendix A, Module Protocol Support*.

For a list of applications and services that dedicated tunnel-server modules support on the E120 and E320 routers, see *E120 and E320 Module Guide, Appendix A, IOA Protocol Support*.

Redundancy and Interface Distribution of Tunnel-Service Interfaces

The redundancy and distribution mechanisms supported for tunnel-service ports configured on ISMs differ from those supported for SMs, the ES2-S1 Service IOA, and shared tunnel-server ports.

This section describes the redundancy and interface distribution mechanisms for all tunnel-server ports.

SMs, ES2-S1 Service IOA, and Shared Tunnel-Server Modules

You can install multiple modules to provide redundancy. If you install multiple modules at the same time, the router automatically distributes the tunnel-service interfaces over the modules in proportion to the available tunnel-service interfaces.

Even distribution of tunnel-service interfaces is not critical to router performance. However, the number of modules that you install must be able to support the extra tunnel if one of the modules becomes unavailable.

NOTE: When both dedicated tunnel-server ports (on SMs) and shared tunnel-server ports (on shared tunnel-server modules) are configured on ERX-7xx models, ERX-14xx models, and the ERX-310 router, the router performs load balancing across all available server ports of the same type. For this purpose, dedicated tunnel-server ports (on SMs) and shared tunnel-server ports (on shared tunnel-server modules) are considered one type of server port, whereas server ports on ISMs are considered a different type.

Interface allocation depends on the types of tunnel-service interface created on the router. For more information about the types of tunnel-service interfaces, see *Types of Tunnel-Service Interfaces* on page 253.

Static IP Tunnel-Service Interfaces

You can configure and delete static IP tunnel-service interfaces.

When you configure a static tunnel-service interface, the router automatically assigns that interface to a particular module. If that module becomes unavailable, the router attempts to reassign the interface to an available module. If no module is currently available, the router keeps track of the interface and assigns it to a module when one become available.

Consequently, if you reinstall a module that was formerly unavailable or removed, the distribution of static tunnel-service interfaces over the modules might be uneven. Because users create and remove static tunnels, the distribution might remain uneven indefinitely.

Dynamic Tunnel-Service Interfaces

The router dynamically creates and deletes dynamic tunnel-service interfaces as dictated by the operation of the relevant protocols. Currently, L2TP sessions are the only dynamic tunnel-service interfaces available.

When the router creates a dynamic tunnel-service interface, it assigns that interface to a particular module. If that module becomes unavailable, the router removes the interface. If the initiator of the dynamic interface requests its reestablishment, the router recreates the dynamic tunnel service interface and assigns it to an available module.

Going forward, if you reinstall a module that was formerly unavailable or removed, the router deletes unwanted dynamic tunnel-service interfaces and creates new ones for applications on other modules. Gradually, the distribution of dynamic tunnel-service interfaces on the modules becomes even.

Interface Allocation for Shared Tunnel-Server Modules

When determining how to distribute interfaces across tunnel-server ports, the E-series router does not perform interface policing to prevent the access services of a shared tunnel-server module from depriving the tunnel services of the requisite interface resources (and vice-versa). We recommend that when provisioning shared tunnel-server ports, you restrict the number of interfaces configured for both access and tunnel services to prevent competition between them.

For example, when paired with the ES2-S1 OC3-8/STM1 IOA or the ES2-S1 GE-4 IOA, the ES2 4G LM on the E320 router can support a maximum of 16,000 access interfaces and 8,000 shared tunnel-server interfaces, both of which must compete for the overall supported maximum of 16,000 interface columns.

For tunneling, PPP, and IP maximums, see *JUNOSe Release Notes, Appendix A, System Maximums*.

ISMs

You can install multiple ISMs to provide redundancy. If you install multiple ISMs at the same time, the router automatically distributes ISM interfaces over the modules in proportion to the available ISM interfaces.

Even distribution of ISM interfaces is not critical to router performance. However, the number of ISMs that you install must be able to support the extra tunnels if one of the modules becomes unavailable.

When you configure a static IPSec interface, the router automatically assigns that interface to a particular ISM. If that ISM becomes unavailable, the interface becomes not present (operational state down).

The router then manages the interface as follows:

- If the interface’s local IP address (tunnel source) is less than the remote IP address (tunnel destination), the router attempts to reassign the interface to an available ISM. If the reassignment is successful, the router immediately initiates an IPSec negotiation, also known as *rekeying* the interface.
- If the interface’s local IP address is greater than the remote IP address, the router attempts to reassign the interface to an available ISM. If the reassignment is successful, the router waits 3 minutes before initiating an IPSec negotiation.

In either case, the interface becomes available (operational state up) when the rekeying operation is completed successfully. If the rekeying operation fails for reasons such as an unreachable remote end or a policy mismatch, the router waits a certain number of minutes and then tries again.

The wait time increases after each unsuccessful rekeying attempt, and follows a progressive pattern. This pattern gradually increases in intervals, starting at 1 minute and reaching a maximum interval of 60 minutes. The 60-minute interval repeats indefinitely. When the rekeying operation is completed successfully, the pattern starts again.

If no ISM is available to which the router can reassign the interface, the interface remains in the not present state until an ISM becomes available. As a result, the distribution of dedicated ISM interfaces over the modules might become uneven.

Tunnel-Service Interface Considerations

To configure a tunnel-server port, you assign the maximum number of tunnel-service interfaces to run on the specified tunnel-server port. This process is referred to as *provisioning*. Conversely, the process of reducing the maximum number of tunnel-service interfaces on a tunnel-server port to zero is referred to as *unprovisioning* the port.

This section describes the considerations for provisioning and unprovisioning tunnel-service interfaces on dedicated and shared tunnel-server ports.

For instructions on how to provision and unprovision tunnel-service interfaces, see *Configuring Tunnel-Server Ports and Tunnel-Service Interfaces* on page 262.

Provisioning Tunnel-Service Interfaces

By default, dedicated tunnel-server ports are configured to have the maximum number of tunnel-service interfaces that the dedicated tunnel-server module supports. You can reduce the maximum number of interfaces or completely unprovision the port by issuing the **max-interfaces** command.

By default, shared tunnel-server ports are configured to have no tunnel-service interfaces. To provision tunnel-service interfaces on shared tunnel-server ports, you must provision the port by assigning a nonzero maximum number of tunnel-service interfaces to run on the port by issuing the **max-interfaces** command.

Bandwidth Limitations of Shared Tunnel-Server Ports

Bandwidth limitations for shared tunnel-server ports and tunnel-service interfaces depend on bandwidth restrictions, if any, that are in effect for the module on which the shared tunnel-server port resides.

Exchanging Tunnel-Server Modules

Tunnel-server modules are available in different hardware revisions that support varying numbers of tunnel-service interfaces. For more information about determining the hardware revision on a module, see *ERX Module Guide, Table 1, Module Combinations*, or *E120 and E320 Module Guide, Table 1, Modules and IOAs*.

When you exchange a tunnel-server module with a lower capacity for tunnel-service interfaces with a module that supports a higher capacity, the tunnel-server port maintains the original number of provisioned tunnel-service interfaces. By using the **all-available** keyword with the **max-interfaces** command, you can configure the tunnel-server port to automatically adjust the number of provisioned tunnel-service interfaces to the maximum value supported by the new module.

When you exchange a tunnel-server module that has a higher number of provisioned interfaces than the new module's capacity, the module adjusts the provisioned number of interfaces to the maximum value that the module supports.

Table 24 displays sample capacity, configuration, and utilization values for exchanging tunnel-server modules with different capacities.

Table 24: Sample Capacity, Configuration, and Utilization Values for Tunnel-Service Interfaces

Old Capacity	Old Provisioned Interfaces (max-interfaces command)	Old Utilization	New Capacity	New Provisioned Interfaces (max-interfaces command)	New Utilization
8000	5000	5000	16,000	5000	5000
8000	8000	8000	16,000	8000	8000
8000	all-available	8000	16,000	all-available	16,000
16,000	5000	5000	8000	5000	5000
16,000	16,000	16,000	8000	8000	8000
16,000	all-available	16,000	8000	all-available	8000

Unprovisioned Tunnel-Service Interfaces

Tunnel-server ports exist whether or not they have been configured. This means that you cannot delete a tunnel-server port from a module. However, you can unprovision all of the tunnel-service interfaces on a tunnel-server port by issuing the **no max-interfaces** command or the **no tunnel-server** command.

You can also restore the default configuration by issuing the **default max-interfaces** command. On dedicated tunnel-server ports, the default configuration is the maximum number of interfaces that the port supports. On shared tunnel-server ports, the default configuration is zero tunnel-service interfaces.

NOTE: If the module on which the tunnel-server port resides supports IP reassembly or NAT services, these services become enabled when you provision tunnel-service interfaces on the port. However, when you unprovision tunnel-service interfaces to zero, only IP reassembly is disabled and NAT remains configured in the current release.

Configuring Tunnel-Server Ports and Tunnel-Service Interfaces

This section describes the tasks associated with configuring a tunnel-server port and tunnel-service interface.

Identifying the Physical Location of the Tunnel-Server Port

To display the physical location of the dedicated tunnel-server port on your module, issue the **show tunnel-server config** command.

```
host1#show tunnel-server config

                          Server Ports
                          ------------
                                         Provisioned
  Port      Type     MaximumInterfaces   Interfaces    HwPresent
--------   -------   -----------------   -----------   ---------
Port 2/2   shared       8000                0             yes
Port 8/0   dedicated    16000               8000          yes
```

Provisioning the Maximum Number of Interfaces on a Tunnel-Server Port

To provision the maximum number of interfaces on a tunnel-server port:

1. From Global Configuration mode, specify the location of the dedicated tunnel-server port that you want to configure.

   On a dedicated tunnel-server port:

   host1(config)#**tunnel-server 8/0**
   host1(config-tunnel-server)#

   On a shared tunnel-server port:

   host1(config)#**tunnel-server 2/2**
   host1(config-tunnel-server)#

   This command accesses Tunnel Server Configuration mode.

2. Provision the maximum number of tunnel-service interfaces to be used on the dedicated tunnel-server port.

   host1(config-tunnel-server)#**max-interfaces all-available**

NOTE: When you issue the **tunnel-server** command, ensure that you specify the same interface specifier that was displayed for this tunnel-server port in the **show tunnel-server config** command in the output described in *Identifying the Physical Location of the Tunnel-Server Port* on page 262. If you specify an incorrect location for the tunnel-server port, the router displays an error message and rejects the command as invalid.

Verifying the Tunnel-Server Interface Configuration

To verify that you properly provisioned the number of tunnel-server interfaces on the tunnel-server port:

1. From Tunnel Server Configuration Mode, return to Privileged Exec mode.

   host1(config-tunnel-server)#**exit**
   host1(config)#**exit**
   host1#

2. Issue the **show tunnel-server config** command.

```
host1#show tunnel-server config

                          Server Ports
                          ------------
                                             Provisioned
  Port      Type     MaximumInterfaces   Interfaces    HwPresent
--------   -------   -----------------   -----------   ---------
Port 2/2   shared       8000                5000          yes
Port 8/0   dedicated    16000               all-available yes
```

   For more information about using the **show tunnel-server** command, see *Monitoring Tunnel-Service Interfaces* on page 264.

Unprovisioning Tunnel-Service Interfaces

To unprovision the tunnel-service interfaces on a tunnel-server port, use any of the following commands, all of which have the same effect:

- Issue the **no max-interfaces** command from Tunnel Server Configuration mode.

  host1(config-tunnel-server)#**no max-interfaces**

- Issue the **max-interfaces 0** command from Tunnel Server Configuration mode.

  host1(config-tunnel-server)#**max-interfaces 0**

- Issue the **no tunnel-server** command from Global Configuration mode. This command unprovisions the tunnel-service interfaces on the specified tunnel-server port but does *not* delete the port itself.

  host1(config)#**no tunnel-server 2/2**

max-interfaces

- Use from Tunnel Server Configuration mode to provision the maximum number of tunnel-service interfaces to be used on a tunnel-server port.
- Specify an integer in the range 0–16000 to provision the maximum number of tunnel-service interfaces.
- Use the **all-available** keyword to provision the maximum number of tunnel-service interfaces to match the maximum value that the tunnel-server module supports.

- Examples

  host1(config-tunnel-server)#**max-interfaces 5000**
  host1(config-tunnel-server)#**max-interfaces all-available**

- Use the **default** version to restore the default configuration. On dedicated tunnel-server ports, the default configuration is the maximum number of tunnel-service interfaces that the tunnel-service module supports (**all-available**). On shared tunnel-server ports, the default configuration is zero tunnel-server interfaces.
- Use the **no** version to reduce the number of provisioned tunnel-service interfaces to zero. Issuing the **no max-interfaces** command has the same effect as issuing the **max-interfaces 0** command.

tunnel-server

- Use from Global Configuration mode to specify the physical location of the tunnel-server port that you want to configure.
- The **tunnel-server** command accesses Tunnel Server Configuration mode, which enables you to provision the maximum number of tunnel-service interfaces to be used on the tunnel-server port.
- For ERX-7xx models, ERX-14xx models, and the ERX-310 router, use the *slot/port* format.
- For the E120 router and the E320 router, use the *slot/adapter/port* format. On dedicated tunnel-server ports, use adapter 0 and port 0. On shared tunnel-server ports, use adapter 2 and port 0.
- Example

  host1(config)#**tunnel-server 12/2**

- Use the **default** version to restore the default configuration. On dedicated tunnel-server ports, the default configuration is the maximum number of tunnel-service interfaces that the tunnel-service module supports. On shared tunnel-server ports, the default configuration is zero tunnel-service interfaces.
- Use the **no** version to reduce the number of provisioned tunnel-service interfaces to zero.

Monitoring Tunnel-Service Interfaces

You can monitor tunnel-service interfaces by using the **show tunnel-server** command.

NOTE: The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

show tunnel-server

- Use to display status and configuration information for dedicated and shared tunnel-server ports and tunnel-service interfaces configured on the router. Unconfigured tunnel-server ports are not displayed in the output.
- You can display information for a specific tunnel-server port or for all tunnel-server ports.
- Use the optional **config** keyword to display information about available and provisioned tunnel-service interfaces on each port, and to indicate whether modules that support the use of dedicated or shared tunnel-server ports are currently installed in the router.
- Field descriptions
  - Port:Appl—Identifier in *slot/port* or *slot/adapter/port* format for the module or tunneling application
    - slot—Number of the slot in the chassis where the module resides
    - adapter—Number of the bay in which the I/O adapter (IOA) resides.

      This identifier applies only to dedicated and shared tunnel-server ports configured on the E120 and E320 routers. Dedicated tunnel-server ports are always adapter 0; shared tunnel-server ports are always adapter 2.
    - *port*—Number of the tunnel-server port on the module; for dedicated tunnel-server ports, this is a virtual port number that is always 0; for shared tunnel-server ports, this is a virtual port number dynamically assigned by the router
  - Card Type or Active Type—Type of port: dedicated or shared
  - Oper State or Max State—Physical state of the port or application
    - up—Port or application is available
    - down—Port or application is unavailable
    - present—Module associated with this port is installed
    - not present—Module associated with this port has been removed
    - pending—Router has not yet detected all previously configured modules during a reboot or initial installation of the module
  - Active Interfaces or Interfaces—Number of tunnel-service interfaces currently configured on this port
  - Max Interfaces—Total number of tunnel-service interfaces available on this module
  - Fill—Percentage of available interfaces used by a server port, an application on a server port, an application on all server ports, and all server ports
  - Appl Totals—Statistics for each application

- Server Ports—Displays configuration information about dedicated and shared tunnel-server ports on the router; this display format appears only when the **config** keyword is specified
  - Port—Identifier in *slot/port* format (ERX-7xx models, ERX-14xx models, and ERX-310 routers) or *slot/adapter/port* format (E120 and E320 routers) for the module on which the tunnel-server port resides
  - Type—Type of tunnel-server port: dedicated or shared
  - MaximumInterfaces—Total number of tunnel-service interfaces available on this module
  - Provisioned Interfaces—Total number of tunnel-service interfaces currently provisioned on this port
  - HwPresent—Indicates whether a module that supports the specified tunnel-server port is currently installed in the router: yes or no
- Example 1—Displays information about a dedicated tunnel-server port on an SM

```
host1#show tunnel-server

                    Card      Oper     Active      Max
   Port:Appl        Type      State  Interfaces Interfaces Fill
--------------- ---------  ------- ---------- ---------- ----
       Port 8/0 dedicated  present          1       8000 0.0%
   ipsec-tunnel               down          0          0 0.0%
ipsec-transport               down          0          0 0.0%
           l2tp                 up          0       8000 0.0%
     gre/dvmrp                  up          1       4000 0.0%
    Appl Totals
   ipsec-tunnel                             0          0 0.0%
ipsec-transport                             0          0 0.0%
           l2tp                             0       8000 0.0%
      gre/dvmrp                             1       4000 0.0%
          total                             2      12000 0.0%
```

- Example 2—Displays information about a dedicated tunnel-server port on an ISM

```
host1#show tunnel-server

Card      Oper     Active      Max
   Port:Appl        Type      State  Interfaces Interfaces Fill
--------------- ---------  ------- ----------  ---------- ----
       Port 2/0 dedicated  present          1        8000 0.0%
   ipsec-tunnel                 up          0           0 0.0%
ipsec-transport               down          0           0 0.0%
           l2tp               down          0        8000 0.0%
      gre/dvmrp                 up          1        4000 0.0%
    Appl Totals
   ipsec-tunnel                             0           0 0.0%
ipsec-transport                             0           0 0.0%
           l2tp                             0       16000 0.0%
      gre/dvmrp                             2        8000 0.0%
          total                             2       16000 0.0%
```

- Example 3—Displays information about a specific shared tunnel-server port

```
host1#show tunnel-server 2/2

                  Card      Oper     Active      Max
   Port:Appl      Type      State  Interfaces Interfaces Fill
--------------- ---------  ------- ---------- ---------- ----
       Port 2/2   shared   present          0       4000 0.0%
   ipsec-tunnel               down          0          0 0.0%
ipsec-transport               down          0          0 0.0%
           l2tp                 up          0       4000 0.0%
     gre/dvmrp                  up          0       4000 0.0%
```

- Example 4—Displays configuration information about dedicated and shared tunnel-server ports

```
host1#show tunnel-server config

                          Server Ports
                          ------------
                                          Provisioned
  Port      Type     MaximumInterfaces   Interfaces    HwPresent
--------   -------   -----------------   -----------   ---------
Port 2/2   shared       8000                4000          yes
Port 8/0   dedicated    16000               16000         yes
```

Index

Numerics

10-Gigabit Ethernet interfaces
- modules ... 177
- specifying an interface ... 185

4xDS3 ATM I/O modules ... 44

A

Address Resolution Protocol. *See* ARP
aggregation, Ethernet link ... 205, 229
all option (show controllers) ... 26, 60
aps commands
- aps events ... 88
- aps force ... 88
- aps group ... 84, 85
- aps lockout ... 85
- aps manual ... 89
- aps protect ... 86
- aps revert ... 86
- aps unidirectional ... 86
- aps working ... 84
- *See also* show aps commands

APS/MSP (Automatic Protect Switching/Multiplex Section Protection)
- automatic switchover ... 68
- channel numbers ... 76, 109
- communication methods ... 70
- configuration example ... 87
- configuring ... 83, 112
- events ... 88
- K1 byte ... 70
- K2 byte ... 70
- manual switchover ... 68, 88
- monitoring ... 98, 162
- overview ... 101
- protect interface ... 68, 76, 85, 109
- reversion after switchover ... 69
- switching mechanisms ... 69
- working interface ... 68, 76, 83, 109

ARP (Address Resolution Protocol) ... 164
ATM virtual circuit (VC) ... 187
audience for documentation ... xi
Automatic Protect Switching. *See* APS/MSP

B

baseline commands
- baseline interface ... 230
- baseline interface serial
  - channelized T3 interfaces ... 26
  - cOCx/STMx interfaces ... 144
  - E3/T3 interfaces ... 60
- baseline line interface sonet ... 91, 145
- baseline path interface sonet ... 91, 145
- baseline section interface sonet ... 92, 145

BERT (bit error rate test) patterns
- channelized T3 interfaces ... 7, 21, 23
- cOCx/STMx interfaces ... 110, 137
- E3/T3 interfaces ... 46, 57

bert command
- channelized T3 interfaces ... 21
- E3/T3 interfaces ... 57

bit error rate test patterns. *See* BERT patterns

C

cable length
- specifying ... 11, 50

cablelength commands
- cablelength ... 11, 50

cell scrambling
- E3 ... 51
- T3 ... 51

CE-side load balancing ... 229
channel numbers, APS/MSP interfaces ... 76, 109
channel-group commands.*See* path ds1 | e1 commands
channelized OCx/STMx interfaces. *See* cOCx/STMx interfaces
channelized T3 interfaces
- bert command ... 21
- configuring ... 8, 20
- configuring HDLC channel ... 17
- equipment loopback command ... 22
- loopback command ... 22
- monitoring parameters ... 25
- numbering scheme ... 5, 7
- references ... 7
- testing ... 20, 25

clock commands
  clock source
    channelized T3 interfaces ... 11, 21
    cOCx/STMx interfaces ... 112, 118
    E3/T3 interfaces ... 50, 57
    OCx/STMx interfaces ... 79
clock source, selecting
  channelized T3 interfaces ... 11, 13
  cOCx/STMx interfaces ... 126
  E1 interfaces on cOCx/STMx ... 118
  E3/T3 interfaces ... 50
  OCx/STMx interfaces ... 79, 112
  T1 interfaces on cOCx/STMx ... 118
  T3 interfaces on cOCx/STMx ... 123
cOCx/STMx interfaces
  configuring HDLC channel ... 130
  configuring T1/E1 ... 116
  loopback ... 56, 136
  monitoring ... 144
  numbering scheme ... 109
  references ... 109
  testing ... 136, 143
COCX-F3 line modules ... 43
configuring. *See specific feature, product, or protocol*
connectivity in SONET/SDH paths ... 90, 143
control traffic for high-density Ethernet ... 181
controller commands
  controller e3 ... 48
  controller sonet ... 80, 112
  controller t3 ... 9, 13, 48
conventions defined
  icons ... xii
  text and syntax ... xiii
counters
  channelized T3 interfaces ... 26
  E3/T3 interfaces ... 59
CRC (cyclic redundancy check)
  channelized T3 interfaces ... 18
  cOCx/STMx interfaces ... 130
  E3/T3 interfaces ... 53
crc command
  channelized T3 interfaces ... 18
  cOCx/STMx interfaces ... 130
  E3/T3 interfaces ... 53
CT3/T3 12 I/O modules ... 45
CT3/T3 12 line modules ... 4
CT3/T3 F0 line modules ... 45
customer support, contacting ... xviii
cyclic redundancy check. *See* CRC

D

data stream inversion, enabling
  channelized T3 interfaces ... 19
  cOCx/STMx interfaces ... 131
  E3/T3 interfaces ... 54
dedicated tunnel-server ports
  configuring ... 262
  overview ... 252
  supported applications ... 257
  supported modules ... 254
description command
  channelized T3 interfaces ... 11
  E3/T3 interfaces ... 51
  unchannelized SONET interfaces ... 80, 113
description, interface
  channelized T3 interfaces ... 11, 13
  cOCx/STMx interfaces ... 116, 117, 123, 127
  E3/T3 interfaces ... 51
  serial interfaces ... 20, 55, 132
  unchannelized SONET interfaces ... 80, 113
Distance Vector Multicast Routing Protocol. *See* DVMRP tunnels
documentation set, E-series and JUNOSe ... xiv
  comments on ... xviii
  obtaining ... xvii
DS0 timeslots
  channelized T3 interfaces ... 14
  cOCx/STMx interfaces ... 106, 108, 118, 128
DS1. *See T1 entries*
DS3. *See T3 entries*
ds3-scramble command ... 51
dsu commands
  dsu bandwidth ... 52
  dsu mode ... 52
duplex command ... 184
DVMRP tunnels ... 253
dynamic interfaces
  configuring PPPoE over static PPPoE S-VLAN oversubscription ... 204
dynamic tunnel-server ports
  applications supported ... 257
  overview ... 255
  unprovisioning ... 263
dynamic tunnel-service interfaces
  monitoring ... 264
  overview ... 253

E

E1
  fractional ... 106
  unframed ... 106
E1 channels
  cOCx/STMx interfaces ... 106, 116
E1 interfaces. *See* cOCx/STMx interfaces

E120 and E320 routers
  Ethernet interfaces ... 165
  tunnel-service interfaces ... 254
E120 routers ... xii, xiv, 71, 165
E3 interfaces
  configuring controllers ... 47
  configuring HDLC channel ... 53
  loopback command ... 59
  monitoring interfaces ... 59
  numbering scheme ... 46
  references ... 46
E320 routers ... xii, xiv, 71, 165, 253
  100 Gbps fabric ... 74, 177
  120 Gbps fabric ... 74
  320 Gbps fabric ... 74, 177
  SONET/SDH interfaces ... 72
e3-scramble command ... 51
encapsulation commands
  encapsulation ppp ... 195, 199
  encapsulation vlan ... 196, 200, 203
equipment loopback command
  channelized T3 interfaces ... 22
  T3 interfaces ... 58
ERX-14xx models ... xii
ERX-310 router ... xii
ERX-7xx models ... xii
ES2 10G line module (LM) ... 174, 175, 179
ES2 10G Uplink line module (LM) ... 178
ES2 4G line module (LM) ... 74, 171, 177
E-series and JUNOSe documentation set ... xiv
  comments on ... xviii
  obtaining ... xvii
E-series router models ... xii
ethernet description command ... 184
Ethernet interfaces
  CE-side load balancing ... 229
  commands
    ethernet description ... 184
    interface fastEthernet ... 184, 203
    interface gigabitEthernet ... 185
    interface lag ... 213
    interface tenGigabitEthernet ... 185
    See also show commands
  configuring ... 183
  disabling interfaces ... 230
  duplex type ... 184
  high-density ... 181
  IEEE 802.1Q ... 187
  IEEE 802.3ad ... 205
  IEEE 802.3ae ... 164, 177
  L2TP ... 165
  line speed ... 187
  link aggregation (LAG) ... 205
  MAC address validation ... 186
  monitoring ... 230
  MPLS ... 214, 225, 229
  multinetting ... 165
  numbering scheme ... 166, 255
  PPPoE over S-VLANs ... 198
  PPPoE over VLANs ... 191, 193
  subnetwork attachment point (SNAP) ... 188
  S-VLANs ... 197, 204
  VLANs ... 187, 197
Ethernet link aggregation
  CE-side load balancing ... 229
  configuration examples ... 209
  configuring ... 207
  enabling CE-side load balancing ... 229
  Martini layer 2 transport ... 229
  MPLS ... 209, 212
  overview ... 205
  PPPoE subinterfaces ... 208, 210
  VLAN subinterfaces ... 208, 211
Ethernet link aggregation commands
  interface lag ... 213
  lacp ... 213
  lacp port-priority ... 213
  member-interface ... 214
  pppoe subinterface lag ... 214
Ethernet link redundancy
  configuration models ... 215
  configuring ... 224
  link behavior ... 220
  overview ... 214
Ethernet link redundancy commands
  redundant-port ... 224
  redundant-port force-failover ... 225
Ethertype value, assigning to S-VLANs ... 200, 204
events
  APS/MSP ... 88

F

facilities data link. *See* FDL
Fast Ethernet interfaces
  modules ... 167
  specifying an interface ... 184, 203
FDL (facilities data link)
  cOCx/STMx interfaces ... 102
    monitoring statistics ... 157
    T1 channel over DS3, configuring ... 128
    T1 over VT, configuring ... 120
  T1 channels on channelized T3 interfaces ... 1
    configuring ... 15
    monitoring statistics ... 34
filtering
  show displays ... 26, 60, 144
fractional T1/E1 ... 6, 106
fractional T3 ... 52

framing command
- channelized T3 interfaces ... 11
- E3/T3 interfaces ... 51

framing format
- channelized T3 interfaces ... 11, 13
- cOCx/STMx interfaces ... 119, 124
- E3/T3 line ... 51

G

Generic Routing Encapsulation. *See* GRE tunnels

Gigabit Ethernet interfaces
- modules ... 168
- redundant port ... 168, 169
- specifying an interface ... 185

GRE (Generic Routing Encapsulation) tunnels ... 253

H

HDLC channel, configuring
- channelized T3 interfaces ... 17
- cOCx/STMx interfaces ... 130
- E3/T3 interfaces ... 53

high-density Ethernet
- overview ... 181
- packet classifier ... 181
- supported modules ... 170, 174, 175, 177

I

icons defined, notice ... xii

idle character
- channelized T3 interfaces ... 18
- cOCx/STMx interfaces ... 119, 131
- E3/T3 interfaces ... 54

idle-character command
- channelized T3 interfaces ... 18
- cOCx/STMx interfaces ... 119, 131
- E3/T3 interfaces ... 54

IEEE 802.1Q ... 187

IEEE 802.1w ... 180

IEEE 802.3 ... 180

IEEE 802.3ad ... 205

IEEE 802.3ae ... 164, 177

IEEE 802.3u ... 180

IEEE 802.3z ... 180

intelligent dropping of packets ... 181

interface commands
- interface fastEthernet ... 184, 203
- interface gigabitEthernet ... 185
- interface lag ... 213
- interface serial
  - channelized T3 interfaces ... 18
  - cOCx/STMx interfaces ... 131
  - E3/T3 interfaces ... 54
- interface tenGigabitEthernet ... 185

interface description
- channelized T3 interfaces ... 11, 13
- cOCx/STMx interfaces ... 116, 117, 123, 127
- E3/T3 interfaces ... 51
- serial interfaces ... 20, 55, 132
- unchannelized SONET interfaces ... 80, 113

interface stack
- cOCx/STMx interfaces ... 105
- E3/T3 interfaces ... 45
- ES2-21 OC48/STM16 POS ... 75
- OC48/STM16 interfaces ... 73
- OCx/STMx POS interfaces ... 73
- OCx/STMx/DS3-ATM interfaces ... 72

interfaces, monitoring
- channelized T3 ... 25
- cOCx/STMx ... 144
- E3/T3 ... 59
- Ethernet ... 230
- OCx/STMx ... 91

internal clocking ... 126
- channelized T3 interfaces ... 11
- cOCx/STMx interfaces ... 112, 126
- E1 interfaces ... 119, 123
- E3/T3 interfaces ... 50
- OCx/STMx interfaces ... 79
- T1 interfaces ... 119, 123

invert data command
- channelized T3 interfaces ... 19
- cOCx/STMx interfaces ... 131
- E3/T3 interfaces ... 54

ip commands
- ip address ... 165, 200
- ip mac-validate ... 186

IP tunnels
- secure ... 253, 259

ISMs (IPSec Service modules)
- monitoring ... 264
- redundancy and interface distribution ... 259

J

JUNOSe software CD ... xvii

K

K1 byte, APS/MSP ... 70

K2 byte, APS/MSP ... 70

L

L2TP (Layer 2 Tunneling Protocol) ... 165, 178

L2TP network server. *See* LNS

LACP (Link Aggregation Control Protocol) ... 206
- PPPoE subinterfaces ... 208, 210
- redundant member link behavior ... 221

layer 2 services over MPLS
- 802.3ad link aggregation 229
- 802.3ad switch 229

Layer 2 Tunneling Protocol. *See* L2TP

line clocking 13, 126
- channelized T3 interfaces 11
- cOCx/STMx interfaces 112, 126
- E1interfaces 119, 123
- E3/T3 interfaces 50
- OCx/STMx interfaces 79
- T1 interfaces 119, 123

line layer, SONET/SDH 105

line modules
- changing 5, 78

line speed 187

link commands
- link failover force 182
- link failover timeout....182
- link selection....182

LNS (L2TP network server)
- termination 253

load-interval command
- channelized T3 interfaces 19
- E3/T3 interfaces 54
- Ethernet interfaces....186

local loopback
- channelized T3 interfaces 22, 24
- cOCx/STMx interfaces 138
- E3/T3 interfaces 59
- OCx/STMx interfaces 89

loopback
- channelized T3 interfaces 22, 24
- cOCx/STMx interfaces 56, 136
- E3/T3 interfaces 59
- T3 interfaces, remote 58

loopback command
- channelized T3 interfaces 21, 22
- cOCx/STMx interfaces 139
- E3/T3 interfaces 59
- OCx/STMx interfaces 89

M

MAC (media access control) addresses
- configuring for S-VLANs 198, 201
- configuring for VLANs 188, 197
- validation....186

MAC pause frames....171

maintenance data link. *See* MDL

manual switchover, APS/MSP....88

manuals, E-series and JUNOSe xiv
- comments on.... xviii

maximum receive unit. *See* MRU

maximum transmission unit. *See* MTU

max-interfaces command 263

MDL (maintenance data link)
- channelized T3 interfaces 1
  - configuring....9
  - monitoring statistics 34
- T3 interfaces 41
  - configuring....49
  - monitoring statistics 64
- T3 on cOCx/STMx interfaces 102
  - configuring....124
  - monitoring statistics 157

mdl commands
- mdl carrier....10, 49
- mdl string 10, 49
- mdl transmit 10, 49

MIBs (Management Information Bases).... xvii

models
- E120....xii
- E320....xii
- ERX-14xx xii
- ERX-310 xii
- ERX-7xx....xii

monitoring commands
- monitor vlan interface 232

monitoring. *See specific feature, product, or protocol*

MPLS (Multiprotocol Label Switching)
- configuring over Ethernet link aggregation....206
- configuring S-VLAN tunnels 201, 204
- fast reroute....79, 112

mpls commands
- mpls 214, 229

MRU (maximum receive unit)
- channelized T3 interfaces 19
- cOCx/STMx interfaces 132
- E3/T3 interfaces....55

mru command
- channelized T3 interfaces 19
- cOCx/STMx interfaces 132
- E3/T3 interfaces....55

MSP (Multiplex Section Protection) 67, 101

MTU (maximum transmission unit)
- channelized T3 interfaces 19
- cOCx/STMx interfaces 132
- E3/T3 interfaces....55
- Ethernet interfaces....186

mtu command
- channelized T3 interfaces 19
- cOCx/STMx interfaces 132
- E3/T3 interfaces....55
- Ethernet interfaces....186

multinetting....165

Multiplex Section Protection. *See* APS/MSP; MSP

Multiprotocol Label Switching. *See* MPLS

N

network loopback
- channelized T3 interfaces ... 22, 24
- cOCx/STMx interfaces ... 138
- E3/T3 interfaces ... 59
- OCx/STMx interfaces ... 89

notice icons defined ... xii
numbering scheme
- ASP/MSP ... 76, 109
- slot/adapter/port ... 77, 166, 256
- slot/port ... 5, 46, 76, 109, 166, 255

O

OC12 I/O modules ... 72
OC3/STM1 GE/FE line module ... 73, 171
OC3-2 GE APS I/O module ... 73, 171
OC3-4 I/O modules ... 72, 73
OCx/STMx interfaces
- configuring ... 78
- disabling ... 82
- line modules ... 67
- monitoring statistics ... 91
- numbering scheme ... 76
- path ds3 loopback remote command ... 142
- testing ... 89

OCx/STMx POS line modules ... 72, 73
OCx/STMx/DS3-ATM line modules ... 44, 72
oversubscription
- S-VLANs ... 204

P

packet classifier ... 181
packets
- intelligently dropping ... 181

path commands
- path ... 113
- path description ... 80, 113
- path e1 unframed ... 117
- path overhead c2 ... 81, 114
- path overhead j1 ... 90, 143
- path snmp trap link-status ... 81, 114
- path trigger alarm ... 82, 114
- path trigger delay ... 82, 115

path ds1 fdl commands
- path ds1 fdl ... 120
- path ds1 fdl carrier ... 120
- path ds1 fdl transmit ... 121

path ds1 remote-loopback command ... 141
path ds1|e1 commands
- path ds1|e1 ... 116
- path ds1|e1 bert ... 137
- path ds1|e1 channel-group description ... 117
- path ds1|e1 channel-group shutdown ... 118
- path ds1|e1 channel-group snmp trap link-status ... 118
- path ds1|e1 channel-group timeslots ... 118
- path ds1|e1 clock source ... 118
- path ds1|e1 description ... 116
- path ds1|e1 framing ... 119
- path ds1|e1 loopback ... 139
- path ds1|e1 loopback remote ... 141
- path ds1|e1 shutdown ... 121
- path ds1|e1 snmp trap link-status ... 119

path ds3 commands
- path ds3 ... 122
- path ds3 bert ... 137
- path ds3 clock source ... 123
- path ds3 description ... 123
- path ds3 framing ... 124
- path ds3 loopback ... 139
- path ds3 loopback remote ... 142
- path ds3 shutdown ... 124
- path ds3 snmp trap link-status ... 124

path ds3 mdl commands
- path ds3 mdl carrier ... 125
- path ds3 mdl string ... 125
- path ds3 mdl transmit ... 125

path ds3 t1 commands
- path ds3 t1 ... 126
- path ds3 t1 bert ... 138
- path ds3 t1 clock source ... 126
- path ds3 t1 description ... 127
- path ds3 t1 framing ... 127
- path ds3 t1 loopback ... 140
- path ds3 t1 loopback remote ... 142
- path ds3 t1 remote-loopback ... 143
- path ds3 t1 shutdown ... 127
- path ds3 t1 snmp trap link-status ... 128
- path ds3 t1 timeslots ... 128

path ds3 t1 fdl commands
- path ds3 t1 fdl ... 129
- path ds3 t1 fdl carrier ... 129
- path ds3 t1 fdl transmit ... 129

path layer, SONET/SDH ... 105
pause frames ... 171
payload loopback
- channelized T3 interfaces ... 22
- E3/T3 interfaces ... 59

platform considerations
- channelized T3 interfaces ... 4
- cOCx/STMx interfaces ... 104
- Ethernet interfaces ... 165
- tunnel-service interfaces ... 253
- unchannelized SONET/SDH interfaces ... 71
- unchannelized T3/E3 interfaces ... 43

PPPoE ... 208
Point-to-Point Protocol over Ethernet. *See* PPPoE

ports, tunnel-server
dedicated 252
shared 252
PPPoE (Point-to-Point Protocol over Ethernet)
subinterfaces for LACP 208, 210
pppoe commands
pppoe 200
pppoe subinterface fastEthernet 196, 200
pppoe subinterface gigabitEthernet 196, 200
pppoe subinterface lag 214
pppoe subinterface tenGigabitEthernet 196, 200
protect interface, APS/MSP 68, 85

R

redundant port, Gigabit Ethernet 168, 169
release notes xvii
remote loopback
channelized T3 interfaces 22
cOCx/STMx interfaces 140
T3 interfaces 58, 59
reversion
after switchover
APS/MSP 69
route interface command 203
RSTP (Rapid Spanning Tree Protocol) 180
Ethernet link redundancy 215, 222

S

scramble command 53
sdh command 82, 115
section layer, SONET/SDH 105
secure IP tunnels 253, 259
serial description command
channelized T3 interfaces 20
cOCx/STMx interfaces 132
E3/T3 interfaces 55
serial interfaces
configuring
channelized T3 interfaces 18
cOCx/STMx interfaces 131
E3/T3 interfaces 54
monitoring
channelized T3 interfaces 37
cOCx/STMx 160
SFPs (small form-factor pluggable transceivers) 234, 238
shared tunnel-server ports
configuring 262
overview 252
supported applications 257
supported modules 255
show aps commands
show aps 98
show aps group 99
show controllers commands
show controllers e3 60
show controllers sonet 92
show controllers sonet configuration 146
show controllers sonet ds1|e1 149
show controllers sonet ds3 151
show controllers sonet line | path | section 94
show controllers sonet line | path | section | tributary 153
show controllers t3 27, 60
show controllers t3 ft1 33
show controllers t3 remote 34, 64, 157
show controllers t3 serial 37
show displays, filtering 26, 60, 144
show interfaces commands
show interfaces fastEthernet 233
show interfaces gigabitEthernet 238
show interfaces lag 243
show interfaces lag members 245
show interfaces serial
channelized T3 interfaces 38
cOCx/STMx interfaces 160
show interfaces tenGigabitEthernet 238
show tunnel-server command 265
show vlan subinterface command 246
shutdown command
channelized T3 interfaces 9
E3/T3 interfaces 48
Ethernet interfaces 230
OCx/STMx interfaces 82
shutting down
DS3 124
E3/T3 interfaces 48
SONET/SDH interface 82
T1 channel 14, 127
T1 subchannel 14, 127
T1/E1 channel 121
T1/E1 channel group 118
T3 controller 9
SMs (Service modules)
monitoring 264
redundancy and interface distribution 257
SNAP (subnetwork attachment point) 188
SNMP (Simple Network Management Protocol) link status processing
channelized T3 interfaces 12, 14
cOCx/STMx interfaces 114, 115, 118, 119, 124, 128
OCx/STMx interfaces 81, 83
snmp trap link-status command
channelized T3 interfaces 12
cOCx/STMx interfaces 115
OCx/STMx interfaces 83
software, installing or updating xi
SONET APS 1 + 1 redundancy. *See* APS/MSP

SONET/SDH (synchronous optical network/Synchronous Digital Hierarchy)
- alarms, configuring ... 87
- line layer ... 105
- line modules supported ... 71
- MPLS fast reroute ... 79, 112
- path layer ... 105
- section layer ... 105

source, clock
- channelized T3 interfaces ... 11, 13
- E3/T3 interfaces ... 50
- OCx/STMx interfaces ... 79, 112

speed command ... 187

stacked virtual local area networks. *See* S-VLANs

static tunnel-service interfaces
- monitoring ... 264
- overview ... 253

subchannels
- configuring ... 14
- monitoring ... 33
- shutting down t1 ... 14

subnetwork attachment point. *See* SNAP

support, requesting ... xviii

svlan commands
- svlan ethertype ... 200, 204
- svlan id
  - for standard S-VLANs ... 201
  - for S-VLAN tunnels ... 204

S-VLANs (stacked virtual local area networks)
- address possibilities ... 197
- configuring PPPoE over S-VLAN ... 197
- configuring tunnel interfaces
  - advantages ... 201
  - example ... 202
  - interface stacking ... 202
- displaying status ... 236, 241
- oversubscription ... 204
- overview ... 197

switch, 802.3ad ... 229

switching mechanisms, APS/MSP ... 69, 70

switchover
- APS/MSP ... 68

Synchronous Digital Hierarchy. *See* SONET/SDH

synchronous optical network. *See* SONET/SDH

T

T1 channels
- channelized T3 interfaces ... 6
- cOCx/STMx interfaces ... 106, 116
- configuring ... 12

t1 commands
- t1 bert ... 23
- t1 clock source ... 13
- t1 description ... 13
- t1 framing ... 13
- t1 loopback ... 24
- t1 remote-loopback ... 25
- t1 shutdown ... 14
- t1 snmp trap link-status ... 14
- t1 timeslots ... 14
- t1 yellow detect ... 17
- t1 yellow generate ... 17

t1 fdl commands
- t1 fdl ... 16
- t1 fdl carrier ... 16
- t1 fdl string ... 16
- t1 fdl transmit ... 16

T1, fractional ... 106

T3 channels ... 122

T3 controllers
- configuring ... 8
- monitoring ... 26

T3 interfaces
- configuring controllers ... 47
- configuring HDLC channel ... 53
- configuring MDL ... 49
- equipment loopback command ... 58
- loopback command ... 59
- monitoring ... 59
- numbering scheme ... 46
- testing ... 139

T3, fractional ... 52

technical support, requesting ... xviii

testing interfaces
- channelized T3 ... 20, 25
- cOCx/STMx ... 136, 143
- OCx/STMx ... 89, 90

text and syntax conventions defined ... xiii

threshold command ... 84, 87

time intervals ... 26, 60

transmit clock source, configuring
- channelized T3 interfaces ... 11, 13
- cOCx/STMx interfaces ... 118, 126
- E3/T3 interfaces ... 50
- OCx/STMx interfaces ... 79, 112

transmit powers and cable length ... 11, 50

tributary unit. *See* TU

trigger delay command ... 83, 115

TU (tributary unit) ... 106

tunnels
- configuring tunnel-service interfaces ... 262
- dedicated tunnel-server ports ... 252
- dynamic tunnel-server ports ... 255
- monitoring ... 264
- secure IP ... 253, 259

tunnel-server ports
- dedicated ... 252
- shared ... 252

tunnel-service interfaces
configuring ... 262
considerations ... 260
E120 and E320 routers ... 254
monitoring ... 264
overview ... 253
redundancy and interface distribution ... 257, 258

U
unframed E1 ... 106

V
virtual local area networks. *See* VLANs
virtual path identifier. *See* VPI
virtual tributary. *See* VT
vlan commands
encapsulation vlan ... 196
monitor vlan interface ... 232
vlan id ... 197
VLANs (virtual local area networks)
configuring ... 189
displaying status ... 236, 241
monitoring ... 230
overview ... 187
VPI (virtual path identifier) ... 188
VT (virtual tributary) ... 106

W
working interface, APS/MSP ... 68, 83

X
XFPs (10-gigabit small form-factor pluggable transceivers) ... 177, 238