JUNOSe™ Software
for E-series™ Routing Platforms

System Basics Configuration Guide

Release 9.1.x

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

Part Number: 162-01960-00, Revision A00

JUNOSe™ Software for E-series™ Routing Platforms System Basics Configuration Guide, Release 9.1.x
Writing: Mark Barnard, Diane Florio, Bruce Gillham, Sarah Lesway-Ball, Brian Wesley Simmons, Fran Singer
Editing: Ben Mann, Fran Mues
Illustration: John Borelli, Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
18 April 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 xix

Objectives ... xix
Audience ... xix
E-series Routers ... xx
Documentation Conventions ... xx
Related E-series and JUNOSe Documentation ... xxii
E-series and JUNOSe Documents ... xxii
JUNOSe Configuration Guides ... xxv
Obtaining Documentation ... xxv
Documentation Feedback ... xxvi
Requesting Technical Support ... xxvi
Self-Help Online Tools and Resources ... xxvi
Opening a Case with JTAC ... xxvii

Chapter 1 Planning Your Network 1

Platform Considerations ... 2
Interface Specifiers ... 2
Edge Applications Overview ... 2
Private Line Aggregation ... 3
xDSL Session Termination ... 4
Layered Approach ... 5
Line Modules, I/O Modules, and IOAs ... 6
Interfaces ... 6
Subinterfaces ... 7
interface Command ... 7
General Configuration Tasks ... 7
Configuring Virtual Routers ... 8
Configuring IPSec ... 9
Configuring Physical Layer Interfaces ... 9
Line Module Features ... 10
Configurable HDLC Parameters ... 11
Configuring Channelized T3 Interfaces ... 11
Configuring T3 and E3 Interfaces ... 12
Configuring OCx/STMx and OC48 Interfaces ... 13
Configuring Channelized OCx/STMx Line Interfaces ... 13
Configuring Ethernet Interfaces ... 14
Configuring IPSec-Service Interfaces ... 15
Configuring Tunnel Service Interfaces ... 15
Configuring Data Link-Layer Interfaces ... 15
Configuring IP/Frame Relay ... 16
Configuring IP/ATM ... 17
Configuring IP/PPP ... 20

Configuring IP/HDLC 21
Configuring IP/Ethernet 22
Configuring IP Tunnels, Shared IP Interfaces, and Subscriber Interfaces 22
Configuring IP Tunnels 22
Configuring Shared Interfaces and Subscriber Interfaces 22
Configuring Routing Protocols 23
Configuring VRRP 24
Configuring Routing Policy 24
Configuring QoS 25
Configuring Policy Management 25
Configuring Remote Access 26

Chapter 2 Command-Line Interface 27

Overview 27
Command Modes 28
Command-Line Prompts 30
Keywords and Parameters 30
Keywords 30
Parameters 30
Keywords and Parameters Together 31
Using CLI Commands 32
Abbreviated Commands 32
The ? Key 32
Backspace or Delete 33
Enter 33
Tab 33
Arrow Keys 33
The no Version 33
run and do Commands 34
show Commands 36
Redirection of **show** Command Output 40
Regular Expressions 40
The - -More- - Prompt 41
Responding to Prompts 45
CLI Status Indicators 45
Levels of Access 46
User Level 46
Privileged Level 46
Initialization Sequence 46
Platform Considerations 47
Accessing the CLI 47
Logging In 47
Privileged-Level Access 48
Defining CLI Levels of Privilege 48
Accessing the Privileged Exec Level 48
Moving from Privileged Exec to User Exec Mode 49
Logging Out 50
CLI Command Privileges 50
CLI Privilege Groups 50
Examples Using Privilege Group Membership 51
CLI Command Exceptions 55
CLI Keyword Mapping 56
Setting Privileges for Ambiguous Commands 56
Setting Privilege Levels for no or default Versions 57

Setting Privilege Levels for Multiple Commands 57
Setting Privilege Levels for All Commands in a Mode 57
Setting Privilege Levels for a Group of Commands 57
Using the Order of Precedence 58
Superseding Privilege Levels with the all Keyword 58
Removing the all Keyword 59
Setting Default Line Privilege 59
Viewing CLI Privilege Information 60
Viewing the Current User Privilege Level 60
Viewing Privilege Levels for All Connected Users 60
Viewing Privilege Levels for Changed CLI Commands 61
Using Help 61
? (Question Mark Key) 62
help Command 64
Partial-keyword <Tab> 64
Using Command-Line Editing 65
Basic Editing 65
Command-Line Editing Keys 65
Command History Keys 66
Pagination Keys 67
Accessing Command Modes 67
Exec Modes 76
Password Protection 77
Global Configuration Mode 78
Executing a Script File 78
AAA Profile Configuration Mode 79
Address Family Configuration Mode 79
ATM VC Configuration Mode 80
ATM VC Class Configuration Mode 80
Classifier Group Configuration Mode 81
Color Mark Profile Configuration Mode 81
Control Plane Configuration Mode 82
Controller Configuration Mode 82
DHCP Local Pool Configuration Mode 83
Domain Map Configuration Mode 83
Domain Map Tunnel Configuration Mode 84
DoS Protection Group Configuration Mode 84
Drop Profile Configuration Mode 85
Explicit Path Configuration Mode 85
Flow Cache Configuration Mode 86
Interface Configuration Mode 86
IP NAT Pool Configuration Mode 87
IP PIM Data MDT Configuration Mode 87
IP Service Profile Configuration Mode 88
IPSec CA Identity Configuration Mode 88
IPSec Identity Configuration Mode 89
IPSec IKE Policy Configuration Mode 89
IPSec Manual Key Configuration Mode 90
IPSec Peer Public Key Configuration Mode 90
IPSec Transport Profile Configuration Mode 91
IPSec Tunnel Profile Configuration Mode 91
IP Tunnel Destination Profile Mode 92
L2 Transport Load-Balancing-Circuit Configuration Mode 92
L2TP Destination Profile Configuration Mode 93

L2TP Destination Profile Host Configuration Mode 93
L2TP Tunnel Switch Profile Configuration Mode 94
Layer 2 Control Configuration Mode 94
Layer 2 Control Neighbor Configuration Mode 95
LDP Configuration Mode 95
Line Configuration Mode 95
Local IPSec Transport Profile Configuration 96
Local User Configuration Mode 96
Map Class Configuration Mode 97
Map List Configuration Mode 97
Parent Group Configuration Mode 98
Policy List Configuration Mode 98
Policy List Parent Group Configuration Mode 99
Policy Parameter Configuration Mode 99
PPPoE Service Name Table Configuration Mode 99
Profile Configuration Mode 100
QoS Parameter Definition Configuration Mode 100
QoS Profile Configuration Mode 101
QoS Shared Shaper Control Configuration 101
Queue Profile Configuration Mode 102
RADIUS Configuration Mode 102
RADIUS Relay Configuration Mode 103
Rate Limit Profile Configuration Mode 103
Redundancy Configuration Mode 104
Remote Neighbor Configuration Mode 104
Route Map Configuration Mode 105
Router Configuration Mode 105
RSVP Configuration Mode 106
RTR Configuration Mode 106
Scheduler Profile Configuration Mode 107
Service Session Profile Configuration Mode 107
SNMP Event Manager Configuration Mode 108
Statistics Profile Configuration Mode 108
Subinterface Configuration Mode 108
Subscriber Policy Configuration Mode 109
Traffic Class Configuration Mode 109
Traffic Class Group Configuration Mode 110
Tunnel Group Configuration Mode 110
Tunnel Group Tunnel Configuration Mode 110
Tunnel Profile Configuration Mode 111
Tunnel Server Configuration Mode 111
VRF Configuration Mode 112
VR Group Configuration Mode 112

Chapter 3 Installing JUNOSe Software 113

Overview 113
Identifying the Software Release File 114
Platform Considerations 115
Installing Software When a Firewall Exists 115
Task 1: Obtain the Required Information 115
Task 2: Divert Network Traffic to Another Router 116
Task 3: Access Privileged Exec Mode 116
Task 4: Configure IP on an Interface 116
Task 5: Copy the Release Files to the Network Host 117

Task 6: Configure Access to the Network Host 117
Task 7: Enable the FTP Server on the Router 118
Task 8: Identify the Files to Transfer 118
Task 9: Transfer Files to the User Space 119
Task 10: Install Files on the System Space 119
Task 11: Save the Current Configuration 119
Task 12: Reboot the System 119
Installing Software When a Firewall Does Not Exist 120
Installing Software in Normal Operational Mode 120
Task 1: Obtain the Required Information 121
Task 2: Divert Network Traffic to Another Router 121
Task 3: Access Privileged Exec Mode 121
Task 4: Configure IP on an Interface 122
Task 5: Configure Access to the Network Host 123
Task 6: Copy the Release Files to the Network Host 124
Task 7: Copy the Software Release File to the Router 124
Task 8: Save the Current Configuration 124
Task 9: Reboot the System 124
Installing Software in Boot Mode 125
Task 1: Obtain the Required Information 125
Task 2: Divert Network Traffic to Another System 126
Task 3: Access the Boot Mode 126
Task 4: Assign an IP Address 126
Task 5: Configure Access to the Network Host 126
Task 6: Resetting the SRP Module 127
Task 7: Copy the Release Files to the Network Host 127
Task 8: Copy the Software Release File to the Router 127
Task 9: Reboot the System 127
Copying Release Files from One Router to Another 128
Upgrading Systems That Are Operating with Two SRP Modules 129
Upgrading from Release 5.1.1 or Lower-Numbered Releases 130
Upgrading Software Remotely Through Telnet or FTP 131
Upgrading Software from an NVS Card 131
Upgrading a System That Contains One SRP Module 132
Upgrading a System That Contains Two SRP Modules 132
Downgrading JUNOSe Software 133

Chapter 4 Configuring SNMP 135

Overview 135
Terminology 136
SNMP Features Supported 137
SNMP Client 137
SNMP Server 138
SNMP MIBs 138
Standard SNMP MIBs 138
Juniper Networks E-series Enterprise MIBs 138
Accessing Supported SNMP MIBs 138
SNMP Versions 138
Security Features 139
Management Features 140
Virtual Routers 141
Creating SNMP Proxy 141
Disabling and Reenabling SNMP Proxy 142

Communicating with the SNMP Engine 142
SNMP Attributes 143
SNMP Operations 143
SNMP PDU Types 144
Platform Considerations 144
References 144
Before You Configure SNMP 145
SNMP Configuration Tasks 145
Enabling SNMP 146
Configuring SNMP v1/v2c Community 147
Community Name 147
Privilege Levels 147
IP Access List 147
Configuring SNMPv3 Users 148
Configuring SNMP Dynamic Groups and Views 148
Setting Server Parameters 149
Configuring SNMP Packet Size 149
Configuring Memory Warning 149
Configuring Encoding Method 150
Managing Interface Sublayers 150
Compressing Interfaces 151
Controlling Interface Numbering 152
Monitoring Interface Tables 153
Configuring Traps 153
IP Hosts 154
Trap Categories 154
Trap Severity Levels 156
Specifying an Egress Point for SNMP Traps 158
Configuring Trap Queues 159
Configuring Trap Notification Logs 159
Recovering Lost Traps 161
Configuring the SNMP Server Event Manager 162
Event MIB Purpose 162
Event MIB Structure 162
Trigger Table 162
Objects Table 163
Event Table 163
Configuration Tasks 164
Defining a Boolean Test 166
Defining an Existence Test 167
Defining a Threshold Test 168
Monitoring Events 173
Collecting Bulk Statistics 178
Interface Strings 179
Understanding Counter Discontinuity 181
Configuring Collectors and Receivers 182
Deleting All Bulkstats Configurations 187
Monitoring Collection Statistics 187
Configuring Schemas 197
igmp Objects 197
if-stats Objects 198
policy Objects 199
Monitoring Schema Statistics 201
Configuring Interface Numbering Mode 202

Using the Bulk Statistics Formatter 203
Setting Remote Filenames 203
Guidelines 203
Specifying End of Line Format 204
Managing Virtual Routers 204
Monitoring SNMP 204
Establishing a Baseline 204
Viewing SNMP Status 205
Output Filtering 213

Chapter 5 Managing the System 215

Overview 216
Platform Considerations 216
Naming the System 217
Configuring the Switch Fabric Bandwidth 217
Configuring Timing 217
Monitoring Timing 219
Using the CLI 219
Managing vty Lines 222
Configuring vty Lines 222
Monitoring vty Lines 224
Clearing Lines 224
Monitoring the Current Configuration 225
Defining the Configuration Output Format 225
Customizing the Configuration Output 230
Configuring the System Automatically 234
Saving the Current Configuration 235
Customizing the User Interface 237
Setting the Console Speed 237
Configuring the Display Terminal 238
Specifying the Character Set 238
Configuring Login Conditions 239
Setting Time Limits for User Login 240
Setting Time Limits for User Input 240
Configuring CLI Messages 241
Monitoring the Console Settings 243
Sending Messages 244
Managing Memory 245
Managing Files 245
Managing the User Space from a Network Host 247
File Commands and FTP Servers 247
Renaming Files 248
Deleting Files 249
Monitoring Files 251
Viewing Files 254
Transferring Files 254
References 255
Copying and Redirecting Files 255
Using the copy Command 257
copy Command Examples 260
Using TFTP to Transfer Files 262
Configuring the FTP Server 262
Features 262
FTP Passive Mode 263

Configuring Authentication 263
Configuration Tasks 263
Configuration Example 264
Monitoring the FTP Server 265
Copying Partial Releases 266
Configuring the NFS Client 269
References 269
Prerequisites 269
Configuration Tasks 269
Monitoring the NFS Client 270
Using a Loopback Interface 271
Using the Telnet Client 271
Configuring DNS 272
References 273
Assigning Name Servers 273
Using One Name Resolver for Multiple Virtual Routers 274
Monitoring DNS 275
Troubleshooting the System 275
Creating Core Dump Files 276
Boot Mode 276
Global Configuration Mode 276
Managing Core Dump Files 279
Enabling and Disabling the Core Dump Monitor 279
Specifying the Core Dump Monitor Interval 280
Viewing Core Dump Monitor Status 280
Accessing the Core Dump File 281
Capturing and Writing Core Dumps 282
Understanding the Core Dump File 283
Tracking IP Prefix Reachability 284
Gathering Information for Customer Support 285
Managing and Monitoring Resources 286
Enabling and Disabling the Resource Threshold Monitor 286
Viewing Resource Threshold Information 287
Monitoring the System 288

Chapter 6 Managing Modules 305

Overview 306
Platform Considerations 306
ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router 306
Line Modules and I/O Modules 306
SRP Modules 307
E120 Router and E320 Router 307
Line Modules and IOAs 307
SRP Modules and SFMs 309
Disabling and Reenabling Line Modules, SRP Modules, and SFMs 310
Disabling and Reenabling IOAs 311
Removing an SRP Module 313
Replacing Line Modules on ERX Routers, the E120 Router, and the E320 Router 314
Replacing a Line Module by Erasing the Slot Configuration 314
Replacing a Line Module Without Erasing the Slot Configuration 315
Replacing IOAs on the E120 Router and the E320 Router 317
Replacing SRP Modules and SFMs 317

Software Compatibility....321
Line Modules....321
I/O Modules and IOAs....321
Configuring Performance Rate of Line Modules on ERX-7xx Models and the ERX-1410 Router....322
Choosing a Combination of Line Modules....322
Slot Groups....322
SRP Modules Bandwidth....323
Line Modules Bandwidth and Switch Usage....323
Allowed Combinations for Line Rate Performance....323
Specifying the Type of Performance....325
Monitoring Bandwidth Oversubscription....325
Troubleshooting Bandwidth Oversubscription....326
Line Module Redundancy....327
Module Requirements....327
ERX-7xx Models and ERX-14xx Models....327
E120 Router and E320 Router....327
Automatic Switchover....328
Limitations of Automatic Switchover....328
Reversion after Switchover....329
Configuring Line Module Redundancy....329
Managing Line Module Redundancy....330
SRP Module Redundancy....330
SRP Module Behavior....331
Specifying the Configuration for Redundant SRP Modules....333
Installing a Redundant SRP Module....333
Managing SRP Module Redundancy....335
Switching to the Redundant SRP Module....336
Upgrading Software on a Redundant SRP Module....337
Monitoring the Status LEDs....337
Monitoring Line Module and SRP Module Redundancy....338
Managing Flash Cards on SRP Modules....341
Flash Features....341
Flash Features on the E120 Router and the E320 Router....342
Installing and Removing Flash Cards....343
Synchronizing Flash Cards....344
Synchronizing Flash Cards of Different Capacities....345
Disabling Autosynchronization....346
Validating and Recovering Redundant SRP File Integrity....347
Reformatting the Primary Flash Card....350
Copying the Image on the Primary SRP Module....351
Scanning Flash Cards....352
Monitoring Flash Cards....354
Updating the Router with JUNOSe Hotfix Files....355
Hotfix Compatibility and Dependency....356
Removing Hotfixes....357
Hotfixes and Backup Settings....357
Hotfixes and Standby SRP Modules....357
Hotfixes and Line Modules....357
Monitoring Hotfixes....360
Example: Using and Monitoring Hotfixes....363
Managing the Ethernet Port on the SRP Module....365
Monitoring Statistics....366
Monitoring the Ethernet Configuration for the SRP Module....366

Enabling Warm Restart Diagnostics on Modules 367
Enabling Warm Restart Diagnostics 368
Monitoring Modules 369

Chapter 7 Managing High Availability 377

Understanding High Availability 377
Platform Considerations 378
Module Requirements 378
Redundancy Modes of Operation 379
File System Synchronization Mode 379
High Availability Mode 379
Understanding SRP State Behavior 381
Disabled State 381
Initializing State 382
Active State 383
Pending State 383
Application Support 384
Before Activating High Availability 389
Activating High Availability 389
Deactivating High Availability 390
Upgrading Software 391
Monitoring High Availability 391
High Availability show Commands 391
Clearing the Redundancy History 399

Chapter 8 Configuring a Unified In-Service Software Upgrade 401

Unified ISSU Overview 401
Router Behavior During a Unified In-Service Software Upgrade 402
Unified ISSU Platform Considerations 403
Unified ISSU Terms That Describe SRP and Line Module Behavior 403
Unified ISSU References 404
Unified ISSU Phases Overview 404
Unified ISSU Initialization Phase Overview 405
Application Data Upgrade on the Standby SRP Module 406
Line Module Arming 406
SNMP Traps 406
Unified ISSU Upgrade Phase Overview 407
Exceptions During the Upgrade Phase 408
Verification of Requirements 409
Upgrade Setup 409
Unified ISSU Service Restoration Phase Overview 411
Application Support for Unified ISSU 412
Unexpected Application-Specific Behavior During Unified ISSU 418
AAA Authentication and Authorization Disabled 418
ATM Affected Behaviors 418
ILMI Sessions Not Maintained 419
OAM CC Effects on VCC 419
OAM VC Integrity Verification Cessation 419
Port Data Rate Monitoring Cessation 419
VC and VP Statistics Monitoring Halts Unified ISSU Progress 419
DHCP Affected Behaviors 419
DHCP Common Component Information Suspended 419
DHCP External Server Prevents Unified ISSU Operation 420

DHCP Relay and DHCP Relay Proxy Prevent Unified ISSU 420
DHCP Packet Capture Halted on Line Modules 420
DoS Protection State Freeze 420
Ethernet Affected Behaviors 420
ARP Packets Briefly Not Sent or Received 420
Link Aggregation interruption 421
Port Data Rate Monitoring Halted 421
VLAN Statistics Monitoring Halts Unified ISSU Progress 421
FTP Server File Transfers Halted 421
IS-IS Effects on Graceful Restart and Network Stability 421
Configuring Graceful Restart Before Unified ISSU Begins 421
Configuring Graceful Restart When BGP And LDP are Configured 422
Routing Around the Restarting Router to Minimize Network Instability 422
L2TP Failover of Established Tunnels 423
OSPF Effects on Graceful Restart, Timeouts, and Network Stability 423
Configuring Graceful Restart Before Unified ISSU Begins 424
Configuring Graceful Restart When BGP And LDP are Configured 424
Configuring a Longer Dead Interval Than Normal 424
Routing Around the Restarting Router to Minimize Network Instability 424
PIM Suspended During Unified ISSU 425
Subscriber Logins and Logouts Suspended During Unified ISSU 426
Subscriber Statistics Accumulation or Deletion 426
SONET/SDH Behavior During Unified ISSU 426
TACACS+ Services Not Available 427
Interruption in Traffic Forwarding for Layer 3 Routing and Signaling Protocols 427
Recommended Routing Protocol Timer Settings 429
Before You Begin a Unified In-Service Software Upgrade 430
Hardware Requirements for Unified ISSU 430
Software Requirements for Unified ISSU 431
Upgrading Router Software with Unified ISSU 432
Halting the Unified ISSU Process and Restoring the Original State of the Router 435
Halting Unified ISSU During Initialization Phase 435
Halting Unified ISSU During Upgrade Phase 436
Monitoring a Unified In-Service Software Upgrade 437

Chapter 9 Passwords and Security 441

Overview 441
Platform Considerations 442
Setting Basic Password Parameters 442
Creating Encrypted Passwords 442
Creating Secrets 443
Encrypting Passwords in Configuration File 443
Commands and Guidelines 444
Setting and Erasing Passwords 445
Privilege Levels 445
Accessing Privilege Levels 446
Setting Enable Passwords 446
Erasing Enable Passwords 446
Setting a Console Password 448

Erasing the Console Password 450
Monitoring Passwords 450
Vty Line Authentication and Authorization 451
Configuring Simple Authentication 451
Configuring AAA Authentication and AAA Authorization 454
Virtual Terminal Access Lists 458
Secure System Administration with SSH 459
Transport 460
User Authentication 460
Connection 460
Key Management 461
User Key Management 461
Host Key Management 461
Performance 462
Security Concerns 462
Before You Configure SSH 462
SSH Configuration Tasks 463
Configuring Encryption 463
Configuring User Authentication 464
Configuring Message Authentication 466
Enabling and Disabling SSH 467
Displaying SSH Status 467
Terminating an SSH Session 468
Restricting User Access 469
Restricting Access to Commands with RADIUS 469
Per-User Enable Authentication 470
Restricting Access to Virtual Routers 470
VSA Configuration Examples 471
Commands Available to Users 472
Denial of Service (DoS) Protection 473
Suspicious Control Flow Detection 475
Suspicious Control Flow Monitoring 475
Configurable Options 476
Display Options 477
Traps and Logs 477
Suspicious Control Flow Commands 477
Monitoring Suspicious Control Flow 479
Denial-of-Service Protection Groups 484
Group Parameters 484
Attaching Groups 485
Protocol Mapping 486
DoS Protection Group Configuration Example 488
DoS Protection Group Commands 489
Monitoring DoS Protection Groups 493

Chapter 10 Writing CLI Macros 495

Platform Considerations 495
Writing Macros 495
Environment Commands 497
Variables 497
Literals 498
Operators 498
Assignment 500
Increment and Decrement 500

String Operations 501
Extraction Operations 501
Arithmetic Operations 502
Relational Operations 502
Logical Operations 502
Miscellaneous Operations 503
Conditional Execution 503
If Constructs 503
While Constructs 505
Passing Parameters in Macros 506
Generating Macro Output 506
Invoking Other Macros 507
Detecting and Recording Macro Errors 509
Detectable Macro Errors 509
Logging Macro Results 509
Viewing Macro Errors 510
onError Macro Examples 510
Detecting Invalid Command Formats 511
Detecting Invalid Commands 512
Detecting Missing Macros 513
Running Macros 514
Practical Examples 516
Configuring Frame Relay 517
Configuring ATM Interfaces 520

Chapter 11 Booting the System 523

Platform Considerations 523
Configuring Your System for Booting 523
Booting the GE-2 Line Module 524
Rebooting Your System 528
Rebooting When a Command Takes a Prolonged Time to Execute 530
Configuration Caching 530
Operations in Boot Mode 531
Displaying Boot Information 531
Output Filtering 533

Chapter 12 Configuring the System Clock 535

Overview 535
NTP 535
System Operation as an NTP Client 536
Synchronization 537
System Operation as an NTP Server 538
Platform Considerations 538
References 539
Setting the System Clock Manually 539
Before You Configure NTP 541
Choosing NTP Servers 541
NTP Configuration Tasks 541
Enabling NTP Services 541
NTP Client Configuration 542
Directing Responses from NTP Servers 543
Refusing Broadcasts from NTP Servers 544

NTP Server Configuration 545
Configuration Examples 546
Monitoring NTP 547

Chapter 13 Configuring Virtual Routers 553

Overview 553
Default Virtual Router 553
Virtual Router Instances 554
Routing Protocols 554
VPNs and VRFs 554
VPNs 554
VRFs 555
Platform Considerations 555
References 555
Configuring Virtual Routers 555
Monitoring Virtual Routers 560

Appendix A Abbreviations and Acronyms 563

Appendix B References 577

RFCs 578
Draft RFCs 586
Other Software Standards 588
Hardware Standards 590

Index 593

About This Guide

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

- Objectives on page xix
- Audience on page xix
- E-series Routers on page xx
- Documentation Conventions on page xx
- Related E-series and JUNOSe Documentation on page xxii
- Obtaining Documentation on page xxv
- Documentation Feedback on page xxvi
- Requesting Technical Support on page xxvi

Objectives

This guide provides general information you will need to manage your router. It covers basic tasks such as configuring passwords, security, the router clock, and virtual 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.
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.

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

Document	Description
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
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)

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

Document	Description
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.
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 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

Planning Your Network

This chapter describes planning steps that will make it easier to configure the physical interfaces, logical interfaces, and routing protocols for the E-series routers in:

- A new network that you are creating and implementing
- An existing network that you are expanding

This chapter contains the following sections:

- Platform Considerations on page 2
- Edge Applications Overview on page 2
- Layered Approach on page 5
- Line Modules, I/O Modules, and IOAs on page 6
- Interfaces on page 6
- General Configuration Tasks on page 7
- Configuring Virtual Routers on page 8
- Configuring IPSec on page 9
- Configuring Physical Layer Interfaces on page 9
- Configuring Data Link-Layer Interfaces on page 15
- Configuring IP Tunnels, Shared IP Interfaces, and Subscriber Interfaces on page 22
- Configuring Routing Protocols on page 23
- Configuring VRRP on page 24
- Configuring Routing Policy on page 24

- Configuring QoS on page 25
- Configuring Policy Management on page 25
- Configuring Remote Access on page 26

Platform Considerations

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Interface Specifiers

The configuration task examples in this chapter use the *slot*/*port* format to specify an interface. However, the interface specifier format that you use depends on the router that you are using.

For ERX-7xx models, ERX-14xx models, and ERX-310 routers, use the *slot*/*port* format. For example, the following command specifies an ATM interface on slot 0, port 1 of an ERX-7xx model, ERX-14xx model, or ERX-310 router.

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

For E120 and E320 routers, use the *slot*/*adapter*/*port* format, which includes an identifier for the bay in which the I/O adapter (IOA) resides. 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). For example, the following command specifies an ATM interface on slot 5, adapter 0, port 0 of an E320 router.

host1(config)**#interface atm 5/0/0**

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

Edge Applications Overview

The E-series router can be used for a number of edge aggregation applications. Two of the most common are:

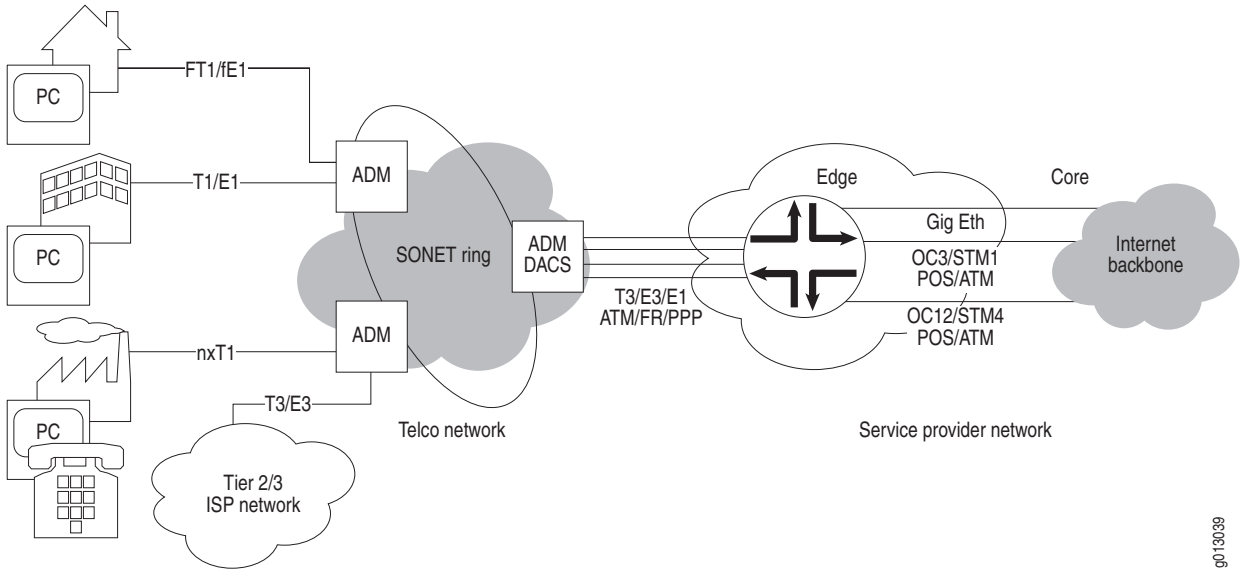
- Private line aggregation
- xDSL session termination

Private Line Aggregation

A major application of the E-series router is for private line aggregation—the consolidation of multiple high-speed access lines into one access point. See Figure 1 on page 3.

In this application, the service provider can use a single router to offer high-speed access (FT1/FE1 through T3/E3) to thousands of subscribers. The individual subscriber lines can be multiplexed into T3 lines by the service provider and fed into the router. (The router can also accept unchannelized T3 or E3 connections from high-speed users and channelized E1 connections directly into the unit.) Once the traffic is received, the router then handles all IP packet processing, including the assignment of QoS and routing policies. The packets are then routed into the backbone network.

Figure 1: Private Line Aggregation with the E-series Router



The router supports a number of access and uplink methods; the most common pairings are listed in Table 4.

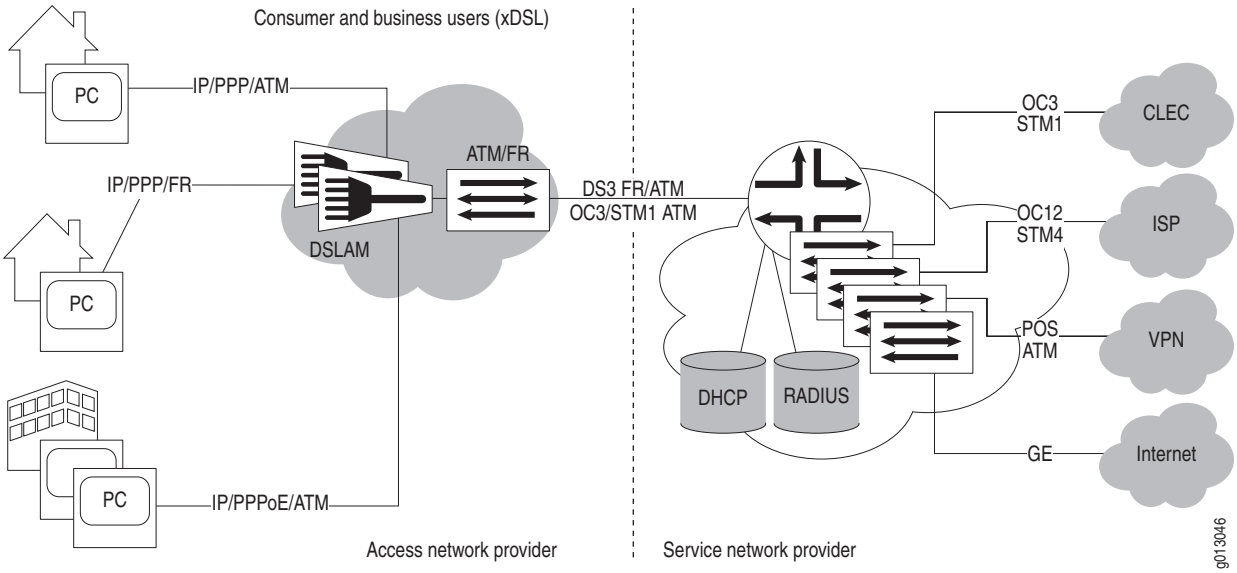
Table 4: Common Access/Uplink Pairings

Access	Uplink
PPP	ATM, Fast Ethernet, Gigabit Ethernet, or POS
Frame Relay	
ATM	

xDSL Session Termination

The router supports Broadband Remote Access Server (B-RAS) applications, as shown in Figure 2 on page 4. In this application, the router handles the aggregated output from the digital subscriber line access multiplexers (DSLAMs). Directly connected to the subscriber premises, the DSLAMs handle the copper termination and aggregate the traffic into a higher-speed uplink. The output from the DSLAM is fed into the router through a DS3 or OC3 link.

Figure 2: B-RAS Application



The router then performs several functions:

- PPP session termination and authentication checking through PAP or CHAP
- Coordination with DHCP servers and local IP pools to assign IP addresses
- Connection to RADIUS servers or use of domain names to associate subscribers with user profile information
- Support for RADIUS accounting to gather detailed billing information
- Application of the user profile to the user traffic flow, which could include QoS, VPN, and routing profiles

The output of the router is typically a high-speed link, such as OC3/STM1 to feed a core backbone router. Virtual routers can also be used to keep the traffic logically separate and to direct packets to different destinations. As shown in Figure 2, the packets can be directed to a CLEC, ISP, corporate VPN, or the Internet.

A large number of xDSL protocols are supported, including:

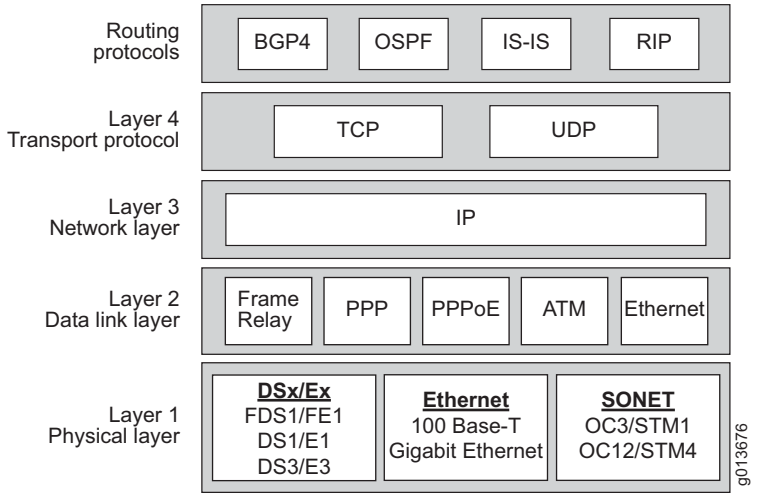
- IP/PPP/ATM
- IP/PPP/Ethernet/ATM
- IP/bridged Ethernet/ATM

See *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access*, for information about configuring B-RAS.

Layered Approach

The JUNOSe CLI enables you to configure your network based on the hierarchy of the OSI model. Therefore, the JUNOSe configuration guides use a bottom-up approach to describe the configuration process. Figure 3 shows the relationship of layers, protocols, and interfaces to the configuration process. Software functions are layered on top of physical (copper or optical) interfaces. The router supports a number of access protocols (PPP/POS, Frame Relay, ATM) that allow service providers to offer a number of access methods and line speeds to their subscribers. The router is optimized to handle IP connections regardless of the access protocol used. The router also supports a number of protocols that are specific to the B-RAS application. These are shown in Figure 3, and include IP/PPP/ATM and IP/PPP/Ethernet/ATM.

Figure 3: Network Configuration Using a Bottom-Up Approach



Layer 2 (data link) defines how the data is packaged and sent to an IP data connection point in layer 3 (IP interfaces). In layer 3, you define the global attributes for IP services that serve as a platform from which you add routing information.

Line Modules, I/O Modules, and IOAs

A range of line modules, I/O modules, and I/O adapters (IOAs) are available for the router. On the ERX-14xx models, ERX-7xx models, and the ERX-310 router, most line modules pair with a corresponding I/O module. On the E120 router and the E320 router, a single line module pairs with all available IOAs.

I/O modules and IOAs provide the input and output connections from the network to the router. Line modules connect to their corresponding I/O modules or IOAs through a passive midplane. A line module receives packets through its I/O module or IOA and processes those packets. The router then routes the packets out to the network through the designated I/O module or IOA.

Each line module, I/O module, and IOA has a label on its faceplate. In this documentation, these modules are identified by that label. For example, the high-density Gigabit Ethernet line module has two ports, and is called the GE-HDE line module. Its corresponding I/O modules are the GE-HDE I/O module and the GE-2 SFP I/O module.

When we refer to a related set of line modules, I/O modules, or IOAs, the generic information from the module labels is used in this documentation. For example, the term “OCx/STMx line modules” refers to both the OCx/STMx ATM and the OCx/STMx POS line modules. Similarly, the term “GE I/O modules” refers to both the GE Multimode I/O module and the GE Single Mode I/O module.

For a complete list of the line modules and I/O modules available for ERX-14xx models, ERX-7xx models, and the ERX-310 router, see *ERX Module Guide, Table 1, Module Combinations*. For more information about line modules and IOAs available with the E120 and E320 routers, see *E120 and E320 Module Guide, Table 1, Modules and IOAs*.

For more information about managing these modules, see *Chapter 6, Managing Modules*.

Interfaces

The term *interfaces* is used in a very specific way in the JUNOSe CLI and this documentation. Interfaces are both physical and logical channels on the router that define how data is transmitted to and received from lower layers in the protocol stack. Conceptually, you configure an interface as part of the physical layer, layer 1.

For example, you can configure the physical and logical characteristics of T3 and T1 lines coming directly from the customer premises or from a central office switch and OC3 lines going out to the core of your network infrastructure. These physical and logical characteristics define an interface.

Interface layering must always be configured in order from the lowest layer to the highest layer. For example, if you have already configured IP to run over ATM and you want to reconfigure the interface to run IP over PPP over ATM, you must first remove the IP interface, apply PPP, and then reapply IP.

Subinterfaces

A subinterface is a mechanism that allows a single physical interface to support multiple logical interfaces or networks. Several logical interfaces or networks can be associated with a single physical interface. Configuring multiple virtual interfaces, or subinterfaces, on a single physical interface allows greater flexibility and connectivity on the network.

Protocols such as Frame Relay and ATM require that you create one or more virtual circuits over which your data traffic is transmitted to higher layers in the protocol stack. The router requires that you define a subinterface on top of a physical interface as a platform for a virtual circuit, such as a permanent virtual circuit (PVC).

Once you have defined the underlying characteristics of an interface, use the **interface** command to:

1. Assign an *interface type*, such as POS or ATM.
2. Assign the associated *interface specifier* to the interface, such as the *slot/port* or *slot/adapter/port* and *channel/subchannel*.
3. Assign one or more subinterfaces.

interface Command

The **interface** command has the following format:

interface *interfaceType interfaceSpecifier*

Each interface type has an interface specifier associated with it. The interface specifier identifies the physical location of the interface on the router, such as the chassis slot and port number, and logical interface information, such as a T1 channel on a channelized T3 interface.

For detailed information about interface types and specifiers and for specific syntax for the interface command, see the *JUNOSe Command Reference Guide, About This Guide*.

General Configuration Tasks

The configuration process for E-series routers involves the following general tasks:

1. Determine IP-addressing information and information about the physical and logical characteristics of the various interfaces that you want to configure.
2. Determine information about the link-layer protocols.
3. Determine how to organize virtual routers on the router.
4. Determine how IPSec will be used to provide security.
5. Determine routing information that defines all or part of the network.
6. Create the virtual routers.

7. Configure the interfaces and subinterfaces (such as channelized T3, OCx/STMx, and HDLC data channels) over which the higher-layer protocols run.

8. Configure the data link-layer protocols, such as Frame Relay, PPP, and ATM, that run over these physical interfaces.

9. Configure the general IP information from which the other routing protocols will operate.

10. Configure IP tunnels, shared interfaces, and subscriber interfaces.

11. Configure IPSec.

12. Configure the routing protocols that will run on the router, such as IP multicasting protocols, OSPF, IS-IS, RIP, BGP-4, and MPLS.

13. Configure the Virtual Router Redundancy Protocol (VRRP) on IP/Ethernet interfaces.

14. Configure QoS and policy management.

15. Configure the router for remote access.

16. Use the appropriate **show** commands to display network activity on each of the interfaces that you have configured. Do this to verify that they are operating as you expect and to help improve the management of your network.

Configuring Virtual Routers

Multiple distinct virtual routers are supported within a single router, which allows service providers to configure multiple, separate, secure routers within a single chassis. These routers are identified as *virtual routers (VRs)*. Applications for this function include the creation of individual routers dedicated to wholesale customers, corporate virtual private network (VPN) users, or a specific traffic type.

The router implements the virtual routers by maintaining a separate instance of each data structure for each virtual router and allowing each protocol to be enabled on a case-by-case basis. Virtual routers provide full support for all supported routing protocols (unicast, multicast, and MPLS).

For information about configuring virtual routers, see *Chapter 13, Configuring Virtual Routers*.

Configuring IPSec

IPSec provides security to IP flows through the use of authentication and encryption.

- Authentication verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.
- Encryption makes data confidential by making it unreadable to everyone except the sender and intended recipient.

IPSec comprises two encapsulating protocols:

- Encapsulating Security Payload (ESP) provides confidentiality and authentication functions to every data packet.
- Authentication header (AH) provides authentication to every data packet.

For information about configuring IPSec, see *JUNOSe IP Services Configuration Guide, Chapter 6, Configuring IPSec*.

Configuring Physical Layer Interfaces

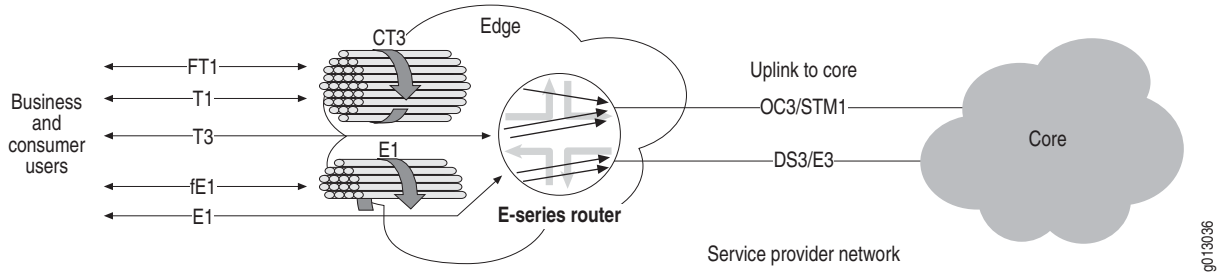
The router supports a number of line rates; some of these are listed per line module below.

- COCX-F3 line module supports unchannelized E3.
- Channelized OCx/STMx (cOCx/STMx) line module supports DS3 channelized to DS1, fractional DS1, or the DS0 level; unchannelized DS3; E1/T1 channelized to fractional DS1; unframed E1.
- CT3 12-F0 line modules support DS3 channelized to DS1, fractional DS1, or the DS0 level. CT3 12-F0 line modules also support unchannelized T3.
- IPSec Service module provides tunnel service for secure tunnels.
- GE/FE line module supports Gigabit Ethernet and Fast Ethernet.
- GE-2 line module and GE-HDE line module support Gigabit Ethernet.
- OCx/STMx ATM line module supports OC3/STM1 ATM, OC12/STM4 ATM, and unchannelized T3.
- OCx/STMx POS line module supports OC3/STM1 POS and OC12/STM4 POS.
- OC48 line module supports OC48/STM16 POS.
- OC3/STM1 GE/FE line module supports OC3/STM1 ATM and Gigabit Ethernet.
- ES2 4G line module (LM) supports OC48/STM16 POS, OC12/STM1 POS, OC3/STM1 ATM, OC12/STM1 ATM, Gigabit Ethernet, 10-Gigabit Ethernet, and tunnel-service interfaces.

- ES2 10G Uplink LM and ES2 10G LM supports 10-Gigabit Ethernet interfaces.
- COCX-F3 line module supports unchannelized T3.
- Service Module (SM) provides tunnel service for IP tunnels and LNS termination.

A variety of protocols are supported over these interfaces, including IP/Frame Relay, IP/ATM, IP/PPP, as well as the protocols to enable B-RAS services. The router's DSx and E1/E3 implementations support termination, statistics gathering, alarm surveillance, and performance monitoring. These links can be used for either network ingress or network egress.

Figure 4: E-series Router Support for Fractional T1/E1 Through T3/E3 Interfaces



As shown in Figure 4, the router can support fractional, full, and channelized interfaces.

NOTE: See *ERX Hardware Guide, Chapter 4, Installing Modules* and *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*, for a discussion of slot groups and modules. See the *ERX Module Guide* and the *E120 and E320 Module Guide,* for a discussion of the combination of line modules allowed in E-series routers.

Line Module Features

The following features are supported by the system line modules:

- Three different clocking options: internal timing, loop timing, and chassis timing
- DS3 framing type—Both M23 framing and C-bit parity
- DS1 framing type—Both D4 framing mode and ESF framing mode
- DS3 loopback—For line, payload, diagnostic, and DS1 loopbacks
- DS1 loopback—For line, payload, and diagnostic loopbacks
- DS3/DS1 line status/alarm monitoring
- DS1 line coding type—Both AMI line encoding and B8ZS line encoding
- Unique IP interface support—For each PPP or Frame Relay PVC interface

Configurable HDLC Parameters

The following HDLC parameters are configurable:

- Mapping of DS0 timeslots for T1/FT1 DS0 mapping
- Setting the speed of the DS0 to Nx56 or Nx64
- HDLC CRC checking (enable/disable)
- HDLC CRC algorithm (CRC16 or CRC32)
- Channel data inversion (enable/disable)
- Maximum receive unit (MRU)
- Maximum transmit unit (MTU)

Statistics are also gathered per line module.

Configuring Channelized T3 Interfaces

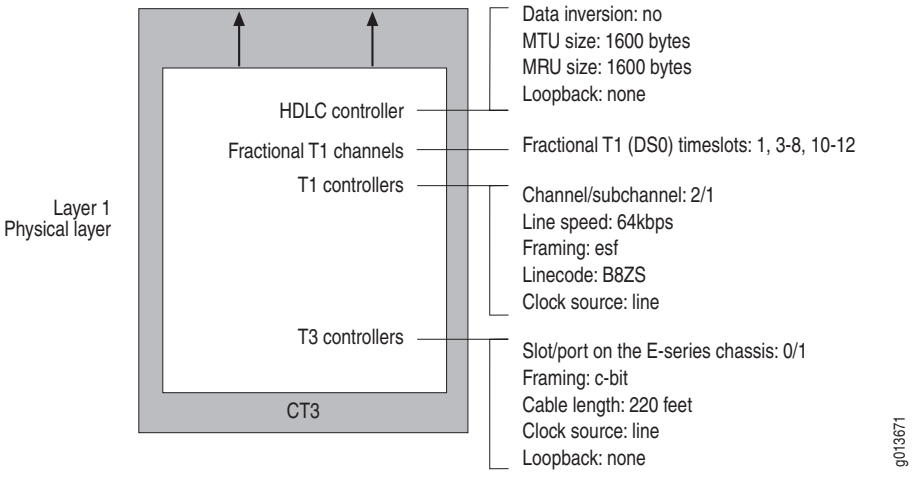
There12 T3 controllers available on each CT3 12-F0 line module. When you configure these T3 controllers, you are actually configuring T3 (DS3) lines. Each T3 controller has, by definition, 28 T1 controllers representing T1 (DS1) lines.

Use the T3 and T1 commands described in *JUNOSe Physical Layer Configuration Guide, Chapter 1, Configuring Channelized T3 Interfaces*, to:

- Specify the line characteristics, such as framing format and clock source, for T3s and associated T1s.
- Assign full and fractional T1 channels (DS0) to a virtual channel.

Figure 5 shows sample parameters for a channelized T3 interface configuration.

Figure 5: Channelized T3 Interface Configuration Parameters



The following sample command sequence configures a serial interface for a CT3 12-F0 module. See *JUNOSe Physical Layer Configuration Guide, Chapter 1, Configuring Channelized T3 Interfaces*, for details.

```
host1(config)#controller t3 0/1
host1(config-controll)#framing c-bit
host1(config-controll)#clock source line
host1(config-controll)#cablelength 220
host1(config-controll)#t1 2/1
host1(config-controll)#t1 2 framing esf
host1(config-controll)#t1 2 lineCoding b8zs
host1(config-controll)#t1 2/1 timeslots 2/1 1,3-8,10-12
host1(config-controll)#interface serial 0/1:2/1
```

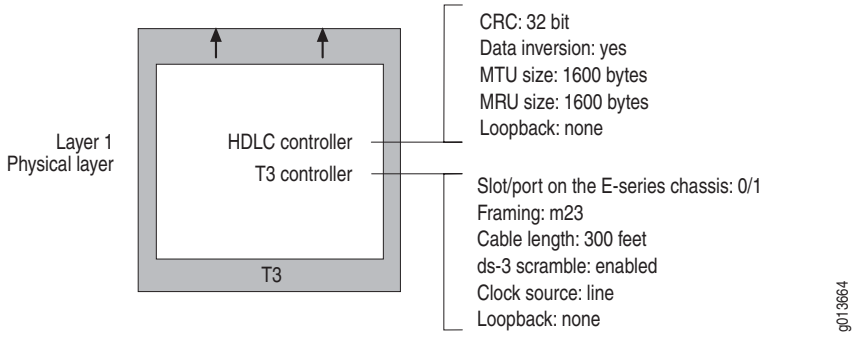
Configuring T3 and E3 Interfaces

The COCX-F3 line module supports the following wide area network (WAN) protocol encapsulations:

- IP over PPP
- IP over ATM
- IP over PPP over ATM
- IP over PPP over PPPoE over ATM
- IP over Frame Relay

Figure 6 shows sample configuration parameters for a T3 interface configuration.

Figure 6: T3 Interface Configuration Parameters



The following sample command sequence configures a serial interface for a T3 module. See *JUNOSe Physical Layer Configuration Guide, Chapter 2, Configuring T3 and E3 Interfaces*, for details.

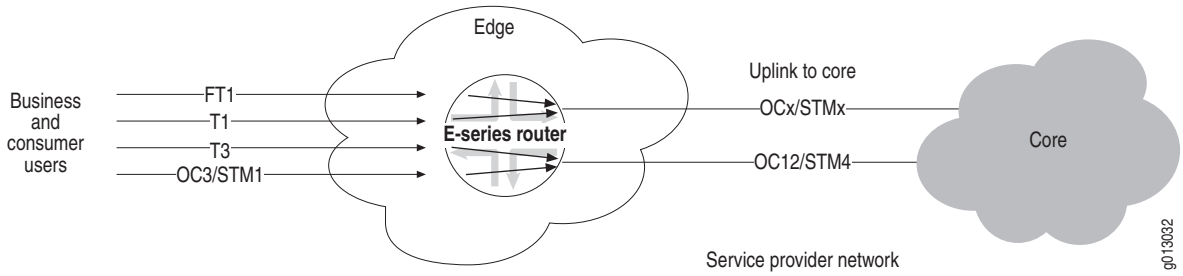
```
host1(config)#controller t3 0/1
host1(config-controll)#framing m23
host1(config-controll)#cablelength 300
host1(config-controll)#ds3-scramble
host1(config-controll)#exit
host1(config)#interface serial 0/1
host1(config-if)#invert data
```

```
host1(config-if)#mtu 1600
host1(config-if)#mru 1600
```

Configuring OCx/STMx and OC48 Interfaces

The router supports IP/ATM, IP/Frame Relay, and IP/PPP over SONET on the OCx/STMx interfaces. OC48 interfaces support IP/Frame Relay and IP/PPP over SONET, but do not support ATM operation. This interface support allows service providers to accept incoming optical connections or connect the router to the backbone network through optical connections. The router's SONET implementation supports termination, statistic gathering, and alarm surveillance at the section, line, and path layers of a SONET interface.

Figure 7: SONET Interfaces



The following sample command sequence configures POS for an OC3 interface. See *JUNOSe Link Layer Configuration Guide, Chapter 9, Configuring Packet over SONET*, for details.

```
host1(config)#interface pos 0/1
host1(config-if)#encapsulation ppp
host1(config-if)#clock source internal module
host1(config-if)#loopback line
host1(config-if)#pos framing sdh
host1(config-if)#mtu 1600
host1(config-if)#mru 1600
host1(config-if)#pos scramble-atm
```

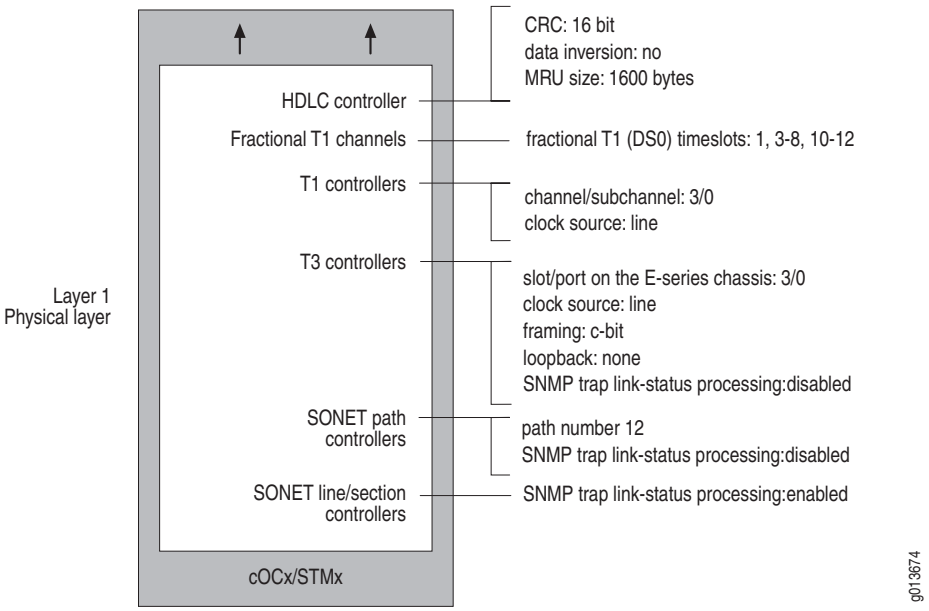
Configuring Channelized OCx/STMx Line Interfaces

The cOCx/STMx modules are generally used for circuit aggregration on the router. These line modules support the following controllers over OC3/STM1 or OC12/STM4, depending on the I/O module used with the line module:

- Fractional T1/E1 over SONET/SDH virtual tributaries or T3
- Unframed E1
- Unchannelized DS3

Figure 8 shows the configuration parameters for a sample T1 over DS3 interface configuration.

Figure 8: Parameters for T1 over DS3 Interface Configuration



The following sample command sequence configures T1 over DS3 on a channelized SONET interface as described in Figure 8. See *JUNOSe Physical Layer Configuration Guide, Chapter 4, Configuring Channelized OCx/STMx Interfaces*, for details.

```
host1(config)#controller sonet 3/0
host1(config-controller)#path 12 oc1 4/1
host1(config-controller)#path 12 ds3 1 channelized
host1(config-controller)#path 12 ds3 1 t1 4
host1(config-controller)#path 12 ds3 1 t1 4/2 timeslots 1, 3-8, 10-12
host1(config)#interface serial 3/0:12/1/4/2
```

Configuring Ethernet Interfaces

Ethernet interfaces support IP, PPPoE, multinetting (multiple IP addresses), and VLANs (subinterfaces). Ethernet modules use the Address Resolution Protocol (ARP) to obtain MAC addresses for outgoing Ethernet frames and support quality of service (QoS) classification. See *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*, for a description of limitations of individual modules.

Use the Fast Ethernet, Gigabit Ethernet, and 10-Gigabit Ethernet commands described in *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces* to:

- Configure with IP only, with PPPoE only, with both IP and PPPoE, and with or without VLANs.
- Specify the line speed and duplex mode.
- Specify the MTU.

The following sample command sequence configures an IP interface on a VLAN on an Ethernet interface:

```
host1(config)#interface fastEthernet 2/0
host1(config-if)#encapsulation vlan
host1(config-if)#interface fastEthernet 2/0.1
host1(config-if)#vlan id 201
host1(config-if)#ip address 192.168.129.5 255.255.255.0
```

The following sample command sequence adds an IP interface over PPPoE to the same VLAN:

```
host1(config)#interface fastEthernet 2/0.1.2
host1(config-if)#encapsulation pppoe
host1(config-if)#interface fastEthernet 2/0.1.2.1
host1(config-if)#encapsulation ppp
host1(config-if)#ip address 192.2.2.1 255.255.255.0
```

Configuring IPSec-Service Interfaces

IPSec Service modules support interfaces associated with secure IP tunnels. You 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 will add and remove tunnels when required.

For information about configuring secure IP interfaces, see *JUNOSe IP Services Configuration Guide, Chapter 6, Configuring IPSec*. For information about managing IPSec service interfaces, see *JUNOSe Physical Layer Configuration Guide, Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces*.

Configuring Tunnel Service Interfaces

You can configure both dynamic tunnels associated with L2TP and static IP tunnels on your E-series router; however, you must first install a Service Module (SM). Dynamic tunnels, which are not associated with a particular interface, are described in *JUNOSe Broadband Access Configuration Guide, Chapter 13, Configuring an L2TP LNS*. Static tunnels, in which the tunnel is assigned to a particular interface and specified in slot/port format, are described in *JUNOSe IP Services Configuration Guide, Chapter 10, Configuring IP Tunnels*.

For information about managing these types of tunnels on the router, see *JUNOSe Physical Layer Configuration Guide, Chapter 6, Managing Tunnel-Service and IPSec-Service Interfaces*.

Configuring Data Link-Layer Interfaces

You can configure the following data link-layer interfaces:

- IP/Frame Relay or multilink Frame Relay
- IP/ATM
- IP/PPP or multilink PPP

- IP/Cisco HDLC
- IP/Ethernet

Configuring IP/Frame Relay

The router supports IP over Frame Relay PVCs on the CT3 12-F0 and OCx/STMx POS modules. The interface presented to the incoming traffic is an IP/Frame Relay router. In addition, IP/PPP/Frame Relay is supported on the T3 and E3 modules. With this interface, the service provider can:

- Receive traffic from subscribers that have CPE equipment, such as routers with Frame Relay interfaces
- Take in traffic from other network devices that use Frame Relay, such as DSLAMs and Frame Relay switches
- Use Frame Relay as an uplink technology on an unchannelized T3 or E3 link

Figure 9 shows the structure of the Frame Relay interface. Each Frame Relay major interface sits on top of an HDLC interface. The Frame Relay implementation is divided into two levels: a major interface and one or more subinterfaces. This division allows a single physical interface to support multiple logical interfaces. Multiple IP interfaces can also be assigned to each Frame Relay major interface through the subinterfaces.

Figure 9: Frame Relay Interface Design

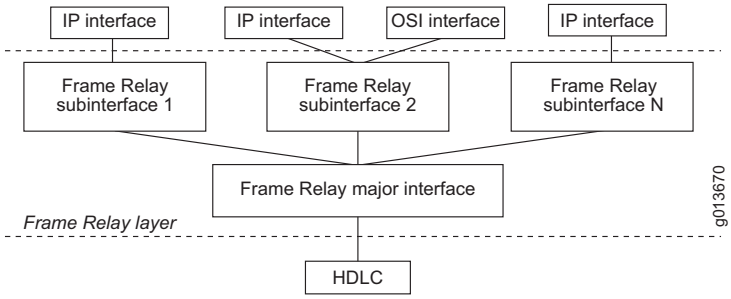
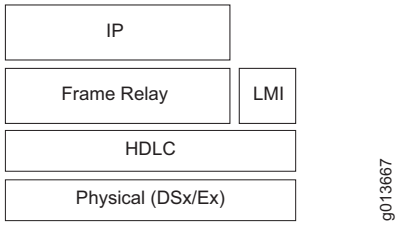


Figure 10 shows the structure of the Frame Relay protocols with the physical layer as the foundation. For Frame Relay, the physical layer can be channelized E1, E3, channelized T1, T3, or a fractional service, as supported by the different line module ports. The HDLC layer is on top of the physical layer and can support flexible assignment of physical resources.

For example, an HDLC channel can support one DS0, a fractional T1, or an entire T1. The major Frame Relay interface sits on top of the HDLC resource, and the subinterfaces sit on top of the major interface. The Frame Relay subinterfaces connect to the IP interface layer.

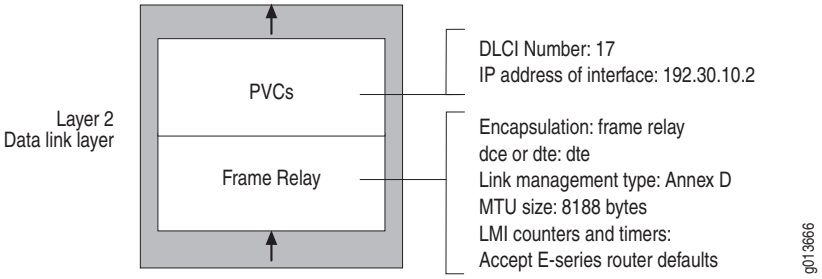
Figure 10: Structure of Frame Relay Protocols



The router supports Frame Relay LMI (local management interface) to provide the operator with configuration and status information relating to the Frame Relay VCs in operation. LMI specifies a polling mechanism to receive incremental and full-status updates from the network. The router can represent either side of the User-to-Network Interface (UNI) and supports unidirectional LMI. Bidirectional support for the Network-to-Network Interface (NNI) is also supported.

Figure 11 shows sample configuration parameters for Frame Relay on a serial interface.

Figure 11: Serial Interface Configuration Parameters for a Frame Relay Connection



The following sample command sequence configures a serial interface for Frame Relay. See *JUNOSe Link Layer Configuration Guide, Chapter 2, Configuring Frame Relay*, for information.

```
host1(config)#interface serial 0/1:1/5
host1(config-if)#encapsulation frame-relay ietf
host1(config-if)#frame-relay intf-type dte
host1(config-if)#frame-relay lmi-type ansi
host1(config-if)#interface serial 0/1:1/5.1
host1(config-subif)#frame-relay interface-dlci 17 ietf
host1(config-subif)#ip address 192.32.10.2 255.255.255.0
```

Configuring IP/ATM

The router supports IP over ATM PVCs on ATM line modules. This support allows service providers to receive traffic from subscribers who have CPE equipment, such as routers with ATM interfaces, to take in traffic from other network devices that use ATM, such as DSLAMs, and to connect to service providers with ATM backbone structures.

Figure 12 shows an IP/ATM access connection.

Figure 12: E-series Router IP/ATM Access Connection

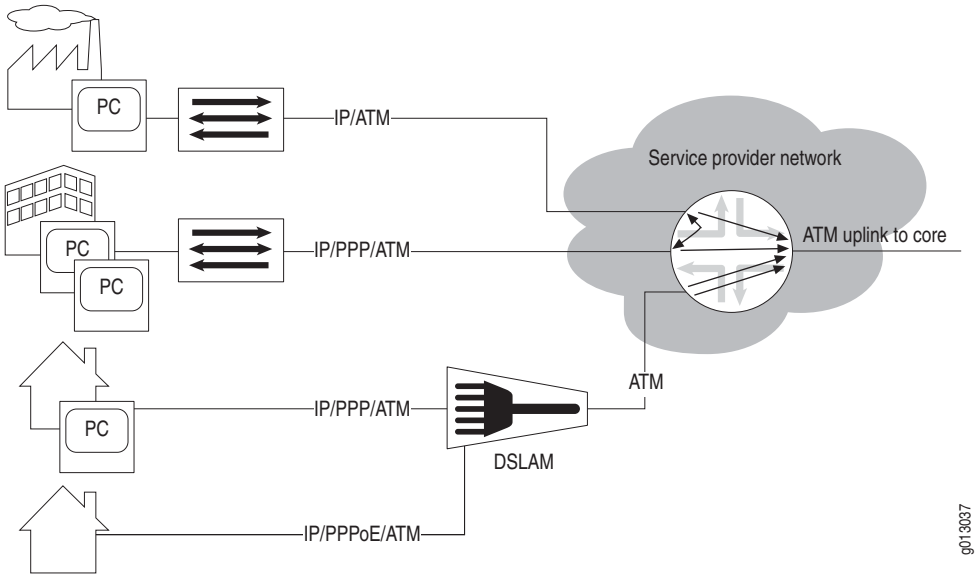


Figure 13 shows the structure of the ATM interface. For ATM, this can be SONET, DS3, or E3 as supported by the different line modules. The major ATM interface sits on top of the SONET/DS3/E3 resource, and the subinterfaces sit on top of the major interface. The ATM subinterfaces connect to the IP interface layer.

Figure 13: Structure of the ATM Interface Design

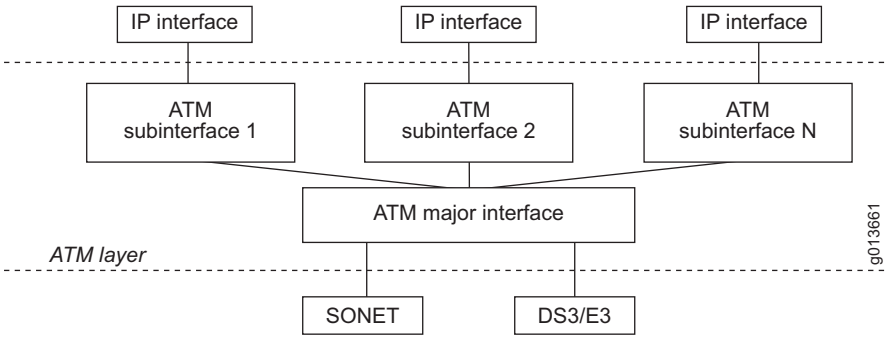


Figure 14 shows the structure of the ATM protocols. The physical layer (SONET and/or DSx/Ex) is the foundation and provider of layer 1 framing service. The ATM layer is on top and provides cell, circuit, and OAM services. The AAL5 layer provides a frame-oriented interface to the ATM layer. The integrated local management interface (ILMI) provides local management across the UNI.

Figure 14: Structure of ATM Protocol

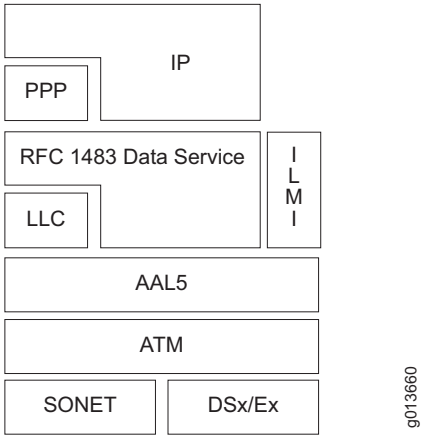
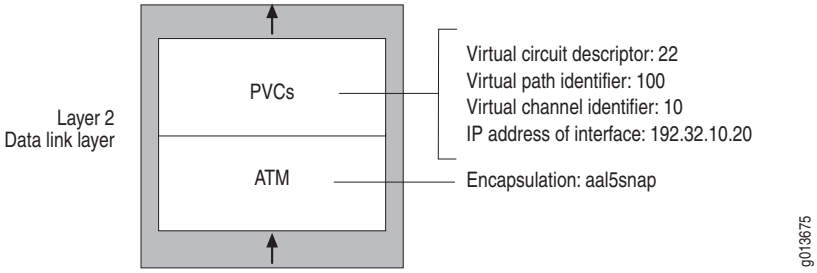


Figure 15 shows sample configuration parameters for a typical ATM interface configuration.

Figure 15: ATM Interface Configuration Parameters



The following sample command sequence configures an ATM interface on port 0 of the line module in slot 1. See *JUNOSe Link Layer Configuration Guide, Chapter 1, Configuring ATM*, for information about how to configure an ATM interface.

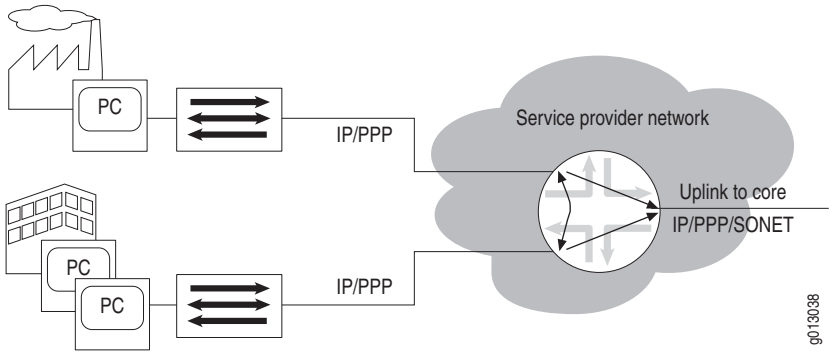
```
host1(config)#interface atm 0/1
host1(config-if)#interface atm 0/1.22
host1(config-if)#atm pvc 22 100 10 aal5snap
host1(config-subif)#ip address 192.32.10.20 255.255.255.0
```

Configuring IP/PPP

The router supports IP/PPP on the channelized T3, E1, and T3/E3 interfaces and IP/PPP/SONET on the OC3/STM1 and OC12/STM4 interfaces. This support allows service providers to accept traffic from subscribers who have CPE equipment, such as routers with PPP interfaces, and to transmit traffic in PPP format to other network devices.

Figure 16 shows that the router supports the incoming IP/PPP traffic from the CPE. This traffic can then be routed to the uplink(s) attached to the router or to other CPEs that are attached to the router.

Figure 16: IP/PPP Connections from the CPE on an E-series Router



As shown in Figure 17, the PPP protocol can exist directly on top of the HDLC layer or on top of a layer 2 Frame Relay or ATM interface. In either case, IP rides on top of PPP, providing support for IP/PPP/ATM, IP/PPP/HDLC, and IP/PPP/Frame Relay. Both SONET and DSx/Ex interfaces are supported at the physical layer.

Figure 17: Structure of PPP

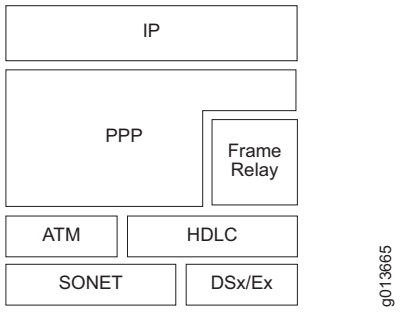
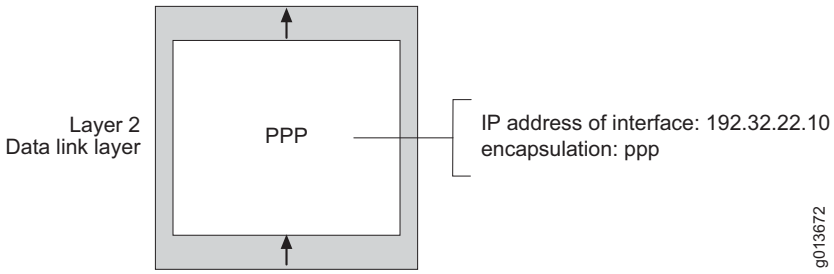


Figure 18 shows sample configuration parameters for PPP on a serial interface.

Figure 18: PPP Interface Configuration Parameters



The following sample command sequence configures PPP on a serial interface. See *JUNOSe Link Layer Configuration Guide, Chapter 7, Configuring Point-to-Point Protocol*, for details.

```
host1(config)#interface serial 3/0:2/5
host1(config-if)#encapsulation ppp
host1(config-if)#ip address 192.32.22.10 255.255.255.0
```

Configuring IP/HDLC

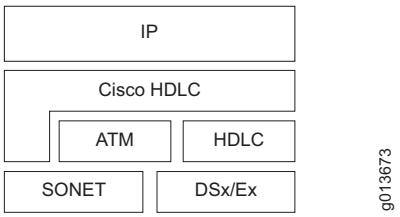
The E-series router supports IP over Cisco HDLC on many types of serial interfaces. Cisco HDLC monitors line status on a serial interface by exchanging keepalive request messages with peer network devices. It also allows routers to discover IP addresses of neighbors by exchanging Serial Link Address Resolution Protocol (SLARP) address request and address response messages with peer network devices.

The E-series router Cisco HDLC is compatible with the Cisco Systems Cisco-HDLC protocol, the default protocol for all Cisco serial interfaces.

The router supports the following framing features:

- HDLC for data-link framing
- 18,000-byte information field size

Figure 19: Structure of Cisco HDLC Protocol



As shown in Figure 19, the Cisco HDLC protocol can exist directly on top of the HDLC layer or ATM or SONET interface. Both SONET and DSx/Ex interfaces are supported at the physical layer.

The following example configures HDLC on a serial interface. See *JUNOSe Link Layer Configuration Guide, Chapter 14, Configuring Cisco HDLC,* for details.

```
host1(config)#interface serial 3/1:2/1
host1(config-if)#encapsulation hdlc
host1(config-if)#ip address 192.32.10.2 255.255.255.0
```

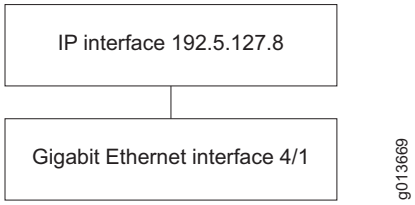
Configuring IP/Ethernet

The E-series router supports IP/Ethernet. When you select an Ethernet interface, you can assign an IP address to it, as the following example shows:

```
host1(config)#interface fastethernet 4/1
host1(config-if)#ip address 192.5.127.8 255.255.255.0
```

Figure 20 shows an IP/Ethernet interface stack.

Figure 20: Example of IP over Ethernet Stacking Configuration Steps



Configuring IP Tunnels, Shared IP Interfaces, and Subscriber Interfaces

The E-series router supports IP tunnels, shared IP interfaces, and subscriber interfaces.

Configuring IP Tunnels

IP tunnels provide a way of transporting datagrams between routers separated by networks that do not support all the protocols that those routers support. To configure an IP tunnel, you must first configure a tunnel-service interface. (See *Configuring Tunnel Service Interfaces* on page 15.)

When you have configured a tunnel-service interface, treat it in the same way as any IP interface on the router. For example, you can configure static IP routes or enable routing protocols on the tunnel interface. The IP configurations that you apply to the tunnels control how traffic travels through the network.

Configuring Shared Interfaces and Subscriber Interfaces

A shared IP interface is one of a group of IP interfaces that use the same layer 2 interface. Shared IP interfaces are unidirectional—they can transmit but not receive traffic. A subscriber interface is an extension of a shared IP interface. Subscriber interfaces are bidirectional—they can both receive and transmit traffic.

You can create multiple shared IP interfaces over the same layer 2 logical interface—for example, atm 5/3.101—enabling more than one IP interface to share the same logical resources. This capability is useful, for example, when data received in one VRF needs to be forwarded out an interface in another VRF, such as for BGP/MPLS VPNs (see *JUNOSe BGP and MPLS Configuration Guide, Chapter 3, Configuring BGP-MPLS Applications*, for more information). You can configure one or more shared IP interfaces. Data sent over shared interfaces uses the same layer 2 interface. You can configure shared interfaces as you would other IP interfaces. Each shared interface has its own statistics.

The E-series router supports subscriber interfaces on a particular type of layer 2 interface, Ethernet. In the absence of VLANS, Ethernet does not have a demultiplexing layer. A subscriber interface adds a demultiplexing layer for an Ethernet interface that is configured without VLANs. Using subscriber interfaces, the router can demultiplex or separate the traffic associated with different subscribers. You can use subscriber interfaces to separate traffic for cable modem subscribers with different levels of service and to separate traffic for VPNs.

For information about configuring shared interfaces and subscriber interfaces, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

Configuring Routing Protocols

After you have set up the interfaces on which IP traffic flows, you can configure the following routing protocols:

- IP multicast protocols—IP multicasting allows a device to send packets to a group of hosts, rather than to a list of individual hosts. Routers use multicast routing algorithms to determine the best route and transmit datagrams throughout the network. See *JUNOSe Multicast Routing Configuration Guide, Chapter 5, Configuring IPv4 Multicast*, for information about how to configure IP multicast.

- Open Shortest Path First (OSPF)—This interior gateway protocol (IGP) advertises the states of network links within an autonomous system. An autonomous system is a set of routers having a single routing policy running under a single technical administration. See *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 5, Configuring OSPF,* for information about how to configure OSPF.

- Integrated Intermediate System–to–Intermediate System (integrated IS-IS)—The integrated IS-IS protocol provides routing for IP networks and is an extension of the original IS-IS protocol, which provides routing for pure Open Systems Interconnection (OSI) environments. This link-state protocol builds a complete and consistent picture of a network's topology by sharing link-state information across network devices in a routing domain. A routing domain is a collection of contiguous networks that provide full connectivity to all end systems located within them. See *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 6, Configuring IS-IS,* for information about how to configure IS-IS.

- Border Gateway Protocol (BGP)—BGP, an external gateway protocol (EGP), provides loop-free interdomain routing between autonomous systems. See *JUNOSe BGP and MPLS Configuration Guide, Chapter 1, Configuring BGP Routing,* for information about how to configure BGP.

- Routing Information Protocol (RIP)—RIP is an IGP created for use in small, homogeneous networks. RIP uses distance-vector routing to route information through IP networks. See *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 4, Configuring RIP*, for information about how to configure RIP.

- Multiprotocol Label Switching (MPLS)—MPLS is a hybrid protocol that integrates network layer routing with label switching to provide a layer 3 network with traffic management capability. Traffic engineering enables more effective use of network resources while maintaining high bandwidth and stability. MPLS enables service providers to offer their customers the best service available given the provider's resources. There are two fundamental aspects to MPLS:

  - Label distribution—The set of actions MPLS performs to establish and maintain a label-switched path (LSP), also known as an MPLS tunnel.

  - Data mapping—The process of getting data packets onto an established LSP.

  See *JUNOSe BGP and MPLS Configuration Guide, Chapter 2, Configuring MPLS*, for information about configuring MPLS.

In addition, if you want to make configuration adjustments to IP, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*, for details.

Configuring VRRP

The Virtual Router Redundancy Protocol (VRRP) can prevent loss of network connectivity to end hosts if the static default IP gateway fails. By implementing VRRP, you can designate a number of routers as "backup" routers in case the default "master" router fails. You can configure VRRP on IP/Ethernet interfaces.

For information about configuring VRRP, see *JUNOSe IP Services Configuration Guide, Chapter 14, Configuring VRRP*.

Configuring Routing Policy

The router supports a number of features that allow the service provider to control the exchange of routing information between virtual routers in the router, between routers in the network, and between protocols within a router:

- Access lists—Provide filters that can be applied to route maps or distribution lists. They allow policies to be created, such as a policy to prevent forwarding of specified routes between the BGP-4 and IS-IS routing tables.

- Route maps—Modify the characteristics of a route (generally to set its metric or to specify additional attributes) as it is transmitted or accepted by a router. Route maps can use access lists to identify the set of routes to modify.

- Distribution lists—Control the routing information that is accepted or transmitted to peer routers. Distribution lists always use access lists to identify routes for distribution. For example, distribution lists could use access lists to specify routes to advertise.
- Redistribute routes—Allow routes to be shared between routing protocols and routing domains. For example, a subset of BGP-4 routes could be leaked into the IS-IS routing tables.

See *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*, for details.

Configuring QoS

QoS is a suite of features that configure queuing and scheduling on the forwarding path of your E-series router. QoS provides a level of predictability and control beyond the best-effort service that is the E-series router's default data delivery service. Packets not assigned to a specific traffic class are carried in the best-effort traffic class. Best-effort service provides packet transmission with no guarantee of results.

The major QoS features that the E-series router provides are:

- Multiple traffic classes
- Configurable scheduling
- Configurable buffer management

For information about configuring QoS, see *JUNOSe Quality of Service Configuration Guide, Chapter 16, Configuring and Attaching QoS Profiles to an Interface*.

Configuring Policy Management

Policy management allows network service providers to implement packet forwarding and routing specifically tailored to their customer's requirements. Using policy management, customers can implement policies that selectively cause packets to take different paths. Policy management provides several types of services:

- Policy routing—Predefines packet flow to a destination port or IP address
- QoS classification and marking—Marks packets of a packet flow.
- Packet forwarding—Allows forwarding of a packet flow.
- Packet filtering—Drops packets of a packet flow.
- Packet logging—Logs packets of a packet flow.

- Rate limiting—Enforces line rates below the physical line rate of the port and sets limits on packet flows.
- RADIUS policy support—Allows you to attached a preconfigured policy to an interface through RADIUS.

See *JUNOSe Policy Management Configuration Guide, Chapter 1, Managing Policies on the E-series Router*, for details about configuring policy management.

Configuring Remote Access

The E-series router supports the following remote access functionality:

- Broadband Remote Access Server (B-RAS)—This application runs on the router and is responsible for:
  - Aggregating the output from DSLAMs
  - Providing user PPP sessions and PPP session termination
  - Enforcing QoS policies
  - Routing traffic into an ISP's backbone network

  See *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access*.
- Layer 2 Tunneling Protocol (L2TP)—A method of encapsulating layer 2 packets, such as PPP, for transmission across a network. In an L2TP relationship, an L2TP access concentrator (LAC) forms a client-server relationship with a destination, known as an L2TP network server (LNS), on a remote network.

  You can configure the router to act as an LAC in PPP pass-through mode. The router creates tunnels dynamically by using AAA authentication parameters and transmits L2TP packets to the LNS through IP/UDP. See *JUNOSe Broadband Access Configuration Guide, Chapter 12, Configuring an L2TP LAC*.
- Non-PPP equal access—A method of allowing remote access in which the router provides IP addresses to subscribers' computers through Dynamic Host Configuration Protocol (DHCP). This method is particularly convenient for broadband (cable and DSL) environments or environments that use bridged Ethernet over ATM, because network operators can support one central system rather than an individual PPPoE client on each subscriber's computer. See *JUNOSe Broadband Access Configuration Guide, Chapter 17, DHCP Overview*.

Chapter 2

Command-Line Interface

This chapter provides information about the E-series router command-line interface (CLI).

This chapter contains the following sections:

- Overview on page 27
- Platform Considerations on page 47
- Accessing the CLI on page 47
- CLI Command Privileges on page 50
- Using Help on page 62
- Using Command-Line Editing on page 66
- Accessing Command Modes on page 68

Overview

The CLI is the interface to the software that you use whenever you access the router—whether from the console or through a remote network connection. The CLI, which automatically starts after the router finishes booting, provides commands that you use to perform various tasks, including configuring the JUNOSe software and monitoring and troubleshooting the software, network connectivity, and the router hardware.

Managing your router using the CLI gives you access to thousands of commands. The router's CLI uses an industry *de facto* standard look and feel, which might be familiar to you. If you are new to this CLI, it is helpful to read this entire chapter, where you can learn about CLI shortcuts and other helpful information.

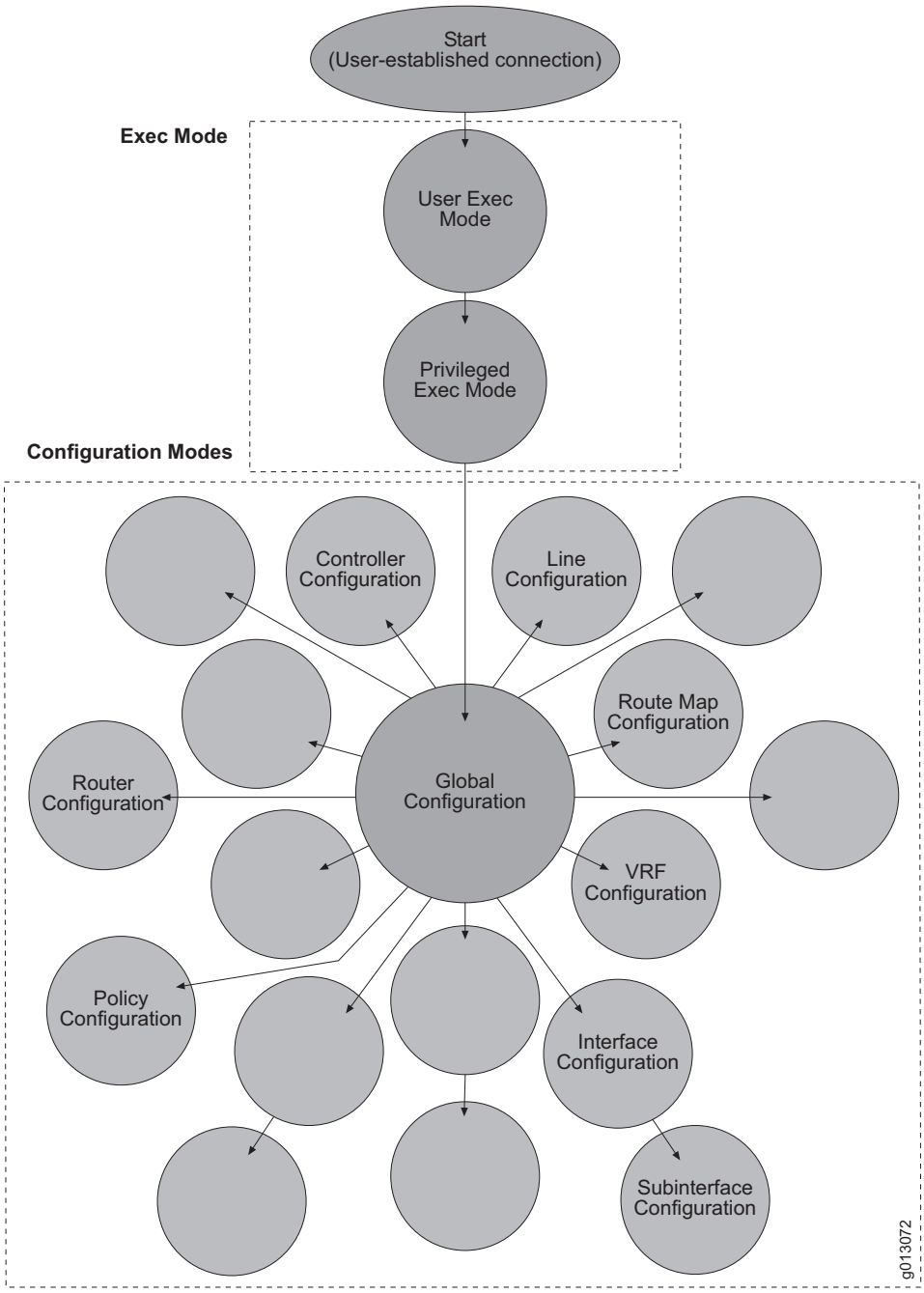
Command Modes

Command modes set a context for the CLI. Each command in the CLI is available from one or more command modes. From some command modes you can only view router information; from others you can perform configuration tasks. For example, you can access User Exec mode to display information and then access Global Configuration mode to set parameters or enable a particular feature. By recognizing the command-line prompt, you can identify where you are in the CLI at any given point. When you can easily identify where you are, it is easy to get to where you want to be.

Figure 21 on page 29 illustrates the command mode architecture. Only some of the many configuration modes are shown.

Command modes are discussed in greater detail in the section *Accessing Command Modes* on page 68. See the *JUNOSe Command Reference Guide* to find related command modes for any command.

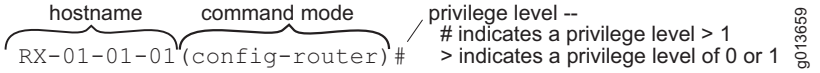
Figure 21: Command Mode Architecture



Command-Line Prompts

Within the CLI, the command-line prompt identifies both the *hostname* and the *command mode*. The hostname is the name of your router; the command mode indicates your location within the CLI system.

For example:



Keywords and Parameters

CLI commands are made up of two primary elements: *keywords* and *parameters*.

Keywords

Every command requires at least one keyword; however, a command can contain other optional keywords. The keyword(s) must be typed into the CLI accurately for it to be recognized. These are examples of keywords:

reload

run

router

map-class

map-list

clear ip isis redistribution

show vlan subinterface

qos-port-type-profile

no rtr reset

radius calling-station-delimiter

You can abbreviate keywords; however, you must enter enough initial characters to unambiguously identify the command. For example, if the keyword you want to specify is **map-class** and you enter only **map-**, an error appears. The error indicates that one or more possible keywords begin with **map-**, thus making your entry ambiguous.

Parameters

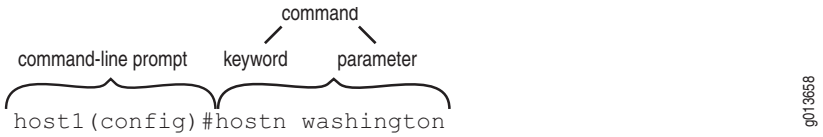
Parameters are often required elements of a command; however, for some commands, parameters are not required. A parameter is most often a value that you specify after the keyword. There are different types of parameters, such as strings, integers, or IP addresses.

The CLI indicates the type of parameter that you must enter. When you see a range of numbers or uppercase letters, it indicates that you must specify a value. For example:

CLI Parameter Placeholder or Range	Sample Parameter User Input
ROUTER[:VRF]	charlie:1234
INTERFACE	3/2:20/15
WORD	windtunnel
<0–4294967295>	5600
A.B.C.D	192.56.32.2

Keywords and Parameters Together

By combining keywords and parameters in the correct sequence, you can begin using the CLI to configure and monitor your router. For example, you could specify the command **hostname** to change the name of your router by entering a keyword and a parameter. You need to type only the portion of the keyword that makes it unambiguous, such as **hostn**. Here, the value of the parameter, which is the name you assign to the host, is a string of up to 64 characters.



When you enter this command, the new hostname appears in the prompt.

Another example is a command that requires you to enter a number from within a given range. The command **ip http port** requires that a value be entered for the *portNumber* parameter. The value of this parameter is a number in the range of 0–65535. For example, you could enter:

```
juniper(config)#ip http port 56789
```

NOTE: You can find detailed information about command syntax, with parameter values defined, in the *JUNOSe Command Reference Guide*.

Using CLI Commands

This section introduces some useful shortcuts and command-related highlights. These include:

- Abbreviated Commands
- The ? Key
- Backspace or Delete Key
- Enter Key
- Tab Key
- Arrow Keys
- The **no** Version (**no** Commands)
- **run** and **do** Commands
- **show** Commands
- The --More-- Prompt
- Responding to Prompts

Abbreviated Commands

Remember, you can abbreviate keywords to save time if you enter at least enough leading characters to uniquely identify the desired keyword. For example:

```
host1(config-if)#ip re
```

This abbreviation is for the command **ip redirects**. The string **ip re** is enough information for the CLI to identify the command you are using. See the section *Using Help* on page 62 for additional information.

The ? Key

Use the **?** key at any time to see all the choices you can enter next. For example:

```
host1(config)#router ?
     bgp Configure the Border-Gateway Protocol (BGP)
     isis Configure ISO IS-IS
     ospfConfigure the Open Shortest Path First protocol (OSPF)
     rip  Configure the Routing Information Protocol
host1(config)#router
```

When you enter the **?** character, all available choices are displayed. The router again displays the command you typed. You then have to type in only the choice you want and press Enter.

A <cr> in the list of choices means that you can press Enter to execute the command. For example:

```
host1(config-if)#isis metric 40 level-2 ?
  <cr>

host1(config-if)#isis metric 40 level-2
```

NOTE: If the list of options extends beyond one screen, the last line on your screen displays the --More-- prompt. If you want to use the **?** character as part of a string, such as a hostname or a regular expression, you must enter the following key sequence: Ctrl + v + ?. Otherwise, the CLI considers the **?** to be a request for assistance in completing the command.

Backspace or Delete

Use either key to delete the character immediately preceding the cursor.

Enter

Always use this key to execute the command you entered.

Tab

Use this key to complete the current keyword. For example, if you entered a portion of a lengthy command, such as

```
host1(config)#class
```

and press Tab, the full name of the command appears:

```
host1(config)#classifier-list
```

Arrow Keys

Some terminals have arrow (or cursor) keys on their keyboards. These arrow keys are very useful; however, to use them you must have an ANSI/VT100 emulating terminal.

The Up Arrow and Down Arrow keys display command history. The Up Arrow key displays the previous command; you can also use Ctrl + p. The Down Arrow key displays the next command; you can also use Ctrl + n.

The Left Arrow and Right Arrow keys allow the user to move the cursor back and forth in the command line.

The no Version

With very few exceptions, every system configuration command has a **no** version, which you can use to negate a command (or a portion of it as specified by an optional keyword) or to restore its default setting. When you use a command *without* the keyword **no**, you can reenable a disabled feature or override a default setting.

You have the option of using the **default** keyword whenever the **no** keyword is also a choice; simply enter the keyword **default** instead of **no**.

In most cases, when you execute the **default** version of a command, it produces the exact results as the **no** version. There are some commands for which the **default** version yields a different result from the **no** version.

Commands for which the **default** behavior differs from the **no** behavior are clearly identified in the *JUNOSe Command Reference Guide*. Unless otherwise specified, therefore, the **default** command is identical to the **no** command and is neither documented nor discussed.

The syntax for each **no** command is described in the *JUNOSe Command Reference Guide*. The few system configuration commands that do not have a **no** version are indicated in the individual command description.

Because **show** commands are for the purpose of monitoring your configurations, they do not have **no** versions. Most User Exec and Privileged Exec mode commands do not have **no** versions.

The CLI can act on **no** versions of commands when you have entered sufficient information to distinguish the command syntactically; the CLI ignores all subsequent input on that line.

To be compatible with some non-Juniper Networks implementations, the **no** versions of commands will accept the same options as the affirmative version of the commands. The CLI ignores the optional input if it has no effect on the command behavior. If using the option changes the behavior of the **no** version, the individual command entry in this guide describes the difference in behavior.

run and do Commands

You can run Exec mode commands while in any configuration mode by preceding the command with the keyword **run** or **do**. For example:

```
host1(config)#run show users
```

NOTE: The **run** and **do** commands are interchangeable.

By using the **run** or **do** command in this way, you can obtain **show** command information without leaving configuration mode.

The only commands that cannot be preceded by **run** or **do** are the **configure** command and those commands that are already available in all modes, such as **sleep** or **exit**.

Example 1

```
host1(config)#run show config | begin interface
interface null 0
!
interface fastEthernet 0/0
 ip address 10.6.129.41 255.255.128.0
!
interface gigabitEthernet 5/0
!

interface atm 6/0
interface atm 6/0.1 point-to-point
 encapsulation pppoe
!
interface atm 6/0.1.7
!
interface atm 6/0.1.5
!
interface atm 6/0.1.2
!
interface atm 6/0.1.9
!
interface atm 6/0.1.11
!
interface atm 6/0.1.15
!
interface atm 6/0.1.18
!
ip route 0.0.0.0 0.0.0.0 10.6.128.1
ip route 10.10.121.72 255.255.255.255 10.6.128.1
!
!
route-map adsf permit 10
router dvmrp
!
router igmp
!
snmp-server community private view everything rw
snmp-server contact Mary
snmp-server
!
! End of generated configuration script.
host 1(config)#int fa 0/0
```

Example 2

```
host1(config-if)#do dir
Please wait...
                                unshared                          in
       file            size       size         date (UTC)        use
------------------   --------   --------   -------------------   ---
reboot.hty              31040      31040   10/30/2001 15:31:10
system.log              20481      20481   10/26/2001 17:24:16
soft_clear_in.mac        8578       8578   10/24/2001 14:39:02
erx_3-3-1.rel        71082105   71082105   10/25/2001 13:02:50    !
erx_3-3-1.rel        70502991   70502991   10/24/2001 19:58:08
autocfg.scr               355        355   09/28/2001 13:33:04
Capacity = 224133120, Bytes Free = 44986177, Reserved = 36700160

host1(config-if)#
```

show Commands

You have access to a variety of **show** commands that display router and protocol information. You can filter the output of a **show** command by specifying | (the UNIX pipe symbol), one of the following keywords, and either a case-sensitive text string or a regular expression.

- **begin**—Displays output beginning with the first line that contains the text string or regular expression
- **include**—Displays output lines that contain the text string or regular expression and excludes lines that do not contain the text string or regular expression
- **exclude**—Displays output lines that do not contain the text string or regular expression and excludes lines that do contain the text string or regular expression

For a list of regular expressions, see *Regular Expressions* on page 40. You can press Ctrl + c to interrupt the **show** command output.

NOTE: The system does not recognize beginning spaces of the text string. For example, if you enter **include IP** as the text string on which to filter, the system ignores the space and displays lines that include words such as RIP.

Example 1 In the following example, the output display starts with the first line that contains the string *inter*. The system omits all the preceding lines of the output from the display because none of them contains the string *inter*.

```
host1#show config include-defaults | begin inter
Please wait...log verbosity low internalNetwork
log verbosity low ipEngine
log verbosity low ipProfileMgr
log verbosity low ipProfileMgrEngineering
no log engineering
log fields timestamp instance no-calling-task
!
timing select primary
timing source primary internal
timing source secondary internal
timing source tertiary internal
!
no disable-autosync
no disable-switch-on-error
no redundancy lockout 0
!
virtual-router default
ip domain-lookup
ip name-server 10.2.0.3
ip domain-name 789df
!
host f 10.10.133.11 ftp anonymous null
interface null 0
interface ip 0/0
 arp timeout 21600
!
interface ip 2/0
 arp timeout 21600
!
```

```
interface ip s10
 arp timeout 21600
!
interface atm 2/0
 no shutdown
 atm sonet stm-1
 loopback line
 atm uni-version 3.0
 atm oam loopback-location 0xFFFFFFFF
 atm vc-per-vp 32768
 atm vp-tunnel 1 10
 load-interval 300
 no atm snmp trap link-status
 no atm shutdown
!
no atm aal5 snmp trap link-status
no atm aal5 shutdown
!
interface atm 2/0.1 point-to-point
 no shutdown
 no atm atm1483 shutdown
 no atm atm1483 snmp trap link-status
!
ip route 0.0.0.0 0.0.0.0 10.13.5.1
ip debounce-time 0
ip source-route
!
router ospf 5
 no ospf shutdown
 ip route-type both
 timers spf 3
 maximum-paths 4
 ospf auto-cost reference-bandwidth 100
 distance ospf intra-area 110
 distance ospf inter-area 112
 distance ospf external 114
! Area 0.0.0.0
!
! Trap Source: <not configured>
! Note: SNMP server not running.
!
host1#
```

Example 2 In the following example, the output display consists only of lines that contain the string *ip*. The system omits all other lines of the output from the display because none of them contains the string *ip*.

```
host1#show config include-defaults | include ip
! Configuration script generated on WED JUN 06 2001 02:17:00 UTC
 strip-domain disable
Please wait...log verbosity low ipEngine
log verbosity low ipEngineering
log verbosity low ipGeneral
log verbosity low ipInterface
log verbosity low ipNhopTrackerEngineering
log verbosity low ipNhopTrackerGeneral
log verbosity low ipProfileMgr
log verbosity low ipProfileMgrEngineering
!
bandwidth oversubscription
ip domain-lookup
ip name-server 10.2.0.3
```

```
ip domain-name 789df
interface ip 0/0
interface ip 2/0
interface ip s10
 ip address 10.13.5.61 255.255.255.0
 no ip proxy-arp
 no ip directed-broadcast
 ip redirects
ip route 0.0.0.0 0.0.0.0 10.13.5.1
ip debounce-time 0
ip source-route
no ip ftp source-address
 type echo protocol ipIcmpEcho 10.5.0.200 source fastEthernet0/0
 type pathEcho protocol ipIcmpEcho 10.2.0.3
 type echo protocol ipIcmpEcho 10.5.0.11 source-ipaddr 10.13.5.61
!
controller t1 6/0
 framing esf
 lineCoding b8zs
 clock source line
 cablelength short 0
 no remote-loopback
!
log engineering
log verbosity low
no log severity
log verbosity low NameResolverLog
log verbosity low atm
log verbosity low atm1483
log verbosity low atmAal5
log verbosity low bgpConnections
log verbosity low bgpDampening
!
host1#
```

Example 3 In the following example, the output display consists only of lines that do not contain the string *!*. The system omits all other lines of the output from the display because each line contains the string *!*.

```
host1#show config include-defaults | exclude !
boot config running-configuration
boot system 3-3-1.rel
no boot backup
no boot subsystem
no boot backup subsystem
boot revert-tolerance 3 1800
no boot force-backup
aaa domain-map jacksonville
 virtual-router miami
 strip-domain disable
aaa domain-map jak
 virtual-router default
 strip-domain disable
aaa domain-map northeast
 virtual-router default
 strip-domain disable
aaa delimiter realmName "/"
hostname host1
no aaa new-model
no service ctrl-x-reboot
no service password-encryption
no baseline show-delta-counts
```

```
clock timezone UTC 0 0
no exception dump
exception protocol ftp anonymous null
controller sonet 2/0
 sdh
 loopback network
 clock source line
 no shutdown
 path 0 overhead j1 msg hello
 path 0 overhead j1 exp-msg
ftp-server enable
no login
log engineering
log verbosity low
no log severity
log verbosity low NameResolverLog
log verbosity low aaaAtm1483Cfg
log verbosity low atm1483
log verbosity low atmAal5
log verbosity low bgpConnections
log verbosity low bgpDampening
log verbosity low bgpEng1
log verbosity low bgpEngineering
log verbosity low bgpEvents
log verbosity low bgpKeepAlives
no log engineering
log fields timestamp instance no-calling-task
timing select primary
timing source primary internal
timing source secondary internal
timing source tertiary internal
no atm aal5 snmp trap link-status
no atm aal5 shutdown
interface atm 2/0.1 point-to-point
 no shutdown
 no atm atm1483 shutdown
 no atm atm1483 snmp trap link-status
ip route 0.0.0.0 0.0.0.0 10.13.5.1
ip debounce-time 0
ip source-route
```

Redirection of show Command Output

You can redirect the output of **show** commands to network files or local files (in NVS memory) using the redirection operators described in Table 5.

Table 5: Redirect Operators

Redirect Operator	Use
>	Redirects output to the specified file, overwriting the file if it already exists, creating the file if it does not.
> >	Appends output to the end of the specified file, creating the file if it does not exist.
&>	Redirects output to the specified file, overwriting the file if it already exists, and displays the output on the screen. The redirection is synchronized with the screen display; for example, if a --More-- prompt appears, the redirection halts until you take further action.
&> >	Appends output to the end of the specified file and displays the output to the screen. The redirection is synchronized with the screen display; for example, if a --More-- prompt appears, the redirection halts until you take further action.

For example, you can redirect the output of the **show config** command to a script file and later run that script:

```
host1#show config > showconfig.scr
```

The following command *writes* the output to a text file, version.txt, on a remote router:

```
host1#show hardware > pc:/erxfiles/version.txt
```

The following command *appends* the output to version.txt:

```
host1#show hardware >> version.txt
```

You can use redirection with output filtering. The general syntax is:

show *options* [{ **>** | **>>** | **&>** | **&>>** } *filename*]
[| { **begin** | **include** | **exclude** } *filterstring*]

The filtering is performed before redirection. In the following example, the cnfgfltr.txt file will contain the output of **show config include-defaults** beginning with the first occurrence of the string *inter*.

```
host1#show config include-defaults &> cnfgfltr.txt | begin inter
```

Regular Expressions

A regular expression uses special characters—often referred to as metacharacters—to define a pattern that is compared with an input string. You can use regular expressions to filter the output of **show** commands and to define AS-path access lists and community lists to more easily filter routes.

For examples of using regular expressions with AS-path access lists and community lists, see *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

Metacharacters

Table 6 describes the metacharacters supported for regular expression pattern-matching.

Table 6: Supported Regular Expression Metacharacters

Metacharacter	Description
^	Matches the beginning of the input string. Alternatively, when used as the first character within brackets—[^]—matches any number except the ones specified within the brackets.
$	Matches the end of the input string.
.	Matches any single character, including white space.
*	Matches 0 or more sequences of the immediately previous character or pattern.
+	Matches 1 or more sequences of the immediately previous character or pattern.
?	Matches 0 or 1 sequence of the immediately previous character or pattern.
()	Specifies patterns for multiple use when followed by one of the multiplier metacharacters: asterisk *, plus sign +, or question mark ?
[ ]	Matches any enclosed character; specifies a range of single characters.
– (hyphen)	Used within brackets to specify a range of AS or community numbers.
_ (underscore)	Matches a ^, a $, a comma, a space, a {, or a }. Placed on either side of a string to specify a literal and disallow substring matching. Numerals enclosed by underscores can be preceded or followed by any of the characters listed above.
|	Matches characters on either side of the metacharacter; logical OR.

Using Metacharacters as Literal Tokens

You can remove the special meaning of a metacharacter by preceding it with a backslash (\). Such a construction denotes that the metacharacter is *not* treated as a metacharacter for that regular expression. It is simply a character or token with no special meaning, just as a numeral has no special meaning. The backslash applies only to the character immediately following it in the regular expression.

On the E-series router, you are likely to do this only for the parentheses characters, **(** or **)**. BGP indicates a segment of an AS path that is of type AS-confed-set or AS-confed-seq by enclosing that segment within parentheses.

The - -More- - Prompt

When command output continues beyond the available space on your monitor screen, the system displays the --More-- prompt. If you press Enter, the system displays the next line of output. If you press the Spacebar, the system displays the next screen of output.

You can begin filtering the output from the --More-- prompt, or change a filter that is already in effect, by entering one of the following characters and a text string:

+ (plus)	Displays all output lines that contain the text string
– (minus)	Displays all output lines that do not contain the text string
/ (forward slash)	Displays all output lines starting at the first line that contains the text string

Initial spaces are not ignored when you filter at the --More-- prompt.

Example 1 In the following example, the output is displayed until the screen is filled and the --More-- prompt appears. By entering the filter **/interf**, the user forces the system to filter out all output lines until the first occurrence of the string *interf*. The system displays that line and all following lines of the output.

```
host1#show config include-defaults
! Configuration script being generated on FRI AUG 04 2006 12:48:48 UTC
! Juniper Edge Routing Switch ERX-700
! Version: 7.3.0 beta-1.6 [BuildId 5672] (July 11, 2006  11:58)
! Copyright (c) 1999-2006 Juniper Networks, Inc.  All rights reserved.
!
boot config running-configuration
boot system erx_7-3-0.rel
no boot backup
no boot subsystem
no boot backup subsystem
boot revert-tolerance 3 1800
no boot force-backup
!
aaa domain-map jacksonville
 virtual-router miami
 strip-domain disable
!
aaa domain-map jak
 virtual-router default
 strip-domain disable
!
aaa domain-map northeast
 virtual-router default

/interf
(Suppressing output until 'interf' is found, press ^C to end...)
interface null 0
interface ip 0/0
 arp timeout 21600
!
interface ip 2/0
 arp timeout 21600
!
interface ip s10
 arp timeout 21600
!
interface atm 2/0
 no shutdown
 atm sonet stm-1
 loopback line
 atm uni-version 3.0
```

```
 atm oam loopback-location 0xFFFFFFFF
 --More--
```

Example 2 In the following example, the output is displayed until the screen is filled and the --More-- prompt appears. By entering the filter **+ip**, the user forces the system to filter out all lines from the remainder of the output that do not contain the string *ip*. The system displays only lines that contain the string *ip*.

```
host1#show config include-defaults
! Configuration script being generated on FRI AUG 04 2006 12:48:48 UTC
! Juniper Edge Routing Switch ERX-700
! Version: 7.3.0 beta-1.6 [BuildId 5672] (July 11, 2006  11:58)
! Copyright (c) 1999-2006 Juniper Networks, Inc.  All rights reserved.
!
boot config running-configuration
boot system erx_7-3-0.rel
boot config running-configuration
boot system 3-3.1.rel
no boot backup
no boot subsystem
no boot backup subsystem
boot revert-tolerance 3 1800
no boot force-backup
!
aaa domain-map jacksonville
 virtual-router miami
 strip-domain disable
!
aaa domain-map jak
 virtual-router default
 strip-domain disable
!
aaa domain-map northeast
 virtual-router default
--More--
+ip
(Displaying only lines that include 'ip', press ^C to end...)
 strip-domain disable
log verbosity low ipEngine
log verbosity low ipEngineering
log verbosity low ipGeneral
log verbosity low ipInterface
log verbosity low ipNhopTrackerEngineering
log verbosity low ipNhopTrackerGeneral
log verbosity low ipProfileMgr
log verbosity low ipProfileMgrEngineering
log verbosity low ipRoutePolicy
log verbosity low ipRoute
log verbosity low ipTraffic
log verbosity low ipTunnel
log verbosity low ripEngineering
log verbosity low ripGeneral
log verbosity low ripRoute
log verbosity low ripRtTable
bandwidth oversubscription
ip domain-lookup
ip name-server 10.2.0.3
ip domain-name 789df
ip explicit-path name xyz disable
interface ip 0/0
interface ip 2/0
 --More--
```

Example 3 In the following example, the output is displayed until the screen is filled and the --More-- prompt appears. By entering the filter **-!**, the user forces the system to filter out all comments from the remainder of the output; that is, output lines that contain the string *!*. The system displays only lines that do not contain the string *!*.

```
host1#show config include-defaults
! Configuration script being generated on FRI AUG 04 2006 12:48:48 UTC
! Juniper Edge Routing Switch ERX-700
! Version: 7.3.0 beta-1.6 [BuildId 5672] (July 11, 2006  11:58)
! Copyright (c) 1999-2006 Juniper Networks, Inc.  All rights reserved.
!
boot config running-configuration
boot system erx_7-3-0.rel
boot config running-configuration
boot system 3-3.1.rel
no boot backup
no boot subsystem
no boot backup subsystem
boot revert-tolerance 3 1800
no boot force-backup
!
aaa domain-map jacksonville
 virtual-router miami
 strip-domain disable
!
aaa domain-map jak
 virtual-router default
 strip-domain disable
!
aaa domain-map northeast
 virtual-router default
--More--
-!
(Displaying only lines that exclude '!'. press ^C to end...)
 strip-domain disable
aaa delimiter realmName "/"
hostname host1
no aaa new-model
no service ctrl-x-reboot
no service password-encryption
no baseline show-delta-counts
clock timezone UTC 0 0
no exception dump
exception protocol ftp anonymous null
line vty 4
 exec-timeout 0 0
 exec-banner
 motd-banner
 timeout login response 30
 data-character-bits 8
 no login
log engineering
log verbosity low
no log severity
log verbosity low NameResolverLog
log verbosity low aaaAtm1483Cfg
log verbosity low aaaEngineGeneral
log verbosity low aaaServerGeneral
log verbosity low aaaUserAccess
log verbosity low addressServerGeneral
log verbosity low atm
log verbosity low atm1483
```

```
log verbosity low atmAal5
log verbosity low bgpConnections
log verbosity low bgpDampening
log verbosity low bgpEng1
--More--
```

Responding to Prompts

For some actions, the system prompts you for a response. The acceptable default responses are the following:

- You can press **y** or Enter to agree with the prompt and continue.
- You can press any other key to disagree with the prompt and cancel the action.

You can use the **confirmations explicit** command to require a more explicit response to CLI prompts.

confirmations explicit

- Use to require an explicit response to a CLI prompt, as follows:
  - To agree with the prompt and continue, you must type **y** and press Enter, type **ye** and press Enter, or type **yes** and press Enter.
  - To disagree with the prompt and cancel the action, you must type **n** and press Enter or type **no** and press Enter.
  - Pressing Enter alone, or entering any other characters, is not an acceptable response, and the CLI will repeat the prompt.
- Acceptable responses to a prompt are not case sensitive.
- Use the **no** version to restore the default state, where pressing **y** or Enter alone responds in the affirmative, and any other entry is accepted as a negative response.

NOTE: The system's CLI supports a powerful command-line editor, enabling you to easily correct, edit, and recall previously entered commands. For more information, see *Using Command-Line Editing* on page 66.

For a description of the commands that you use to get around the CLI, see *Chapter 5, Managing the System*.

CLI Status Indicators

The E-series software includes two types of indicators to inform you of the status of your CLI operation.

- The **dot service** indicator is used when your operation does not finish within 2 seconds. The service displays the Please wait message and a dot every 5 seconds until the operation is completed. The dot service is used for all CLI operations, except those that use the more descriptive progress indicator.
- The **progress indicator** is an animated representation of how much progress has been made on a CLI operation that does not finish within the expected completion time. This type of status indicator is supported for the file system synchronization application and the file copy application.

The progress indicator displays a series of dots that represents the time required to complete the operation. The dots are followed by the actual percentage of the total that has been completed and by an oscillating asterisk that indicates ongoing activity.

As the application progresses, the dots are replaced with asterisks, starting at the left, to represent how much of the operation is finished. The actual percentage is also adjusted accordingly. When the operation is complete, all dots are replaced by asterisks, and the message DONE replaces the numerical percentage.

The number of dots that appears and the percentage of completion represented by each dot or asterisk are based on the terminal width. For example, if the terminal is set to 80 characters, each of the 50 dots indicates 2 percent of the total time (2 percent x 50 characters = 100 percent). See *Chapter 5, Managing the System* for information about setting the terminal width.

The following examples show progress indicator output for a 50-character-wide display.

```
*****..................................... (10%) *

**********************************************..... (90%) *

************************************************** (DONE)
```

Levels of Access

The CLI has two levels of access: *user* and *privileged*.

User Level

User level allows you only to view a router's status. This level restricts you to User Exec mode.

Privileged Level

Privileged level allows you to view a router configuration, change a configuration, and run debugging commands. You need a password to access this level. This level gives you full CLI privileges. Passwords are covered in more detail in *Chapter 9, Passwords and Security*.

Initialization Sequence

Each line module in a router is initialized independently. As a result, the CLI on the SRP module can become available before the line modules have completed initialization. Commands relating to a line module can fail if the module has not completed initialization. The **show version** command can be used to display line module status. Do not enter commands for a line module until its state is online.

Platform Considerations

The CLI is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Accessing the CLI

This section describes logging in to and exiting from the router.

Logging In

The system supports a local console session and up to 30 virtual terminal (vty) sessions simultaneously. A virtual terminal session can be a Telnet session, Secure Shell Server (SSH) protocol session, or File Transfer Protocol (FTP) server session.

NOTE: The vty session factory default is 5. Use the **line** command to configure up to a maximum of 30 vtys. The configured vtys are shared among all types of connections; for example, if you configure 7 vtys, then no more than a total of 7 SSH plus FTP plus Telnet sessions can simultaneously exist on the router.

To access the system through a local console, attach a terminal to the system console port. To access the system through Telnet, Telnet client software must be installed on your host system. To access the system through SSH, SSH version 2.0 client software must be installed on your host system. To access the system through FTP, FTP client software must be installed on your host system.

You can configure Telnet to validate login requests. See *Vty Line Authentication and Authorization* in *Chapter 9, Passwords and Security*, for more information. Once Telnet is running on your host system, type in the E-series router name or its IP address and press Enter. To use a name, your network must have a name server.

For example, for Microsoft Windows NT enter:

telnet 192.168.1.13

or

telnet westford2

You are connected to your E-series router when the following prompt appears:

```
Logging in.
host1>
```

NOTE: At this point, you have access only to User Exec commands.

To connect through SSH, refer to your SSH client documentation.

Privileged-Level Access

You access the CLI Privileged Exec commands using the **enable** command.

Defining CLI Levels of Privilege

The CLI has the ability to map any command to one of 16 levels of command privilege (0 to 15). When you access the Privileged Exec mode, you have access to those commands that map to your access level or below. In other words, if you access the Privileged Exec mode at access level 10 (the default), you have access to all commands with an access level setting of 10 or lower.

In general, command privileges fall within one of the following levels:

- 0—Allows you to execute the **help**, **enable**, **disable**, and **exit** commands
- 1—Allows you to execute commands in User Exec mode plus commands at level 0
- 5—Allows you to execute Privileged Exec **show** commands plus the commands at levels 1 and 0
- 10—Allows you to execute all commands except support commands, which may be provided by Juniper Networks Customer Service, or the **privilege** command to assign privileges to commands
- 15—Allows you to execute support commands and assign privileges to commands

For information about how to set individual command levels, see *CLI Command Privileges* on page 50.

Accessing the Privileged Exec Level

You can access the Privileged Exec commands using one of 16 levels of command privilege. If you do not enter a privilege level and you are not accessing the router through a RADIUS authentication account, the default CLI access level is 10.

To access the default Privileged Exec mode:

1. At the prompt, type **enable** and press Enter.

```
host1>enable
Password:
```

NOTE: You will be prompted for a password only if your system has been configured with one. Refer to the **enable secret** and **enable password** Global Configuration commands described in *Chapter 9, Passwords and Security*.

2. Type your password and press Enter.

```
Password:******<Enter>
host1#
```

You can tell that you have access to Privileged Exec mode when the command prompt changes from a > character to a # character.

enable

- Use to move from User Exec to Privileged Exec mode.
- Privileged Exec mode allows you to access all other user interface modes. From here you can configure, monitor, and manage all aspects of the router.
- You can access the Privileged Exec commands using one of 16 levels of command privilege. If you do not enter a privilege level and you are not accessing the router through a RADIUS authentication account, the default CLI access level is 10.
- Set a password for this mode by using either the **enable password** or the **enable secret** command in Global Configuration mode. This protects the system from any unauthorized use.
- Once a password is set, anyone trying to use Privileged Exec mode will be asked to provide the password.
- Example 1 (accessing Privileged Exec mode at the default level [10])

```
host1>enable
password:*******
host1#
```

- Example 2 (accessing Privileged Exec mode at the highest level [15]; a password is not set for this example)

```
host1>enable 15
host1#
```

- There is no **no** version.

Moving from Privileged Exec to User Exec Mode

To move from the Privileged Exec mode to the User Exec mode, enter the **disable** command. For example:

```
host1#disable
host1>
```

NOTE: Using the **exit** command from either the Privileged Exec or User Exec mode logs out of the CLI.

To move to a lower Privileged Exec mode, follow the **disable** command with an access level value. For example:

```
host1#show privilege
Privilege level is 10
host1#disable 5
```

```
host1#show privilege
Privilege level is 5
```

disable

- Use to exit Privileged Exec mode and return to User Exec mode.
- Use to shift to a lower Privilege Exec mode level without returning to User Exec mode. Specifying a privilege level after the **disable** command changes the Privileged Exec mode to the lower level that you specify; you do not return to User Exec mode.
- Example 1

  ```
  host1#disable
  host1>
  ```

- Example 2

  ```
  host1#show privilege
  Privilege level is 10
  host1#disable 5
  host1#show privilege
  Privilege level is 5
  ```

- There is no **no** version.

Logging Out

You can log out of the CLI from either the User Exec and Privileged Exec modes by entering the **exit** command. For example:

```
host1>exit
logging out.
```

or

```
host1#exit
logging out.
```

CLI Command Privileges

You can change the privilege level of most commands by using the **privilege** command that is available in Global Configuration mode. To use this command, you must enable your CLI session to privilege level 15.

CLI Privilege Groups

You can change privilege group accessibility. Privilege groups are no longer required to be hierarchical. You can modify the privilege group membership and define which privilege group is a member of another privilege group.

A privilege group can contain commands and other privilege groups as members. A group always has access to commands in its own privilege group and in privilege group 0. By default, all groups have one member and a specific privilege group has access to all commands in all privilege groups with a lower number than the specific group.

A privilege group is reachable from another privilege group when it is a member of that privilege group, or a member of a group that is a member of that privilege group until a search of all member groups is exhausted. This can go through several recursions as long as there are no circular dependencies.

Privilege group 0 is not a member of any group and you cannot assign member groups to it, but it is reachable from every privilege group.

Numbers in the range 0—15 identify the 16 privilege groups. Each of the 16 groups can have a name or an alias. The default internal name is the privilege group number. By default, the groups are hierarchical and each group, with the exception of groups 1 and 0, contains one group. When a group contains a group, the contained group is a member of the original group: privilege group p has one member, privilege group p-1. For example, privilege group 15 has member 14, privilege group 14 has member 13, and privilege group 2 has member 1.

For hierarchical groups, groups 0 through 14 are reachable from privilege group 15, groups 0 through 13 are reachable from privilege group 14, groups 0 to 4 are reachable from 5, and so forth. Hierarchical groups can also contain other privilege groups. For example, group A is reachable from group B if group A is a member of group B or is a member of a group that is a member of group B. If group X has member Y and Y has member Z then Z is reachable from X.

You cannot configure circular dependencies. For example, you cannot configure a circular dependency where group X has member Y, Y has member Z, Z has member P, and X can reach Z and P. Group X cannot have member Z or P because Z and P are reachable through Y.

Examples Using Privilege Group Membership

In each of the following examples, privilege groups are at the default setting, where privilege group 0 is reachable from every privilege group, 15 contains 14, 14 contains 13, 13 contains 12, and so forth. The commands in each example change the privilege group settings from the default.

Example 1

```
host1(config)#privilege-group membership clear 11
host1(config)#privilege-group membership 15 add 10
```

In Example 1:

- Privilege group 11 does not contain any privilege groups
- Privilege group 15 contains group 10. Therefore, privilege group 10 and all groups contained or reachable from privilege group 10 are now reachable from privilege group 15.
- Because privilege group 15 already contains privilege group 14, all groups with the exception of privilege group 11 are reachable from privilege group 15.
- A command that is in privilege group 11 can only be executed by a user at privilege 11. A user at any other privilege does not have access to privilege group 11 commands.

Example 2 host1(config)#**privilege-group membership 14 remove 13**

In Example 2:

- Privilege group 14 does not contain any privilege groups.
- Privilege group 15 contains two groups: 14 and 10. The privilege groups 0, 1, 2, 4, 5, 6, 7, 8, 9, 10, and 14 are reachable from privilege group 15.
- A user at privilege 15 does not have access to commands in privilege groups 11, 12, or 13.

Example 3
```
host1(config)#privilege-group membership clear 13
host1(config)#privilege-group membership 13 add 10
```

In Example 3:

- Commands are executed in the following sequence: 15 contains 14, 14 contains 13, 13 contains 12, and so forth,
- Privilege group 13 contains one privilege group: privilege group 10.
- The privilege groups 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 are reachable from privilege group 13.

Example 4
```
host1(config)#privilege-group membership 12 remove 11
host1(config)#privilege-group membership 12 add 5
host1(config)#privilege-group membership 11 add 5
```

In Example 4:

- Commands are executed in the following sequence: 15 contains 14, 14 contains 13, 13 contains 12, and so forth.
- Privilege group 12 contains one privilege group: the privilege group 5.
- Privilege group 11 contains one privilege group: the privilege group 5.
- Privilege groups 0, 1, 2, 3, 4, 5 are reachable from privilege groups 12 and 11.

Example 5
```
host1(config)#privilege-group membership clear 9 8 7
host1(config)#privilege-group membership 7 add 1
host1(config)#privilege-group membership 8 add 14
```

In Example 5:

- Privilege group 9 contains no privilege groups.
- Privilege group 8 contains group 14.
- Privilege group 7 contains group 1.

Example 6
```
host1(config)#privilege-group alias 13 LI
host1(config)#privilege-group alias 10 dailyAdmin
host1(config)#privilege-group alias 7 weekendAdmin
host1(config)#privilege-group alias 6 dailyTroll
```

```
host1(config)#privilege-group alias 5 basicUser
host1(config)#privilege-group alias 0 minUser
host1(config)#privilege-group alias 15 superUser
```

In Example 6, a number or name can specify the seven privilege groups 0, 5, 6, 7, 10, 13, and 15.

Example 7

```
host1(config)#privilege-group membership clear dailyAdmin
host1(config)#privilege-group membership dailyAdmin add dailyTroll
```

In Example 7, privilege group 10 alias dailyAdmin has one member: privilege group 6 alias dailyTroll.

Example 8

```
host1(config)#no privilege-group membership 9
```

Example 8 reverts one privilege group membership to its default setting. Prior to the execution of this command, the following group memberships were in place:

group	member	reachable
8	12	12,0
9	--	0
10	9	9,0
11	10	10,9,0
12	11	11,10,9,0

Reverting privilege group 9 to its default gives it one member: privilege group 8. This creates the circular dependency: 8 contains 12, 12 contains 11, 11 contains 10, 10 contains 9, and 9 contains 8.

Example 9

```
host1(config)#no privilege-group membership
```

In Example 9, privilege group membership reverts to the default setting. All privilege groups revert to hierarchical settings: 15 contains 14, 14 contains 13, 13 contains 12, and so forth. Privilege group 0 is reachable from every privilege group.

Example 10

```
host1(config)#no privilege-group membership 7
```

In this example, one privilege group membership reverts to its default setting. Privilege group 7 contains group 6.

Example 11

```
host1(config)#no privilege-group alias
```

In Example 11, all alias settings are removed.

Example 12

```
host1#show privilege group

privilege      privilege          directly          all
 group          group              reachable      reachable
               alias              groups           groups *
----------    ----------        --------       -----------------
0             minUser           --             --
1             --                --             0
2             --                1              0 1
3             --                2              0 1 2
4             --                3              0 1 2 3
```

```
5             basicUser         4             0 1 2 3 4
6             dailyTroll        5             0 1 2 3 4 5
7             weekendAdmin      1             0 1
8             --                14            0 14
9             --                --            0
10            dailyAdmin        6             0 1 2 3 4 5 6
11            --                5             0 1 2 3 4 5
12            --                5             0 1 2 3 4 5
13            LI                10            0 1 2 3 4 5 6 10
14            --                --            0
15            superUser         10 14         0 1 2 3 4 5 6 10 14 15

*Privilege Group can reach itself
```

Example 12 shows privilege group overrides in effect.

Example 13

```
host1#show privilege group 15 superUser
The following groups are directly reachable:
14
dailyAdmin

The following groups are reachable:
1
14
2
3
4
basicUser
dailyAdmin
dailyTroll
minUser
```

In Example 13, groups 14 and dailyAdmin are directly reachable and groups 1, 14, 2, 3, 4, basicUser, dailyAdmin, dailyTroll, and minUser are reachable.

privilege

- Use to change the privilege level of any command within a specified mode.
- Example 1

  host1(config)#**privilege exec level 12 terminal width**

- Example 2

  host1(config)#**privilege exec all level 5 terminal**

- Use the **all** keyword to change the privilege level of groups of commands. For more information, see *Setting Privilege Levels for Multiple Commands* on page 57.
- Use the **reset** version to restore the default privilege level for the command; issuing this command results in the **show configuration** command not showing the default privilege setting for the command.
- Use the **no** version to restore the default privilege level for the command; issuing this command results in the **show configuration** command showing the default privilege level of the command in its output.

NOTE: You must access the CLI at privilege level 15 to view or use this command.

privilege-group alias

- Use to give the privilege group name alias to the privilege group.
- Example

  host1(config-if)#**privilege-group alias**

- Use the **no** version to remove the privilege group alias.

privilege-group membership

- Use to add the member group to or remove the member group from the privilege group.
- Example

  host1(config-if)#**privilege-group membership**

- Use the **no** version to restore one or all privilege groups to the default settings. When all privilege groups are reset to the default settings, the privilege group membership is hierarchical.

privilege-group membership clear

- Use to clear a privilege group or all members from a privilege group.
- Example

  host1(config-if)#**privilege-group membership clear**

- There is no **no** version.

CLI Command Exceptions

Changing command privilege levels can be a powerful security tool. However, changing the command privilege for some commands could render the CLI unusable and require you to reboot the router. To eliminate this possibility, the CLI does not allow you to remap the following commands:

- **disable**
- **enable**
- **exit**
- **help**
- **privilege**
- **support**

CLI Keyword Mapping

You cannot change the privilege level of keywords that are separated from the command string by a parameter in the command sequence. In other words, once the privilege algorithm reaches a parameter, the privilege algorithm that maps the commands to the desired privilege level stops and allows any keyword options that may follow in the command sequence. The algorithm then waits for a carriage return before looking at the next command sequence.

For example, you can change the command privilege level for the **telnet** command. However, because the **telnet** command is immediately followed by a variable (that is, a hostname or IP address) and not a keyword, you cannot change the privilege level for any keywords that follow the command.

```
host1#telnet ?
  HOSTNAME or A.B.C.D  The ip address of the remote system

host1#telnet router2 ?
  <0 - 65535>       The port on which to send the request
  bgp               Border Gateway Protocol (179)
  chargen           Character generator (19)
  cmd               Remote commands (rcmd, 514)
  .
  .
  .
```

Setting Privileges for Ambiguous Commands

The **privilege** command allows you to set command privilege levels for parts of commands that the CLI would normally consider ambiguous. In other words, you can set privilege levels by specifying letters that represent only the beginning part of a command or group of commands (even the first letter of a command or group of commands).

The following example sets the privilege level to 12 for any Exec mode (user or privileged) command that start with the letter "t":

```
host1(config)#privilege exec level 12 t
```

The list of affected commands includes **telnet**, **terminal**, **test**, and **traceroute**.

The following example changes all the above commands, with the exception of the **traceroute** command, to level 15:

```
host1(config)#privilege exec level 15 te
```

The following example changes all commands that start with the letters "te" (for example, **telnet**, **terminal**, and **test**) and any second keyword that starts with the letter "i" and follows a command that starts with the letters "te" (for example, the keyword "ip" in the command **test ip**) to level 1:

```
host1(config)#privilege exec level 1 te i
```

When you enter an ambiguous command and an exact match of the command is found, partial matches are ignored and are not modified.

For example, the **traffic-class** and **traffic-class-group** commands are available in Global Configuration mode. If you issue the **privilege configure level 5 traffic-class** command, an exact match is made to **traffic-class**, and **traffic-class-group** is not modified.

If you want to set the privilege level for both **traffic-class** and **traffic-class-group** and you do not want the exact match to be made to **traffic-class**, issue a partial command such as **traffic-c**. The privilege level of all commands that begin with **traffic-c** is modified.

Setting Privilege Levels for no or default Versions

The **privilege** command allows you to set command privilege levels for **no** and **default** versions of commands. However, setting the privilege level for either the **no** or **default** versions of a command does *not* set the privilege level of the affirmative version of the command. This means that you can have the **no** or **default** version of a command at a different privilege level than its affirmative version.

NOTE: You can set the **no** or **default** command to a separate privilege level without specifying any other command to follow. This would force all commands that have a **no** or **default** version to function only for that privilege level and higher.

For example, if you issue the **privilege exec level 10 no** command, all **no** versions in the Privileged Exec mode are available to users at level 10 and higher.

Setting Privilege Levels for Multiple Commands

The **all** keyword is a wildcard parameter that enables you to set privilege levels for multiple commands rather than setting them individually.

Setting Privilege Levels for All Commands in a Mode

You can set the privilege level for all commands within a specified mode. This setting includes all commands in modes that you can access from a specified mode.

If the command specified in the **privilege** command changes the configuration mode, all commands in the configuration will also be set to the specified privilege level. For more information about accessing modes, see *Accessing Command Modes* on page 68.

For example, issuing the **configure** command in Privileged Exec mode changes the configuration mode to Global Configuration. If you issue the **privilege exec all level 5 configure** command, all commands in Global Configuration mode become accessible to users who have CLI privileges at level 5 and higher. For more information about user privilege levels, see *Privileged-Level Access* on page 48.

Setting Privilege Levels for a Group of Commands

You can set the privilege level for a group of commands by using the beginning keyword in a command.

For example, if you issue the **privilege configure all level 5 snmp** command, all commands in Global Configuration mode that begin with **snmp** become accessible to users who have CLI privileges at level 5 and higher.

Using the Order of Precedence

The effectiveness of a privilege level that is set with the **all** keyword depends on its precedence level in the CLI. A privilege level is considered to be in effect only if a privilege level that is configured at a higher precedence level does not override it.

The CLI uses the following order of precedence:

1. Privilege level set for all commands within a mode, including modes that are accessed from another mode; for example, Global Configuration mode

2. Privilege level set for all commands that begin with the same keyword; for example, **snmp** commands

3. Privilege level set for individual commands; for example, **snmp-server community**

NOTE: This order of precedence does not apply to privilege levels that are set without the **all** keyword.

In the following example, the privilege level of the **snmp-server community** command is set to level 11, the privilege level for all commands that begin with **snmp** is set to level 10, and the privilege level for all commands in Global Configuration mode is set to level 5.

```
host1(config)#privilege configure level 11 snmp-server community
host1(config)#privilege configure all level 10 snmp
host1(config)#privilege exec all level 5 configure
```

The following **show configuration** output displays the privilege levels set above. The privilege levels for the **snmp-server community** command and the **snmp-server** group of commands are still present in the output. However, the privilege level of Global Configuration mode takes precedence, and the privilege levels of the other commands are rendered ineffective. Users can access all **snmp** commands at level 5 or higher.

```
host1#show config category management cli command-privileges
privilege configure level 11 snmp-server community
privilege configure all level 10 snmp-server
privilege exec all level 5 configure
```

Superseding Privilege Levels with the all Keyword

Issuing the **all** keyword supersedes privilege levels that were previously set without the **all** keyword.

In the following example, the **snmp-server-community** command is set to level 7, and the **snmp** keyword is set to level 6. The privilege level of the **snmp** keyword does not override the **snmp-server community** setting, because both of these commands are set without the **all** keyword.

```
host1(config)#privilege configure level 7 snmp-server community
host1(config)#privilege configure level 6 snmp
```

All **snmp** commands are then changed to level 5 with the **all** keyword.

```
host1(config)#privilege configure all level 5 snmp
```

The **show configuration** output displays all **snmp** commands at level 5, superseding the existing level 6 setting. The **snmp-server community** command is still present in the show configuration output, but it is ineffective.

```
host1#show config category management cli command-privileges
privilege configure level 7 snmp-server community
privilege configure all level 5 snmp-server
```

Removing the all Keyword

Using the **no** version or **reset** version removes the **all** keyword and restores default privilege levels.

If the privilege setting of the mode or command for which you are restoring default privilege levels takes precedence over any ineffective privilege settings, those settings will automatically take effect according to the order of precedence (see *Using the Order of Precedence* on page 58).

The difference between the **no** version and the **reset** version is that the **reset** version removes the configuration from the **show configuration** output. This is useful when you want to remove a configuration that has been overridden and rendered ineffective by a privilege level that takes precedence.

Setting Default Line Privilege

The factory default privilege level for the console line and all vty lines is 1. However, you can use the **privilege level** command in Line Configuration mode to set the default login privilege for the console line or any number of vty lines.

To change the default privilege level:

1. Access line configuration mode on the router for the console.

   ```
   host1(config)#line console 0
   host1(config-line)#
   ```

   or on one or more vty lines

   ```
   host1(config)#line vty 0 12
   host1(config-line)#
   ```

NOTE: The latter command configures vty lines 0 to 12.

2. Specify a starting privilege level for the line or lines.

   ```
   host1(config-line)#privilege level 5
   ```

The default privilege level for the specified line (or lines) changes. The new values take effect immediately for any new users. If using the console line, you must exit out of the CLI and reestablish a connection before the default takes effect.

If you are validating through RADIUS or TACACS+ and the server specifies an enable level, that enable level takes precedence over the line privilege level.

privilege level

- Use to change the default privilege level of the console line or one or more vty lines.
- Example

  host1(config-line)#**privilege level 5**

- Use the **no** or **default** version to restore the default privilege level for the command.

NOTE: You must access the CLI at privilege level 15 to view or use this command.

Viewing CLI Privilege Information

You can view CLI privilege information for yourself (the current user), all connected users on the router, or for any modified CLI commands.

Viewing the Current User Privilege Level

Use the **show privilege** command to view your current privilege level.

show privilege

- Use to view your current privilege level.
- Example

  host1#**show privilege**
  Privilege level is 10

- There is no **no** version.

Viewing Privilege Levels for All Connected Users

Use the **show users detail** command to view the privilege levels for all users currently connected to the router. See *Monitoring the FTP Server* on page 265 for information about the **show users detail** command.

Viewing Privilege Levels for Changed CLI Commands

Use the **show configuration** command to view the changed privilege levels for any modified CLI commands. See *Saving the Current Configuration* on page 235 for information about the **show configuration** command.

NOTE: The **show configuration** command output displays output specific to the session access level. For example, if the session is enabled at level 5, issuing the **show configuration** command displays only output for commands at level 5 and below.

show privilege group

- Use to view the privilege groups.
- Example

```
host1(config-if)#show privilege group superUser
The following groups are directly reachable:
14
dailyAdmin

The following groups are reachable:
1
14
2
3
4
basicUser
dailyAdmin
dailyTroll
minUser
```

- There is no **no** version.

Using Help

The system CLI provides a variety of useful context-sensitive help features. An important thing to remember about using the help features is that the use of a space or the lack of a space before the **?** gives different results. Table 7 describes the help system.

Table 7: Help Commands

Command	Description
?	Lists all keywords applicable to the current command mode
help	Displays a brief description of the help system (available in all command modes)
partial-keyword?	Lists the keywords that begin with a certain character string
partial-keyword < Tab >	Completes the partial keyword you entered, if you have provided an unambiguous abbreviation
command < Space > ?	Lists the set of all valid next available choices

Commands listed in the left column of Table 7 are further described with examples in the following sections.

? (Question Mark Key)

You can use the question mark (**?**) key whenever you need additional information. When you enter **?**, all available choices are displayed. The CLI then redisplays the command you typed. The following examples show different ways you can use the **?** key.

When you use **?** on a line by itself or when it is preceded by one or more spaces, a list of all next available choices is displayed.

Example 1

```
host1(config)#?
  aaa                       Configure authentication, authorization, and
                            accounting characteristics
  access-list               Configure an access list entry
  arp                       Configure a static ARP entry
  bandwidth                 Configure slot-group bandwidth control
  banner                    Define a banner line
  baseline                  Configure baseline operations
  boot                      Configure boot time behavior
  bulkstats                 Configure bulkstats parameters
  classifier-list           Configure a classifier list entry
  clns                      Configure CLNS characteristics
  clock                     Set the system's clock
  confirmations             Configure confirmation mode
  controller                Configure controller parameters
  crypto                    Configure cryptographic parameters
  default                   Set a command to its default(s)
  disable-autosync          Disable automatic synchronization of redundant
                            system controller file system
  disable-switch-on-error   Disable automatic switch to redundant system
                            controller upon software/hardware error
  do                        Run an exec mode command (alias command run)
  enable                    Configure security related options
  end                       Exit Global Configuration mode
  exception                 Configure core dump
  exclude-subsystem         Exclude copying a subsystem from the release
  exit                      Exit from the current command mode
  ftp-server                Configure FTP Server characteristics
  help                      Describe the interactive help system
  host                      Add/modify an entry to the host table
  hostname                  Set the host (system) name
  interface                 Enter Interface Configuration mode
  ip                        Configure IP characteristics
  l2tp                      Configure L2TP parameters
  license                   Configure licenses
  line                      Enter Line Configuration mode
  log                       Configure logging settings
  macro                     Run a CLI macro
  map-list                  Create an NBMA static map
  memory                    Configure and administer memory operations
  mpls                      Configure MPLS global parameters
  no                        Negate a command or set its default(s)
  ntp                       Configure the Network Time Protocol
  policy-list               Enter Policy Configuration mode
  pppoe                     Configure PPPoE
  profile                   Specify a profile
  radius                    Configure RADIUS server
```

```
  rate-limit-profile       Enter rate limit profile configuration mode
  redundancy               Perform a redundancy configuration
  route-map                Configure a route map
  router                   Configure a routing protocol
  rtr                      Configure rtr parameters
  run                      Run an exec mode command (alias command do)
  service                  Configure system-level services
  set                      Configure
  sleep                    Make the Command Interface pause for a specified
                           duration
  slot                     Configure and administer slot operation
  snmp-server              Configure SNMP parameters
  sscc                     The SSC Client telnet
  telnet                   telnet daemon configuration
  timing                   Configure network timing
  traffic-shape-profile    Enter traffic shape profile configuration mode
  virtual-router           Specify a virtual router
```

Example 2

```
host1(config)#ip ?
address-pool                Configure address pool for PPP Broadband RAS
                            clients
  as-path                   Configure a path filter for AS-Paths in BGP
  bgp-community             Format for BGP community
  community-list            Configure an entry in a community list
  debounce-time             Specify the minimum amount of time that an event
                            needs to be in same state before being reported
  dhcp-local                The DHCP Local Server protocol
  dhcp-server               DHCP Server for Proxy Client
  domain-lookup             Enable DNS lookup
  domain-name               Specify local Domain name
  dvmrp                     configure dvmrp paramaters
  dynamic-interface-prefix  Specify name prefix for dynamic Ip shared
                            interfaces
  explicit-path             Configure an explicit path
  extcommunity-list         The extended community list
  ftp                       Configure FTP characteristics
  http                      Configure http server
  local                     Local IP address assignment
  multicast-routing         Enable IP multicast forwarding
  name-server               Configure DNS server
  pim                       Configure PIM Protocol
  prefix-list               Configure a prefix list entry
  prefix-tree               Configure a prefix tree entry
  route                     Define a static IP route
  router-id                 Configure the router-id to be used
  rpf-route                 Define a static IP route for mcast RPF check
  source-route              Configure source-routing capabilities
  ssh                       Configure SSH characteristics
  ttl                       Configure the default value to be used by IP for
                            Time-To-Live
  tunnel                    Configure tunnel parameter
  vpn-id                    Configure the VPN ID associated with this router
  vrf                       Specify a VRF

host1(config)#ip
```

Example 3

```
host1(config)#ip community-list ?
<1 - 99>  The community list

host1(config)#ip community-list
```

When you want to see a list of commands that begin with a particular set of characters, type a question mark (**?**) immediately after the last letter. Do not use a space between the partial keyword and the **?** key. For example:

```
host1#sh?
show shutdown
host1#sh
```

NOTE: If you want to use the **?** character as part of a string, such as a hostname or a regular expression, you must enter the following key sequence: Ctrl + v + ?. Otherwise, the CLI considers the **?** to be a request for assistance in completing the command.

help Command

Use the **help** command when you want to see a brief description of the context-sensitive help system.

```
host1>help
Use the help options as follows:

?, or command<Space>? - Lists the set of all valid next keywords or arguments
partial-keyword?      - Lists the keywords that begin with a certain character
                        string
partial-keyword<Tab>  - Completes the partial keyword
host1>
```

Partial-keyword <Tab>

When you cannot recall a complete command name or keyword, type in the first few letters, press Tab, and the system completes your partial entry. You must type enough characters to provide a unique abbreviation. If you type a few letters, press Tab, and your terminal beeps, then you have not typed enough characters to be unambiguous.

```
host1(config)#int<Tab>
host1(config)#interface
```

Using Command-Line Editing

This section provides information about the command-line editor.

Basic Editing

Here are a few basic command-line editing notes:

- Case—Keywords are not case sensitive; that is, they can be entered in uppercase, lowercase, or a mix of both. Filenames may be case sensitive. Local filenames are case sensitive; remote filenames are case sensitive if the host system treats filenames as case sensitive. Passwords are case sensitive.
- Abbreviating keywords—You may abbreviate keywords using as few characters as you want, as long as the characters provide a unique abbreviation.
- Executing a command—Always use the Enter key.

Command-Line Editing Keys

You can use several keys to edit the command line. Table 8 defines the keys for editing the command line. Arrow keys functions only on ANSI-compatible terminals, such as VT100s.

Table 8: Command-Line Editing Keys

Key(s)	Function
Delete *or* Backspace	Removes characters to left of cursor
Left Arrow	Moves cursor one character to left
Right Arrow	Moves cursor one character to right
Ctrl + a	Moves cursor to beginning of command line
Ctrl + b	Moves cursor back one character
Ctrl + d	Deletes character at cursor
Ctrl + e	Moves cursor to end of command line
Ctrl + f	Moves cursor forward one character
Ctrl + h	Deletes character to left of cursor
Ctrl + k	Deletes all characters from cursor to end of command line
Ctrl + l	Redisplays system prompt and command line
Ctrl + o	Toggles overwrite/insert mode
Ctrl + t	Transposes character to left of cursor with character located at cursor
Ctrl + u	Deletes entire command line
Ctrl + v	Allows the “?” character to be used as a character instead of as a request for help
Ctrl + w	Deletes the previous word

Table 8: Command-Line Editing Keys (continued)

Key(s)	Function
Ctrl + x	In all modes, reboots the system. This feature is useful if a command is taking a prolonged time to complete and hangs the console. The command has no effect if you access the system through Telnet. Set the boot option flag by using the **service ctrl-x-reboot** command from Global Configuration mode.
Ctrl + y	Recalls most recent entry from delete buffer; recalled characters overwrite or are inserted in current line depending on overwrite/insert toggle
Ctrl + z	In all modes except User Exec mode, executes any command typed immediately before the command sequence and then changes the mode to Privileged Exec mode. In User Exec mode, only executes any command typed immediately before the command sequence.
Esc + b	Moves cursor back one word
Esc + Backspace	Deletes previous word
Esc + d	Deletes current or next word

Command History Keys

The CLI maintains two separate command histories. The first command history maintains only Exec mode commands. The second history maintains all commands entered in any of the configuration modes. The appropriate history will automatically be restored as you transition between Global Configuration mode and Exec mode.

Table 9 defines the keys related to command history. Arrow keys functions only on ANSI-compatible terminals, such as VT100s.

Table 9: Command History Keys

Key	Function
Up Arrow *or* Ctrl + p	Recalls commands in history buffer, starting with most recent command. Repeat key sequence to recall successively older commands.
Down Arrow *or* Ctrl + n	Returns to more recent commands in history buffer after recalling commands with Up Arrow or Ctrl + p. Repeat key sequence to recall successively more recent commands.
Ctrl + r	Begin a *reverse search* for a previously entered string in the history buffer by providing a character string when prompted. Enter Ctrl + r to continue searching. Ctrl + h or Del deletes the last character in the string and starts a search on the new string.

Pagination Keys

If the system needs to display more text than you can fit on the screen, the output pauses and the --More-- prompt appears. Table 10 defines the pagination keys that you can use when the --More-- prompt appears. For more information, see *The - -More- - Prompt* on page 41.

Table 10: Pagination Keys

Key	Function
Enter	Scrolls down one more line
Spacebar	Displays one more screen
+	Displays all output lines that contain the text string
–	Displays all output lines that do not contain the text string
/	Displays all output lines starting at the first line that contains the text string
Any other key	Aborts output and returns you to command prompt

Accessing Command Modes

Table 11 describes the command modes available in the CLI.

Table 11: Command Mode Overview

Mode Name	Use of Mode	Access to Mode	Exit from Mode
AAA Profile Configuration	■ Configure new AAA profiles.	■ From Global Configuration mode, use **aaa-profile** command. ■ Prompt: `host1(config-aaa-profile)#`	■ Use the **exit** command to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Address Family Configuration	■ Configure BGP or RIP address family parameters.	■ From Global Configuration mode, use **router bgp** or **router rip** to enter Router Configuration mode. From Router Configuration, use the **address-family** command. ■ Prompt: `host1(config-router-af)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
ATM VC Class Configuration	■ Configure a class of attributes for an ATM data PVC.	■ From Global Configuration mode, use the **vc-class atm** command, and specify the name of the VC class. ■ Prompt: `host1(config-vc-class)#`	■ Use the **exit** command to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
ATM VC Configuration	■ Configure individual attributes for an ATM data PVC.	■ From Global Configuration mode, use the **interface** command to enter Subinterface Configuration mode. From Subinterface Configuration mode, use the **pvc** command. ■ Prompt: `host1(config-subif-atm-vc)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
Classifier Group Configuration	■ Configure classifier groups with policy rules used for policy lists.	■ To create a classifier group, from Policy List Configuration mode use the **classifier-group** command and identify the CLACL and precedence. ■ Prompt: `host1(config-policy-list-classifier-group)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Color Mark Profile Configuration	■ Configure packet color after exit from rate-limit hierarchy.	■ From Rate Limit Profile Configuration Mode, use the **color-mark-profile** command and identify the interface type (IP, IPv6, MPLS). ■ Prompt: `host1(config-color-mark-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Control Plane Configuration	■ Configure SRP module policing.	■ From Global Configuration Mode, use the **control-plane** command. ■ Prompt: `host1(config-control-plane)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Controller Configuration	■ Configure physical interfaces (for example, T3).	■ From Global Configuration mode, use the **controller** command. ■ Prompt: `host1(config-controll)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
DHCP Local Pool Configuration	■ Configure DHCP local pools.	■ From Global Configuration mode, use the **ip dhcp-local pool** command. ■ Prompt: `host1(config-dhcp-local)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Domain Map Configuration	■ Configure domain maps.	■ From Global Configuration mode, use the **aaa domain-map** command. ■ Prompt: `host1(config-domain-map)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Domain Map Tunnel Configuration	■ Configure tunnel parameters.	■ From Domain-Map Configuration mode, use the **tunnel** command. ■ Prompt: `host1(config-domain-map-tunnel)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
DoS Protection Group Configuration	■ Configure parameters for DoS protection groups.	■ From Global Configuration Mode, use the **dos-protection-group** command. ■ Prompt: `host1(config-dos-group)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Drop Profile Configuration	■ Configure drop profiles.	■ From Global Configuration mode, use the **drop-profile** command. ■ Prompt: `host1(config-drop-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Explicit Path Configuration	■ Configure MPLS explicit path parameters.	■ From Global Configuration mode, specify the **mpls explicit-path name** command. ■ Prompt: `host1(config-expl-path)#`	■ Use the **exit** command to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
Flow Cache Configuration	■ Configure parameters for the aggregation cache.	■ From Global Configuration Mode, use the **ip flow-aggregation cache** command. ■ Prompt: `host1(config-flow-cache)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Global Configuration	■ Enable a feature or function. ■ Disable a feature or function. ■ Configure a feature or function.	■ From Privileged Exec mode, use the **configure** command. ■ Prompt: `host1(config)#`	■ Use the **exit** command, or press Ctrl + z to return to Exec mode. ■ Use the **interface** command to enter Interface Configuration mode.
Interface Configuration	■ Create an interface. ■ Modify the operation of an interface, such as bandwidth or clock rate.	■ From Global Configuration mode, use the **interface** command and identify the interface by slot/port. ■ Prompt: `host1(config-if)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IP NAT Pool Configuration	■ Create a NAT pool with a multiple, discontinuous range.	■ From Global Configuration mode, use the **ip nat pool** command and specify only a prefix length value. ■ Prompt: `host1(config-ipnat-pool)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IP PIM Data MDT Configuration	■ Create and activate data multicast distribution trees (MDTs)	■ From Global Configuration mode, use the **ip pim data-mdt** command and specify a name. ■ Prompt: `host1(config-ip-pim-data-mdt)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IP Service Profile Configuration	■ Create a service profile to use in route maps for subscriber management and to authenticate subscribers with RADIUS.	■ From Global Configuration mode, use the **ip service-profile** command and specify a service profile name with up to 32 ASCII characters. ■ Prompt: `host1(config-service-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IPSec CA Identity Configuration	■ Create an IPSec identity used in online certificate requests and during negotiations with IKE peers.	■ From the Global Configuration mode, use the **ipsec ca identity** command. ■ Prompt: `host1(config-ca-identity)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IPSec Identity Configuration	■ Create an IPSec identity used in offline certificate requests and during negotiations with IKE peers.	■ From the Global Configuration mode, use the **ipsec identity** command. ■ Prompt: `host1(config-ipsec-identity)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IPSec IKE Policy Configuration	■ Define an IKE policy.	■ From the Global Configuration mode, use the **ipsec ike-policy-rule** command. ■ Prompt: `host1(config-ike-policy)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
IPSec Manual Key Configuration	■ Enter manual keys.	■ From Global Configuration mode, use the **ipsec key manual pre-share** command. ■ Prompt: `host1(config-manual-key)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IPSec Peer Public Key Configuration	■ Enter an ISAKMP/IKE public key that a remote peer uses for RSA authentication without the need for a digital certificate.	■ From Global Configuration mode, use the **ipsec key pubkey-chain rsa** command. ■ Prompt: `host1(config-peer-public-key)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IPSec Transport Profile Configuration	■ Configure a profile for L2TP over IPSec.	■ From Global Configuration mode, use the **ipsec transport profile** command. ■ Prompt: `host1(config-ipsec-transport-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IPSec Tunnel Profile Configuration	■ Configure a profile for IPSec tunnels.	■ From Global Configuration mode, use the **ipsec tunnel profile** command. ■ Prompt: `host1(config-ipsec-tunnel-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
IP Tunnel Destination Profile Configuration	■ Create a profile for dynamic GRE or DVMRP tunnels	■ From Global Configuration mode, use the **gre destination profile** command or the **dvmrp destination profile** command and specify a destination profile name. ■ Prompt: `host1(config-dest-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
L2 Transport Load-Balancing -Circuit Configuration	■ Configure Martini layer 2 transport circuit associated with load-balancing group.	■ From Global Configuration mode, specify the **mpls l2transport load-balancing-group** command. ■ Prompt: `host1(config-l2transport-load-balancing-circuit)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
L2TP Destination Profile Configuration	■ Define the location of an LAC.	■ From Global Configuration mode, use the **l2tp destination profile** command. ■ Prompt: `host1(config-l2tp-dest-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
L2TP Destination Profile Host Configuration	■ Configure host profile attributes.	■ From L2TP Destination Profile Configuration mode, use the **remote host** command. ■ Prompt: `host1(config-l2tp-dest-profile-host)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
L2TP Tunnel Switch Profile Configuration	■ Configure the L2TP tunnel switching behavior for interfaces to which this profile is assigned.	■ From Global Configuration mode, use the **l2tp switch-profile** command, and specify the name of the L2TP tunnel switch profile. ■ Prompt: `host1(config-l2tp-tunnel-switch-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Layer 2 Control Configuration	■ Configure ANCP (L2C) parameters.	■ From Global Configuration mode, use the **l2c** command. ■ Prompt: `host1(config-l2c)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Layer 2 Control Neighbor Configuration	■ Configure ANCP (L2C) neighbor parameters.	■ From Layer 2 Configuration mode, use the **neighbor** command. ■ Prompt: `host1(config-l2c-neighbor)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
LDP Configuration	■ Configure MPLS LDP profile parameters.	■ From Global Configuration mode, specify the **mpls ldp profile** command. ■ Prompt: `host1(config-ldp)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Line Configuration	■ Modify a virtual terminal line.	■ From Global Configuration mode, use the **line** command. ■ Prompt: `host1(config-line)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Local IPSec Transport Profile Configuration	■ Configure preshared IKE keys for L2TP over IPSec profiles.	■ From the IPSec Transport Profile Configuration mode, use the **local ip address** command. ■ Prompt: `host1(config-ipsec-transport-profile-local)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Local User Configuration	■ Configure user parameters in local user databases.	■ From Global Configuration mode, specify the **aaa local username** or the **aaa local database** command. ■ Prompt: `host1(config-local-user)#`	■ Use the **exit** command to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Map Class Configuration	■ Specify fragmentation for a map class.	■ From Global Configuration mode, specify the **map-class frame-relay** command. ■ Prompt: `host1(config-map-class)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Map List Configuration	■ Configure map list parameters.	■ From Global Configuration mode, use the **map-list** command. ■ Prompt: `host1(config-map-list)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
Parent Group Configuration	■ Configure an external parent group.	■ From Global Configuration mode, use the **parent-group** command. ■ Prompt: `host1(config-parent-group)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Policy List Configuration	■ Configure policy lists.	■ To create a policy list, from Global Configuration mode use the **policy-list** command and identify the type of policy list. ■ Prompt: `host1(config-policy-list)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Policy List Parent Group Configuration	■ Configure an internal parent group in a hierarchy.	■ From Global Configuration Mode, use the **policy-list** command to create or access a policy list. From Policy List Configuration Mode, use the **parent-group** command. ■ Prompt: `host1(config-policy-list-parent-group)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Policy Parameter Configuration	■ Configure a policy parameter.	■ From Global Configuration mode, use the **policy-parameter** command. ■ Prompt: `host1(config-policy-parameter)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
PPPoE Service Name Table Configuration	■ Configure services for a PPPoE service name table.	■ From Global Configuration mode, use the **pppoe-service-name-table** command, and specify the alphanumeric name of the PPPoE service name table. ■ Prompt: `host1(config-pppoe-service-name-table)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Privileged Exec	■ Show system information. ■ Set operating parameters. ■ Access Global Configuration mode.	■ From User Exec mode, use the **enable** command. ■ Prompt: `host1#`	■ Use the **disable** command to return to User Exec mode. ■ Use the **exit** command to log out of the CLI. ■ Use the **configure** command to enter Global Configuration mode.
Profile Configuration	■ Configure profiles.	■ From Global Configuration mode, use the **profile** command. ■ Prompt: `host1(config-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
QoS Parameter Definition Configuration	■ Configure QoS parameter definitions.	■ From Global Configuration mode, use the **qos-parameter-define** command. ■ Prompt: `host1(config-qos-parameter-define)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
QoS Profile Configuration	■ Configure QoS profiles.	■ From Global Configuration mode, use the **qos-profile** command. ■ Prompt: `host1(config-qos-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
QoS Shared Shaper Control Configuration	■ Configure variables within the simple shared shaper algorithm.	■ From Global Configuration mode, use the **qos-shared-shaper-control** command. ■ Prompt: `host1(config-qos-shared-shaper-control)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Queue Profile Configuration	■ Configure queue profiles.	■ From Global Configuration mode, use the **queue-profile** command. ■ Prompt: `host1(config-queue)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
RADIUS Configuration	■ Configure Broadband Remote Access Server (B-RAS) parameters.	■ From Global Configuration mode, use the **radius server** command. ■ Prompt: `host1(config-radius)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
RADIUS Relay Configuration	■ Configure RADIUS relay server parameters.	■ From Global Configuration mode, use the **radius relay server** command. ■ Prompt: `host1(config-radius-relay)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Rate Limit Profile Configuration	■ Configure an IP or L2TP rate limit parameters.	■ To create an IP rate limit profile, from Global Configuration mode use the **ip rate-limit-profile** command. ■ To create an L2TP rate limit profile, from Global Configuration mode use the **l2tp rate-limit-profile** command. ■ Prompt: `host1(config-rate-limit-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Redundancy Configuration	■ Configure high availability (stateful SRP switchover).	■ From Global Configuration mode, use the **redundancy** command. ■ Prompt: `host1(config-redundancy)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Remote Neighbor Configuration	■ Configure remote neighbor parameters for OSPF, PIM, or RIP.	■ From Router Configuration mode, use the **remote-neighbor** command. ■ Prompt: `host1(config-router-rn)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Route Map Configuration	■ Configure routing tables and source and destination information.	■ From Global Configuration mode, use the **route-map** command. ■ Prompt: `host1(config-route-map)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
Router Configuration	■ Configure a routing protocol.	■ From Global Configuration mode, specify a routing protocol with the **router** command. ■ Prompt: `host1(config-router)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
RSVP Configuration	■ Configure an RSVP profile.	■ From Global Configuration mode, use the **mpls rsvp profile** command. ■ Prompt: `host1(config-rsvp)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
RTR Configuration	■ Configure RTR parameters.	■ From Global Configuration mode, use the **rtr** command. ■ Prompt: `host1(config-rtr)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Scheduler Profile Configuration	■ Configure shaping parameters. ■ Configure scheduler profiles.	■ From Global Configuration mode, use the **scheduler-profile** command. ■ Prompt: `host1(config-scheduler-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec menu.
Service Session Profile Configuration	■ Configure attributes for Service Manager service session profiles.	■ From Global Configuration mode, use the **service-management service-session-profile** command. ■ Prompt: `host1(config-service-session-profile)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
SNMP Event Manager Configuration	■ Configure SNMP events.	■ From Global Configuration mode, use the **snmp-server management-event** command. ■ Prompt: `host1(config-mgmtevent)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec menu.
Statistics Profile Configuration	■ Configure statistics profiles.	■ From Global Configuration mode, use the **statistics-profile** command. ■ Prompt: `host1(config-statistics-profile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec menu.
Subinterface Configuration	■ Configure multiple virtual interfaces on a single physical interface.	■ From Global Configuration mode, use the **interface** command and identify the interface (slot/port.subinterface). ■ Prompt: `host1(config-subif)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Subscriber Policy Configuration	■ Configure a nondefault subscriber policy for a subscriber (client) bridge group interface.	■ From Global Configuration mode, use the **subscriber-policy** command and specify the alphanumeric name of the subscriber policy. ■ Prompt: `host1(config-policy)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

Table 11: Command Mode Overview (continued)

Mode Name	Use of Mode	Access to Mode	Exit from Mode
Traffic Class Configuration	■ Configure a traffic class.	■ From Global Configuration mode, use the **traffic-class** command. ■ Prompt: `host1(config-traffic-class)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Traffic Class Group Configuration	■ Configure a traffic class group.	■ From Global Configuration mode, use the **traffic-class-group** command. ■ Prompt: `host1(config-traffic-class-group)`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Tunnel Group Configuration	■ Add up to 31 tunnel definitions to a tunnel group.	■ From Global Configuration mode, use the **aaa tunnel-group** command and specify the name of the tunnel. ■ Prompt: `host1(config-tunnel-group)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Tunnel Group Tunnel Configuration	■ Configure attributes for a tunnel group tunnel.	■ From Tunnel Group Configuration mode, use the **tunnel** command and specify the tag value (1-31) of the tunnel. ■ Prompt: `host1(config-tunnel-group-tunnel)#`	■ Use the **exit** command twice to return to Global Configuration Mode. ■ Press Ctrl + z to return to Exec mode.
Tunnel Profile Configuration	■ Configure tunnel profile parameters.	■ From Global Configuration mode, specify the **mpls tunnels profile** command. ■ Prompt: `host1(config-tunnelprofile)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
Tunnel Server Configuration	■ Configure the maximum number of tunnel-service interfaces for a dynamic tunnel-server port.	■ From Global Configuration mode, use the **tunnel-server** command and identify the slot/port location of the dynamic tunnel-server port. ■ Prompt: `host1(config-tunnel-server)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
User Exec	■ Change terminal settings on a temporary basis. ■ Show system information. ■ Access Privileged Exec mode.	■ Log into system. ■ Prompt: `host1>`	■ Use the **enable** command to enter Privileged Exec mode. ■ Use the **exit** command to log out of the CLI.
VRF Configuration	■ Configure VRF parameters for BGP/MPLS VPNs.	■ From Global Configuration mode, use the **ip vrf** command. ■ Prompt: `host1(config-vrf)#`	■ Use the **exit** command once to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.
VR Group Configuration	■ Configure a virtual router group for AAA broadcast accounting.	■ From Global Configuration mode, use **aaa accounting vr-group** to enter VR Group Configuration mode. ■ Prompt: `host1(config-vr-group)#`	■ Use the **exit** command twice to return to Global Configuration mode. ■ Press Ctrl + z to return to Exec mode.

NOTE: Within any configuration mode, the commands that are available to the user include the commands defined for that configuration mode and all commands defined for Global Configuration mode. See Figure 21 on page 29. For example, from Router Configuration mode, you could use the **interface** Global Configuration mode command without first explicitly going back to Global Configuration mode.

```
host1(router-config)# interface atm 4/0.3
host1(config-if)#
```

Exec Modes

There are two Exec modes: User Exec and Privileged Exec.

After you log in to the system, the CLI is in User Exec mode. By default, the commands you can execute from User Exec mode provide only user-level access; however, you should password protect it to prevent unauthorized use. The User Exec commands allow you to perform such functions as:

- Change terminal settings on a temporary basis.
- Perform **ping** and **trace** commands.
- Display system information.

```
host1>?
  clear       Clear system information
  default     Set a command to its default(s)
  dir         Display a list of local files
  disable     Reduce the command privilege level
  enable      Enable access to privileged commands
  erase       Erase configuration settings
  exit        Exit from the current command mode
  flash-disk  Perform flash disk operations
  help        Describe the interactive help system
  ip          Configure IP attributes on an interface
  ipv6        Configure IPv6 attributes
  l2tp        L2TP operations
  macro       Run a CLI macro
  mpls        Execute MPLS commands
  mtrace      Trace the path that packets will traverse from source to
              destination for a given group
  no          Negate a command or set its default(s)
  ping        Send echo request to remote host
  show        Display system information
  sleep       Make the Command Interface pause for a specified duration
  terminal    Configure the terminal line settings
  test        Test the outcome of a command
  traceroute  Trace the path that packets traverse to their destination
```

Privileged Exec mode provides privileged-level access and therefore should also be password protected to prevent unauthorized use. Privileged Exec commands allow you to perform such functions as:

- Display system information.
- Set operating parameters.
- Gain access to Global Configuration mode.

Password Protection

If the system administrator has configured the system to have a password, the CLI prompts you to enter that password before you receive access to Privileged Exec mode. The password is case sensitive and appears as asterisks on the screen.

To access Privileged Exec mode:

1. At the prompt, type **enable** and press Enter.

   ```
   host1>enable
   Password:
   ```

2. At the password prompt, type your password and press Enter.

   ```
   Password:*********
   host1#
   ```

NOTE: The > character in the command-line prompt changes to the # character.

```
host1#?
  baseline          Set a baseline for statistics
  clear             Clear a state
  clock             Set the system's clock
  configure         Enter Global Configuration mode
  copy              Copy files
  debug             Configure debugging functions
  default           Set a command to its default(s)
  delete            Delete a local file
  dir               Display a list of local files
  disable           Reduce the command privilege level
  disconnect        Disconnect remote CLI session
  enable            Enable access to privileged commands
  exit              Exit from the current command mode
  flash-disk        Perform flash disk operations
  halt              Halt the system in preparation for power down
  help              Describe the interactive help system
  ip                Configure IP attributes on an interface
  ipv6              Configure IPv6 attributes
  l2tp              L2TP operations
  log               Configure logging settings
  logout            Logout PPP Subscribers
  macro             Run a CLI macro
  more              Display contents of a file
  mpls              Execute MPLS commands
  mtrace            Trace the path that packets will traverse from source to
                    destination for a given group
```

```
no                Negate a command or set its default(s)
ping              Send echo request to remote host
pppoe             Set PPPoE information
profile-reassign  Perform profile reassignment
redundancy        Perform a redundancy action
reload            Halt and perform a cold restart
rename            Rename a local file
send              Send a message to specified lines
show              Display system information
sleep             Make the Command Interface pause for a specified duration
srp               Perform SRP operations
synchronize       Manually synchronize redundant system controller file system
telnet            Access a remote system via telnet
terminal          Configure the terminal line settings
test              Test the outcome of a command
traceroute        Trace the path that packets traverse to their destination
undebug           Disable debug logging functions
virtual-router    Specify a virtual router
write             Write the system's running configuration to a destination
```

In addition, you can execute a script file (.scr), which is simply a file containing a sequence of CLI commands, through the **configure** command.

Global Configuration Mode

Within Global Configuration mode, you can:

- Apply features globally to a router.
- Enable a feature or function.
- Disable a feature or function.
- Configure a feature or function.
- Access all Configuration modes.

To access Global Configuration mode, you begin in Privileged Exec mode. Type **configure terminal** and press Enter.

```
host1#configure terminal
Enter configuration commands, one per line. End with ^Z.
host1(config)#
```

The system is now in Global Configuration mode.

Executing a Script File

To execute a script file:

1. From Privileged Exec mode, type **configure** and the filename you want to execute, and press Enter.

```
host1#configure file
File name:/myFile.scr
Proceed with configure? [confirm]
```

NOTE: The filename must end with an .scr extension, and the file must contain a series of valid CLI commands. The file can be a local file on the router or a remote file on a host system.

2. Press **y** or Enter to confirm; pressing any other key aborts the procedure.

```
host1#
```

For more information, see the section *Managing Files* in *Chapter 5, Managing the System*.

AAA Profile Configuration Mode

From this mode, you can restrict or allow the use of domain names, translate an original domain name to a new domain name, or create domain name aliases.

From Global Configuration mode, type the **aaa profile** command and a *profileName*, and then press Enter.

```
host1(config)#aaa profile charlie
host1(config-aaa-profile)#?
  allow      Configure the authorization domain name
  default    Set a command to its default(s)
  deny       Configure the authorization domain name
  do         Run an exec mode command (alias command run)
  exit       Exit from the current command mode
  help       Describe the interactive help system
  log        Configure logging settings
  macro      Run a CLI macro
  no         Negate a command or set its default(s)
  run        Run an exec mode command (alias command do)
  sleep      Make the Command Interface pause for a specified duration
  translate  Configure the translation map for domain name
```

Address Family Configuration Mode

From this mode, you can configure address family parameters for BGP VPN services or RIP VPN services.

From Global Configuration mode, type the **router bgp** command to enter Router Configuration mode for BGP. Type either the **address-family ipv4** or **address-family vpnv4** command, and then press Enter.

```
host1(config)#router bgp 100
host1(config-router)#address-family ?
  ipv4   Configure IPv4 address family
  vpnv4  Configure VPN-IPv4 address family
```

From Global Configuration mode, type the **router rip** command to enter Router Configuration mode for RIP. Type the **address-family ipv4** command, and then press Enter.

```
host1(config)#router rip 100
host1(config-router)#address-family ?
  ipv4   Configure IPv4 address family
```

ATM VC Configuration Mode

In this mode, you can configure individual attributes for an ATM data PVC. These attributes include the service category, encapsulation method, Inverse Address Resolution Protocol (Inverse ARP), and F5 Operation, Administration, and Management (OAM) parameters.

From Global Configuration mode, type the **interface** command and specify the ATM subinterface identifier to enter Subinterface Configuration mode. From Subinterface Configuration mode, type the **pvc** command and specify the virtual circuit descriptor (VCD), virtual path identifier (VPI) and virtual circuit identifier (VCI) values (in the format *vpi*/*vci*), and then press Enter.

```
host1(config)#interface atm 3/2.1
host1(config-subif)#pvc 100 0/100
host1(config-subif-atm-vc)#?
  cbr             Configure the Constant Bit Rate (CBR) service class
  class-vc        Assign a Virtual Circuit class to the Permanent Virtual
                  Circuit
  default         Set a command to its default(s)
  do              Run an exec mode command (alias command run)
  encapsulation   Configure the ATM encapsulation
  exit            Exit from the current command mode
  help            Describe the interactive help system
  inarp           Configure the Inverse Address Resolution Protocol (InARP)
                  protocol
  log             Configure logging settings
  macro           Run a CLI macro
  no              Negate a command or set its default(s)
  oam             Configure Operations, Administration, and Management (OAM)
  oam-pvc         Configure Operations, Administration, and Management (OAM) for
                  Permanent Virtual Circuit (PVC)
  run             Run an exec mode command (alias command do)
  sleep           Make the Command Interface pause for a specified duration
  ubr             Configure the Unspecified Bit Rate (UBR) service class
  vbr-nrt         Configure the Variable Bit Rate Non-Real Time (VBR-nrt)
                  service class
  vbr-rt          Configure the Variable Bit Rate Real Time (VBR-rt) service
                  class
```

ATM VC Class Configuration Mode

In this mode, you can configure a class of attributes for an ATM data PVC. The VC class can include attributes for the service category, encapsulation method, F5 OAM options, and Inverse ARP. You then apply the set of attributes as a group by assigning the VC class to an individual PVC, to all PVCs created on a specified ATM major interface, to all PVCs created on a specified ATM 1483 subinterface, or to a base profile from which bulk-configured VC ranges are dynamically created.

From Global Configuration mode, type the **vc-class atm** command followed by an alphanumeric VC class name of up to 32 characters, and press Enter.

```
host1(config)#vc-class atm premium-subscriber-class
host1(config-vc-class)#?
  cbr             Configure the Constant Bit Rate (CBR) service class
  default         Set a command to its default(s)
  do              Run an exec mode command (alias command run)
  encapsulation   Configure the ATM encapsulation
  exit            Exit from the current command mode
  help            Describe the interactive help system
```

```
  inarp          Configure the Inverse Address Resolution Protocol (InARP)
                 protocol
  log            Configure logging settings
  macro          Run a CLI macro
  no             Negate a command or set its default(s)
  oam            Configure Operations, Administration, and Management (OAM)
  oam-pvc        Configure Operations, Administration, and Management (OAM) for
                 Permanent Virtual Circuit (PVC)
  run            Run an exec mode command (alias command do)
  sleep          Make the Command Interface pause for a specified duration
  ubr            Configure the Unspecified Bit Rate (UBR) service class
  vbr-nrt        Configure the Variable Bit Rate Non-Real Time (VBR-nrt)
                 service class
  vbr-rt         Configure the Variable Bit Rate Real Time (VBR-rt) service
                 class
```

Classifier Group Configuration Mode

In this mode, you can configure the set of rules for a classification group in a policy list that you can attach to an interface.

From Policy List Configuration mode, type the **classifier-group** command and its attributes, and then press Enter.

```
host1(config-policy-list)#classifier-group ipCLACL10 precedence 75
host1(config-policy-list-classifier-group)#?
  color               Create a color policy
  default             Set a command to its default(s)
  do                  Run an exec mode command (alias command run)
  exit                Exit from the current command mode
  filter              Create a filter policy
  forward             Create a forward policy
  help                Describe the interactive help system
  log                 Configure logging settings
  macro               Run a CLI macro
  mark                Create a set TOS byte policy
  next-hop            Create a next-hop policy
  next-interface      Create a next-interface policy
  no                  Negate a command or set its default(s)
  rate-limit-profile  Create a rate-limit policy
  run                 Run an exec mode command (alias command do)
  sleep               Make the Command Interface pause for a specified duration
  suspend             Suspend a policy rule
  traffic-class       Create a traffic class policy
  user-packet-class   Create a user packet class policy
```

Color Mark Profile Configuration Mode

In this mode, you can configure translation for a color to a type-dependent mark for TOS or EXP for an IP, IPv6 or MPLS interface.

From Rate Limit Profile Configuration mode, type the **color-mark-profile** command and specify a *profileName*, and then press Enter.

```
host1(config-rate-limit-profile)#mpls color-mark-profile myprofile
host1(config-color-mark-profile)#?
  default      Set a command to its default(s)
  do           Run an exec mode command (alias command run)
  exit         Exit from the current command mode
```

```
green-mark   Apply TOS mark to IP packets classified Green by the rate limit
             hierarchy
help         Describe the interactive help system
log          Configure logging settings
macro        Run a CLI macro
mask-value   Mask for all TOS values applied by the color-mark profile
no           Negate a command or set its default(s)
red-mark     Apply TOS mark to IP packets classified Red by the rate limit
             hierarchy
run          Run an exec mode command (alias command do)
sleep        Make the Command Interface pause for a specified duration
yellow-mark  Apply TOS mark to IP packets classified Yellow by the rate limit
             hierarchy
```

Control Plane Configuration Mode

In this mode, you can configure policing for a specific protocol.

From Global Configuration mode, type the **control-plane** command and press Enter.

```
host1(config)#control-plane
host1(config-control-plane)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  policer  Configure policing
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

Controller Configuration Mode

You can configure physical interfaces such as a T3 in Controller Configuration mode.

From Global Configuration mode, type the appropriate **controller** command and its attributes, and then press Enter.

```
host1(config)#controller t3 9/1
host1(config-controll)#

host1(config)#controller ?
  e1     Configure a channelized E1 controller
  e3     Configure a E3 controller
  sonet  Configure a Sonet controller
  t1     Configure a channelized T1 controller
  t3     Configure a T3 controller
```

DHCP Local Pool Configuration Mode

In this mode, you can configure DHCP local pools. For example, you can specify a DNS or NetBIOS server.

From Global Configuration mode, type the command **ip dhcp-local pool** and a *poolName*, and then press Enter.

```
host1(config)#ip dhcp-local pool charlie
host1(config-dhcp-local)#?
  default                  Set a command to its default(s)
  default-router           The default-router to use for this pool
  dns-server               The dns-server to use for this pool
  do                       Run an exec mode command (alias command run)
  domain-name              The domain name for the pool
  exit                     Exit from the current command mode
  grace-period             The grace period to be applied to leases
  help                     Describe the interactive help system
  lease                    The lease time for addresses from this pool
  link                     Link to another DHCP Pool
  log                      Configure logging settings
  macro                    Run a CLI macro
  netbios-name-server      The netbios-name-server to use for this pool
  netbios-node-type        The netbios-node-type to use for this pool
  network                  The network specified for this pool
  no                       Negate a command or set its default(s)
  reserve                  Reserve an ip address for a specific Mac Address
  run                      Run an exec mode command (alias command do)
  server-address           The DHCP Server address to send to clients
  sleep                    Make the Command Interface pause for a specified
                           duration
  snmpTrap                 Enable snmp pool utilization traps
  use-release-grace-period Apply the grace period to released leases
  warning                  Configure utilization warnings
```

Domain Map Configuration Mode

In this mode, you can map a user domain name to a virtual router and loopback interface.

From Global Configuration mode, type the **aaa domain-map** command and the domain name value as found in the client's login name. Then press Enter.

```
host1(config)#aaa domain-map charlie76
host1(config-domain-map)#?
  address-pool-name  Configure the address-pool-name for the domain name
  atm                Configure ATM parameters
  default            Set a command to its default(s)
  do                  Run an exec mode command (alias command run)
  exit               Exit from the current command mode
  help               Describe the interactive help system
  ip-hint            Configure the IP hint feature for the domain
  local-interface    Configure the local interface value for remote clients
  log                Configure logging settings
  loopback           Configure the loopback interface to use when RX has an
                     unnumbered interface to the PPP client
  macro              Run a CLI macro
  no                 Negate a command or set its default(s)
  override-user      Configure the username and password values to use instead
                     of the values from the remote client
```

```
padn              Configure pppoe active discovery network parameters for
                  the domain name
router-name       Configure the virtual-router for the domain name
run               Run an exec mode command (alias command do)
sleep             Make the Command Interface pause for a specified duration
strip-domain      Configure the domain name stripping feature for the domain
tunnel            Configure tunnel tag
virtual-router    Configure the virtual-router for the domain name
```

Domain Map Tunnel Configuration Mode

In this mode, you can configure tunnel parameters such as the tunnel's endpoint.

From Domain-Map Configuration mode, type **tunnel** and a *tunnelNumber*, and press Enter.

```
host1(config-domain-map)#tunnel 17
host1(config-domain-map-tunnel)#?
  address         Configure tunnel endpoint address
  client-name Configure the client hostname of the tunnel
  default         Set a command to its default(s)
  exit            Exit from the current command mode
  do              Run an exec mode command (alias command run)
  help            Describe the interactive help system
  hostname        Configure the client hostname of the tunnel
  identification  Configure tunnel identification
  log             Configure logging settings
  macro           Run a CLI macro
  max-sessions    Configure maximum sessions for this tunnel
  medium          Configure tunnel medium
  no              Negate a command or set its default(s)
  password        Configure tunnel password
  preference      Configure tunnel preference
  run             Run an exec mode command (alias command do)
  server-name     Configure the remote hostname for the tunnel
  sleep           Make the Command Interface pause for a specified duration
  source-address  Configure tunnel source address
  type            Configure tunnel type
```

DoS Protection Group Configuration Mode

In this mode, you can configure parameters for Denial of Service (DoS) protection groups.

From Global Configuration mode, type the **dos-protection-group** command and press Enter.

```
host1(config)#dos-protection-group
host1(config-dos-protection)#?
  default   Set a command to its default(s)
  do        Run an exec mode command (alias command run)
  exit      Exit from the current command mode
  help      Describe the interactive help system
  log       Configure logging settings
  macro     Run a CLI macro
  no        Negate a command or set its default(s)
  priority  Specify the priority
```

```
  protocol  Specify the protocol
  run       Run an exec mode command (alias command do)
  sleep     Make the Command Interface pause for a specified duration
  use       Configure usagehost1(config-dos-protection-group)#?
```

Drop Profile Configuration Mode

In this mode, you can configure drop profiles for QoS. Drop profiles control RED dropping behavior.

From Global Configuration mode, type the **drop-profile** command, and press Enter.

```
host1(config)#drop profile
host1(config-drop-profile)#?
  average-length-exponent  Select TAQL coefficient
  committed-threshold      Specify committed queue thresholds and maximum drop
                           probability
  conformed-threshold      Specify conformed queue thresholds and maximum drop
                           probability
  default                  Set a command to its default(s)
  do                       Run an exec mode command (alias command run)
  exceeded-threshold       Specify exceeded queue thresholds and maximum drop
                           probability
  exit                     Exit from the current command mode
  help                     Describe the interactive help system
  log                      Configure logging settings
  macro                    Run a CLI macro
  no                       Negate a command or set its default(s)
  run                      Run an exec mode command (alias command do)
  sleep                    Make the Command Interface pause for a specified duration
```

Explicit Path Configuration Mode

From this mode, you can name and configure an explicit path within MPLS.

From Global Configuration mode, type **mpls explicit-path name** and the *explicitPathName*, and press Enter.

```
host1(config)#mpls explicit-path name xyz
host1(config-expl-path)#?
  append-after  Add an entry after a specified index
  default       Set a command to its default(s)
  do            Run an exec mode command (alias command run)
  exit          Exit from the current command mode
  help          Describe the interactive help system
  index         Specify the index of the entry to be added or edited
  list          List part or all of the entries in current explicit path
  log           Configure logging settings
  macro         Run a CLI macro
  next-address  Configure an IP address at the last hop of the explicit path
  no            Negate a command or set its default(s)
  run           Run an exec mode command (alias command do)
  sleep         Make the Command Interface pause for a specified duration
```

Flow Cache Configuration Mode

In this mode, you can configure parameters for the aggregation cache.

From Global Configuration mode, type the **ip flow-aggregation cache** command and press Enter.

```
host1(config)#ip flow-aggregation cache
host1(config-flow-cache)#?
  cache    Configure Flow Stats cache parameters
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  enabled  Start flow cache operation
  exit     Exit from the current command mode
  export   Configure Flow-Cache export parameters
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

Interface Configuration Mode

From Interface Configuration mode, you can enable many system features for each interface you create. Interface Configuration commands allow you to:

- Create an interface.
- Modify the operation of an interface.
- Access Subinterface Configuration mode.

From Global Configuration mode, type **interface** and identify the interface you want to configure and press Enter.

```
host1(config)#interface atm 0/1
host1(config-if)#
```

The CLI is now in Interface Configuration mode.

```
host1(config)#interface ?
  atm              ATM interface
  fastEthernet     IEEE 802.3 fastEthernet interface
  gigabitEthernet  IEEE 802.3 gigabitEthernet interface
  hssi             High Speed Serial interface
  ip               Ip shared interface
  ipv6             Ipv6 shared interface
  lag              Link Aggregation interface
  loopback         Loopback interface
  mlframe-relay    Multilink frame-relay interface
  mlppp            Multilink PPP interface
  null             Null interface
  pos              Packet over SONET interface
  serial           Serial interface
  tunnel           Tunnel interface
```

Some Interface Configuration commands can affect general interface parameters, such as bandwidth and clock rate. For interface-specific commands, such as commands for ATM interfaces, see the appropriate chapter in this documentation set.

NOTE: Although it appears in the list of configurable interfaces, you cannot configure any values on a null interface. For information about using the null interface, see *JUNOSe IP Services Configuration Guide, Chapter 1, Configuring Routing Policy*.

IP NAT Pool Configuration Mode

In this mode, you can specify the information that the system uses in creating IP Network Address Translation (NAT) pools. From Global Configuration mode, type **ip nat pool multiplerange prefix-length** and press Enter.

```
host1(config)#ip nat pool multiplerange prefix-length 30
host1(config-ipnat-pool)#?
  address  Configure address ranges
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

IP PIM Data MDT Configuration Mode

In this mode, you can specify parameters for data MDTs.From Global Configuration mode, type **ip pim data-mdt**, and press Enter:

```
host1:pe1:pe13(config)#ip pim data-mdt
host1:western:eastern(config-ip-pim-data-mdt)#?
  default           Set a command to its default(s)
  do                Run an exec mode command (alias command run)
  exit              Exit from the current command mode
  help              Describe the interactive help system
  log               Configure logging settings
  macro             Run a CLI macro
  mdt-data-delay    Configure MDT_DATA_DELAY timeout
  mdt-data-holdown  Configure MDT_DATA_HOLDOWN timeout
  mdt-data-timeout  Configure MDT_DATA_TIMEOUT
  mdt-interval      Configure MDT_INTERVAL timer
  no                Negate a command or set its default(s)
  route-map         Configure route-map
  run               Run an exec mode command (alias command do)
  sleep             Make the Command Interface pause for a specified duration
  tunnel            Configure tunnel parameters
```

IP Service Profile Configuration Mode

In this mode, you can specify the information that the system uses in creating IP service profiles.

From Global Configuration mode, type **ip service-profile** and the service profile name, and press Enter.

```
host1(config)#ip service-profile radius
host1(config-service-profile)#?
  default      Set a command to its default(s)
  do           Run an exec mode command (alias command run)
  domain       Configure a username domain
  exit         Exit from the current command mode
  help         Describe the interactive help system
  include      Configure an attribute to be included in a username
  log          Configure logging settings
  macro        Run a CLI macro
  no           Negate a command or set its default(s)
  password     Configure a user password
  run          Run an exec mode command (alias command do)
  sleep        Make the Command Interface pause for a specified duration
  user-name    Configure a user name
  user-prefix  Configure a username prefix
```

IPSec CA Identity Configuration Mode

In this mode, you can specify the information that the system uses in online certificate requests and during negotiations with its peers.

From Global Configuration mode, type **ipsec ca identity**, and press Enter.

```
host1(config)#ipsec ca identity
host1(config-ca-identity)#?
  crl                Certificate Revocation List checking
  default            Set a command to its default(s)
  do                 Run an exec mode command (alias command run)
  enrollment         Configure enrollment parameters
  exit               Exit from the current command mode
  help               Describe the interactive help system
  issuer-identifier  issuer identifier
  log                Configure logging settings
  macro              Run a CLI macro
  no                 Negate a command or set its default(s)
  root               Specify root proxy
  run                Run an exec mode command (alias command do)
  sleep              Make the Command Interface pause for a specified
```

IPSec Identity Configuration Mode

In this mode, you can specify the information that the system uses in offline certificate requests and during negotiations with its peers.

From Global Configuration mode, type **ipsec identity**, and press Enter.

```
host1(config)#ipsec identity
host1(config-ipsec-identity)#?
  common-name   Common Name
  country       Country name
  default       Set a command to its default(s)
  do            Run an exec mode command (alias command run)
  domain-name   Domain name
  exit          Exit from the current command mode
  help          Describe the interactive help system
  log           Configure logging settings
  macro         Run a CLI macro
  no            Negate a command or set its default(s)
  organization  Organization name
  sleep         Make the Command Interface pause for a specified duration
```

IPSec IKE Policy Configuration Mode

In this mode, you can create an IKE policy, which is used during IKE phase 1 negotiation.

From the Global Configuration mode, type **ipsec ike-policy-rule** and the *policyNumber*, and press Enter.

```
host1(config)#ipsec ike-policy-rule 10
host1(config-ike-policy)#?
  aggressive-mode  Allows aggressive mode negotiation for the tunnel
  authentication   Configure the authentication method
  default          Set a command to its default(s)
  do               Run an exec mode command (alias command run)
  encryption       Configure the encryption algorithm within an IKE policy
  exit             Exit from the current command mode
  group            Configure the Diffie-Hellman group identifier
  hash             Configure the hash algorithm within an IKE policy
  help             Describe the interactive help system
  lifetime         Configure the time an SA will live before expiration
  log              Configure logging settings
  macro            Run a CLI macro
  no               Negate a command or set its default(s)
  run              Run an exec mode command (alias command do)
  sleep            Make the Command Interface pause for a specified duration
```

IPSec Manual Key Configuration Mode

In this mode, you can enter the manual key that a peer uses for authentication during the tunnel establishment phase.

From the Global Configuration mode, type **ipsec key manual pre-share** and the *peerIPaddress*, and press Enter.

```
host1(config)#ipsec key manual pre-share 10.10.1.1
host1(config-manual-key)#?
  default     Set a command to its default(s)
  do          Run an exec mode command (alias command run)
  exit        Exit from the current command mode
  help        Describe the interactive help system
  key         Manually specify a key
  log         Configure logging settings
  macro       Run a CLI macro
  masked-key  Enter a masked key (not for manual entry, show config generates)
  no          Negate a command or set its default(s)
  run         Run an exec mode command (alias command do)
  sleep       Make the Command Interface pause for a specified duration
```

IPSec Peer Public Key Configuration Mode

In this mode, you can configure the ISAKMP/IKE public key that a remote peer uses for RSA authentication during the tunnel establishment phase without the need for a digital certificate.

From Global Configuration mode, type **ipsec key pubkey-chain rsa** and either the IP address or fully qualified domain name of the remote peer, and press Enter.

```
host1(config)#ipsec key pubkey-chain rsa address 192.168.50.5
host1(config-peer-public-key)#?
  default     Set a command to its default(s)
  do          Run an exec mode command (alias command run)
  exit        Exit from the current command mode
  help        Describe the interactive help system
  key-string  Enter key string
  log         Configure logging settings
  macro       Run a CLI macro
  no          Negate a command or set its default(s)
  run         Run an exec mode command (alias command do)
  sleep       Make the Command Interface pause for a specified duration
```

IPSec Transport Profile Configuration Mode

In this mode, you can configure an IP Security (IPSec) transport profile, which is used for Layer 2 Tunneling Protocol (L2TP) over IPSec connections.

From the Global Configuration mode, type **ipsec transport profile**, the *profileName*, **virtual-router** *vrName*, **ip address** *ipAddress*, and press Enter.

```
host1(config)#ipsec transport profile secureL2tp virtual-router default ip address 0.0.0.0
host1(config-ipsec-transport-profile)#?
  application    Configure the application type that is protected by the l2tp
  default        Set a command to its default(s)
  do             Run an exec mode command (alias command run)
  exit           Exit from the current command mode
  help           Describe the interactive help system
  lifetime       Configure the renegotiation time
  local          Configure local endpoint of the transport connection
  log            Configure logging settings
  macro          Run a CLI macro
  no             Negate a command or set its default(s)
  pfs            Configure perfect forward secrecy
  run            Run an exec mode command (alias command do)
  sleep          Make the Command Interface pause for a specified duration
  transform-set  Configure the transform set used by ipsec transport profile
```

IPSec Tunnel Profile Configuration Mode

In this mode, you can configure a profile of an IPSec tunnel.

From Global Configuration mode, type **ipsec tunnel profile** and the *profileName*, and press Enter.

```
host1(config)#ipsec tunnel profile profile1
host1(config-ipsec-tunnel-profile)#?
  default                  Set a command to its default(s)
  do                       Run an exec mode command (alias command run)
  domain-suffix            Configure a domain suffix to be appended to users on
                           this profile
  exit                     Exit from the current command mode
  extended-authentication  Configure extended authentication parameters
  help                     Describe the interactive help system
  ike                      Configure IKE characteristics
  ip                       Configure local IP characteristics
  lifetime                 Configure the phase 2 life parameters
  local                    Configure local characteristics
  log                      Configure logging settings
  macro                    Run a CLI macro
  max-interfaces           Configure the maximum allowed dynamic interface
                           instantiations
  no                       Negate a command or set its default(s)
  peer                     Configure peer characteristics
  pfs                      Configure the phase 2 perfect forward secrecy
  run                      Run an exec mode command (alias command do)
  sleep                    Make the Command Interface pause for a specified
                           duration
  transform                Configure the phase 2 transforms allowed on this
                           IPSEC tunnel profile
  tunnel                   Configure tunnel parameters
```

IP Tunnel Destination Profile Mode

In this mode, you can specify parameters for GRE or DVMRP dynamic tunnels.

From Global Configuration mode, type **gre destination profile** or **dvmrp destination profile** and the destination profile name, and press Enter.

```
host1(config)#gre destination profile global
host1(config-dest-profile)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  enable   Enable a tunnel parameter
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  profile  Assign a profile
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
  tunnel   Configure a tunnel parameter

host1(config)#dvmrp destination profile global
host1(config-dest-profile)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  enable   Enable a tunnel parameter
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  profile  Assign a profile
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
  tunnel   Configure a tunnel parameter
```

L2 Transport Load-Balancing-Circuit Configuration Mode

In this mode, you can specify a member subinterface for a Martini layer 2 circuit that is associated with a load-balancing group.

From Global Configuration mode, type **mpls l2transport load-balancing-group**, specify a group number and a Martini circuit, and press Enter.

```
host1(config)#mpls l2transport load-balancing-group 100 mpls-relay 10.1.1.1 30
host1(config-l2transport-load-balancing-circuit)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  member   Configure members of a l2transport load-balancing circuit
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

L2TP Destination Profile Configuration Mode

In this mode, you can create the destination profile that defines the location of an L2TP Access Concentrator (LAC) and define the attributes used when an L2TP Network Server (LNS) communicates with an LAC. The destination is necessary to enable an LAC to connect to the LNS.

From Global Configuration mode, type **l2tp destination profile,** the *profileName*, an *ipAddress*, and press Enter.

```
host1(config)#l2tp destination profile augusta ip address 123.45.76.16
host1(config-l2tp-dest-profile)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  remote   Configure L2TP remote parameters
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

L2TP Destination Profile Host Configuration Mode

In this mode, you can set and modify L2TP host profile attributes, such as the proxy Link Control Protocol (LCP), the local hostname, the local IP address, or the interface profile.

From Global Configuration mode, enter L2TP Destination Profile mode (see above), and type **remote host** and a *hostName,* and press Enter.

```
host1(config-l2tp-dest-profile)#remote host george
host1(config-l2tp-dest-profile-host)#?
  default  Set a command to its default(s)
  disable  Disable L2TP parameter for remote host
  do       Run an exec mode command (alias command run)
  enable   Enable L2TP parameter for remote host
  exit     Exit from the current command mode
  help     Describe the interactive help system
  local    Configure L2TP local parameters for remote host
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  profile  Assign a profile for remote host
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
  tunnel   Configure L2TP tunnel parameters for remote host
```

L2TP Tunnel Switch Profile Configuration Mode

In this mode, you can create an L2TP tunnel switch profile, which configures the L2TP tunnel switching behavior for the interfaces to which this profile is assigned. Issue the **avp** command from this mode to define the L2TP tunnel switching behavior for a specified L2TP attribute-value pair (AVP) type.

From Global Configuration mode, type the **l2tp switch-profile** command followed by an alphanumeric profile name of up to 64 characters, and press Enter.

```
host1(config)#l2tp switch-profile concord
host1(config-l2tp-tunnel-switch-profile)#?
  avp      Configure AVP behavior
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

Layer 2 Control Configuration Mode

In this mode, you can define session timeout values and access the L2C Neighbor Configuration mode to specify the L2C neighbor.

From Global Configuration mode, type **l2c** and press Enter.

```
host1(config)#l2c
host1(config-l2c)#?
  default          Set a command to its default(s)
  do               Run an exec mode command (alias command run)
  exit             Exit from the current command mode
  help             Describe the interactive help system
  log              Configure logging settings
  macro            Run a CLI macro
  neighbor         Configure l2c neighbor parameters
  no               Negate a command or set its default(s)
  run              Run an exec mode command (alias command do)
  session-timeout  Configure the l2c time-out attribute
  sleep            Make the Command Interface pause for a specified duration
```

Layer 2 Control Neighbor Configuration Mode

In this mode, you can specify a neighbor ID and the maximum number of branches that the neighbor can have.

From Global Configuration mode, type **neighbor** and press Enter.

```
host1(config-l2c)#neighbor
host1(config-l2c-neighbor)#?
  default       Set a command to its default(s)
  do            Run an exec mode command (alias command run)
  exit          Exit from the current command mode
  help          Describe the interactive help system
  id            Configure neighbor-id associated with neighbor
  log           Configure logging settings
  macro         Run a CLI macro
  max-branches  Configure max number of branches for neighbor
  no            Negate a command or set its default(s)
  run           Run an exec mode command (alias command do)
  sleep         Make the Command Interface pause for a specified duration
```

LDP Configuration Mode

In this mode, you can create and configure MPLS Label Distribution Protocol (LDP) profile parameters.

From Global Configuation mode, type **mpls ldp interface profile** and the *profileName*, and press Enter.

```
host1(config)#mpls ldp interface profile shell
host1(config-ldp)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  hello    Configure hello parameters
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

Line Configuration Mode

In this mode, you can modify the operation of a virtual terminal (vty) line.

From Global Configuration mode, type the **line vty** command and either the *lineNumber* or the *rangeOfLineNumbers* you want to configure, and press Enter.

NOTE: The factory default is 5 vty lines. However, you can increase the number of vty lines available by typing the start number and end number of the vty line range. Once you execute the **line vty** command, you will have access to line numbers up to the ending line number.

```
host1(config)#line vty 0 29
host1(config-line)#?
  access-class         Restrict or permit telnet access based on an access list
  data-character-bits  Set the number of bits per character used by the display
```

```
  default              Set a command to its default(s)
  do                   Run an exec mode command (alias command run)
  exec-banner          Enable the exec banner
  exec-timeout         Set the inactivity timeout
  exit                 Exit from the current command mode
  help                 Describe the interactive help system
  log                  Configure logging settings
  login                Require the use of passwords for vty logins
  macro                Run a CLI macro
  motd-banner          Enable the message of the day banner
  no                   Negate a command or set its default(s)
  password             Configure the password for line access
  run                  Run an exec mode command (alias command do)
  sleep                Make the Command Interface pause for a specified duration
  timeout              Specify the login timeout value for the selected line(s)
```

NOTE: The **privilege** command is available in Line Configuration mode when the user is logged in at privilege level 15. For more information, see *Privileged-Level Access* on page 48 and *CLI Command Privileges* on page 50.

Local IPSec Transport Profile Configuration

In this mode, you can configure preshared IKE keys for IPSec transport profiles.

From the IPSec Transport Profile Configuration mode, type **local ip address** and the *ipAddress*, and press Enter.

```
host1(config-ipsec-transport-profile)#local ip address 10.10.1.1
host1(config-ipsec-transport-profile-local)#?
  default           Set a command to its default(s)
  do                Run an exec mode command (alias command run)
  exit              Exit from the current command mode
  help              Describe the interactive help system
  log               Configure logging settings
  macro             Run a CLI macro
  no                Negate a command or set its default(s)
  pre-share         Specify pre-shared group key based on local ip address
  pre-share-masked  A pre-encrypted key, generated by show config rather than
                    interactive
  run               Run an exec mode command (alias command do)
  sleep             Make the Command Interface pause for a specified duration
```

Local User Configuration Mode

In this mode, you can configure parameters for user entries in local user databases.

From the Global Configuration mode, type either **aaa local username** and the *userName* and *databaseName* or **aaa local database** and the *databaseName*. Then press Enter.

```
host1(config)#aaa local username curt38 database westLocal12
host1(config-local-user)#?
  default                     Set a command to its default(s)
  do                          Run an exec mode command (alias command run)
  exit                        Exit from the current command mode
  help                        Describe the interactive help system
  ip-address                  Specify an IP address for the user
  ip-address-pool             Specify an IP address pool for the user
```

```
log                          Configure logging settings
macro                        Run a CLI macro
no                           Negate a command or set its default(s)
operational-virtual-router   Specify an operational virtual router for the
                             user
password                     Configure the password
run                          Run an exec mode command (alias command do)
secret                       Configure the secret
sleep                        Make the Command Interface pause for a specified
                             duration
support                      Enter Support mode
```

Map Class Configuration Mode

In this mode, you can specify Frame Relay End-to-End fragmentation and reassembly for a map class. Optionally, you can specify the maximum payload size of a fragment or specify fragmentation only or reassembly only.

From Global Configuration mode, type the **map-class frame-relay** command and the *mapClassName* you want to configure, and press Enter.

```
host1(config)#map-class frame-relay testmapclass
host1(config-map-class)#?
  default      Set a command to its default(s)
  do           Run an exec mode command (alias command run)
  exit         Exit from the current command mode
  frame-relay  Configure frame relay parameters
  help         Describe the interactive help system
  log          Configure logging settings
  macro        Run a CLI macro
  no           Negate a command or set its default(s)
  run          Run an exec mode command (alias command do)
  sleep        Make the Command Interface pause for a specified duration
```

Map List Configuration Mode

In this mode, you can configure map list parameters. In Map List Configuration mode, commands such as **map-list** and **ip atm-vc** are used to configure ATM NBMA interfaces.

From Global Configuration mode, type **map-list** and a *mapListName,* and press Enter.

```
host1(config)#map-list mjt3330
host1(config-map-list)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  ip       Add IP address to the map
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

Parent Group Configuration Mode

In this mode, you can configure a parent group in a hierarchy.

From Global Configuration mode, type the **parent-group** command and specify a *parentGroupName*, and press Enter.

```
host1(config)#parent-group group1
host1(config-parent-group)#?
  default             Set a command to its default(s)
  do                  Run an exec mode command (alias command run)
  exit                Exit from the current command mode
  help                Describe the interactive help system
  log                 Configure logging settings
  macro               Run a CLI macro
  next-parent         Specify the next parent group to call in hierarchy
  no                  Negate a command or set its default(s)
  rate-limit-profile  Specify a hierarchical rate limit profile
  run                 Run an exec mode command (alias command do)
  sleep               Make the Command Interface pause for a specified
```

Policy List Configuration Mode

In this mode, you can configure a policy list—that is, a set of rules—that you can attach to an interface. You can modify a policy list and update it wherever the policy list is used in the configuration.

To create a policy list, from Global Configuration mode type **policy-list** command preceded by the type of policy and press Enter. For example,

host1(config)#**l2tp policy-list routeL2tp100**

NOTE: If you do not include the type of policy, the system creates an IP policy list.

```
host1(config)#ip policy-list routeForABBCCorp
host1(config-policy-list)#?
  classifier-group       Specify the classifier list
  color                  Create a color policy
  default                Set a command to its default(s)
  do                     Run an exec mode command
  exit                   Exit from the current command mode
  filter                 Create a filter policy
  forward                Create a forward policy
  help                   Describe the interactive help system
  log                    Configure logging settings
  macro                  Run a CLI macro
  mark                   Create a set TOS byte policy
  next-hop               Create a next-hop policy
  next-interface         Create a next-interface policy
  no                     Negate a command or set its default(s)
  rate-limit-profile     Create a rate-limit policy
  run                    Run an exec mode command (alias command do)
  sleep                  Make the Command Interface pause for a specified
                         duration
  suspend                Suspend a policy rule
  traffic-class          Create a traffic class policy
  traffic-shape-profile  Create a traffic-shape policy
  user-packet-class      Create a user packet class policy
```

Policy List Parent Group Configuration Mode

In this mode, you can configure a parent group in a hierarchy.

From Policy List Configuration Mode, type the **parent-group** command and specify a *parentGroupName*, and press Enter.

```
host1(config)#policy-list grouppol1
host1(config-policy-list)#parent-group group1
host1(config-policy-list-parent-group)#?
  default             Set a command to its default(s)
  do                  Run an exec mode command (alias command run)
  exit                Exit from the current command mode
  help                Describe the interactive help system
  log                 Configure logging settings
  macro               Run a CLI macro
  no                  Negate a command or set its default(s)
  rate-limit-profile  Specify the hierarchical rate limit profile
  run                 Run an exec mode command (alias command do)
  sleep               Make the Command Interface pause for a specified
```

Policy Parameter Configuration Mode

In this mode, you can configure a policy parameter.

From Global Configuration mode, type the **policy-parameter** command and specify a *policyParameterType*, the **hierarchical** keyword, and press Enter.

```
host1(config)#policy-parameter param1 hierarchical
host1(config-policy-parameter)#?
  aggregation-node  Configure the aggregation node value
  default           Set a command to its default(s)
  do                Run an exec mode command (alias command run)
  exit              Exit from the current command mode
  help              Describe the interactive help system
  log               Configure logging settings
  macro             Run a CLI macro
  no                Negate a command or set its default(s)
  run               Run an exec mode command (alias command do)
  sleep             Make the Command Interface pause for a specified time
```

PPPoE Service Name Table Configuration Mode

In this mode, you can configure entries for a PPPoE service name table. PPPoE clients use these entries to request that an access concentrator (AC), such as an E-series router, support certain services. Issue the **service** command from this mode to configure a specific service name entry, or to specify that the AC should ignore (drop), rather than respond to (terminate, the default action), a PPPoE Active Discovery Initiation (PADI) request from a client containing the empty service name tag.

From Global Configuration mode, type the **pppoe-service-name-table** command followed by an alphanumeric table name of up to 32 characters, and press Enter.

```
host1(config)#pppoe-service-name-table serviceTable1
host1(config-pppoe-service-name-table)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
```

```
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  service  Configure service-name table entries
  sleep    Make the Command Interface pause for a specified duration
```

Profile Configuration Mode

In this mode, you can configure a profile to subsequently configure dynamic IP interfaces.

From Global Configuration mode, type the **profile** command followed by a profile name of up to 80 characters, and press Enter.

```
host1(config)#profile germany78
host1(config-profile)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  ip       Configure IP characteristics
  l2tp     Configure L2TP characteristics
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  ppp      Configure PPP parameters
  pppoe    Pppoe information
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

QoS Parameter Definition Configuration Mode

In this mode, you can configure QoS parameter definitions.

From Global Configuration mode, type the **qos-parameter-define** command followed by a *QosParameterDefinitionName*, and press Enter.

```
host1(config)#qos-parameter-define vpSharedShaper1
host1(config-qos-parameter-define)#?
  controlled-interface-type  Configure the valid interface types controlled by
                             this parameter
  default                    Set a command to its default(s)
  do                         Run an exec mode command (alias command run)
  exit                       Exit from the current command mode
  help                       Describe the interactive help system
  instance-interface-type    Configure the interface types upon which
                             parameters can be instantiated
  log                        Configure logging settings
  macro                      Run a CLI macro
  no                         Negate a command or set its default(s)
  range                      Set the valid range of a QoS parameter
  run                        Run an exec mode command (alias command do)
  sleep                      Make the Command Interface pause for a specified
                             duration
  subscriber-interface-type  Configure interface types representing subscriber
                             interfaces
```

QoS Profile Configuration Mode

In this mode, you can specify queue profiles and scheduler profiles in combination with interface types.

From Global Configuration mode, type the **qos-profile** command followed by a *QosProfileName*, and press Enter.

```
host1(config)#qos-profile testabc
host1(config-qos-profile)#?
atm          ATM interface
  atm-vc       ATM-VC interface
  bridge       Bridge interface
  default      Set a command to its default(s)
  do           Run an exec mode command (alias command run)
  ethernet     Ethernet interface
  exit         Exit from the current command mode
  fr-vc        Frame Relay subinterface
  help         Describe the interactive help system
  ip           IP interface
  ip-tunnel    IP FROM-tunnel interface
  l2tp-tunnel  L2tp FROM-tunnel interface
  log          Configure logging settings
  lsp          Lsp (MPLS) interface
  macro        Run a CLI macro
  no           Negate a command or set its default(s)
  run          Run an exec mode command (alias command do)
  serial       Serial interface
  server-port  Server Port interface
  sleep        Make the Command Interface pause for a specified duration
  svlan        Stacked VLAN subinterface
  vlan         VLAN subinterface
```

QoS Shared Shaper Control Configuration

In this mode, you can configure variables within the simple shared shaper algorithm to control the minimum dynamic rate for all simple shared shapers on the router.

From Global Configuration mode, type the **qos-shared-shaper-control** command and press Enter.

```
host1(config)#qos-shared-shaper-control
host1(config-qos-shared-shaper-control)#?
  convergence-factor            Configure how quickly the simple shared shaper
                                converges to a calculated rate
  default                       Set a command to its default(s)
  do                            Run an exec mode command (alias command run)
  exit                          Exit from the current command mode
  help                          Describe the interactive help system
  log                           Configure logging settings
  macro                         Run a CLI macro
  maximum-voql                  Configure the simple shared shaper's maximum
                                virtual output queue length
```

```
  minimum-dynamic-rate-percent  Configure the minimum dynamic rate for a simple
                                shared shaper as a percentage of the
                                shared-shaping-rate
  no                            Negate a command or set its default(s)
  reaction-factor               Configure how the simple shared shaper reacts
                                to changes in measured rate
  run                           Run an exec mode command (alias command do)
  sleep                         Make the Command Interface pause for a
                                specified duration
```

Queue Profile Configuration Mode

In this mode, you can configure queue profiles and various queue profile parameters, such as constraints on queue lengths or queue buffer weights.

From Global Configuration mode, type the **queue-profile** command followed by a *queueProfileName*, and press Enter.

```
host1(config)#queue-profile testabcd1234
host1(config-queue)#?
  buffer-weight       Set drop threshold in proportion to this weight
  committed-length    Set min and max constraints for committed threshold
  conformed-fraction  Set conformed threshold as a percentage of committed
  conformed-length    Set min and max constraints for conformed threshold
  default             Set a command to its default(s)
  do                  Run an exec mode command (alias command run)
  exceeded-fraction   Set exceeded threshold as a percentage of committed
  exceeded-length     Set min and max constraints for exceeded threshold
  exit                Exit from the current command mode
  help                Describe the interactive help system
  log                 Configure logging settings
  macro               Run a CLI macro
  no                  Negate a command or set its default(s)
  run                 Run an exec mode command (alias command do)
  sleep               Make the Command Interface pause for a specified duration
```

RADIUS Configuration Mode

In this mode, you can configure various parameters of your RADIUS authentication, accounting, and dynamic-request servers.

From Global Configuration mode, type either the **radius authentication server**, **radius accounting server**, or **radius dynamic-request server** command with the server *ipAddress*, and press Enter.

```
host1(config)#radius authentication server 1.2.1.3
host1(config-radius)#?
  deadtime      Configure the amount of time a timed-out server is dropped for usage
  default       Set a command to its default(s)
  do            Run an exec mode command (alias command run)
  exit          Exit from the current command mode
  help          Describe the interactive help system
  key           Configure the secret used in RADIUS client to server exchange
  log           Configure logging settings
  macro         Run a CLI macro
  max-sessions  Configure the number of outstanding requests allowed to the server
  no            Negate a command or set its default(s)
  retransmit    Configure the number of times to retransmit RADIUS request
                before failing
  run           Run an exec mode command (alias command do)
```

```
sleep         Make the Command Interface pause for a specified duration
timeout       Configure the number of seconds to wait for a RADIUS response
              before retransmitting
udp-port      Configure the RADIUS server's UDP port
```

RADIUS Relay Configuration Mode

In this mode, you can configure various parameters of your RADIUS relay authentication and accounting servers.

From Global Configuration mode, type either the **radius relay authentication server** or **radius relay accounting server** command, and press Enter.

```
host1(config)#radius authentication server
host1(config-radius-relay)#?
  default   Set a command to its default(s)
  do        Run an exec mode command (alias command run)
  exit      Exit from the current command mode
  help      Describe the interactive help system
  key       Configure the secret used in RADIUS client to relay server exchange
  log       Configure logging settings
  macro     Run a CLI macro
  no        Negate a command or set its default(s)
  run       Run an exec mode command (alias command do)
  sleep     Make the Command Interface pause for a specified duration
  udp-port  Configure the RADIUS relay server's udp port
```

Rate Limit Profile Configuration Mode

In this mode, you can set parameters for an IP or L2TP rate-limit profile, which is a set of bandwidth attributes and associated actions that become part of a policy list. The policy list is then applied to the ingress or egress of an interface.

To create a hierarchical rate-limit-profile for an IP interface, from Global Configuration mode type **rate-limit-profile** and a *profileName*, and add the keyword **hierarchical**, and press Enter.

To create an IP rate-limit profile, from Global Configuration mode type **ip rate-limit-profile** and a *profileName,* and press Enter.

To create an L2TP rate limit profile, from Global Configuration mode type **l2tp rate-limit-profile** and a *profileName,* and press Enter.

NOTE: If you do not include either the **ip** or **l2tp** keywords, the system creates an IP rate limit profile.

```
host1(config)#ip rate-limit-profile fm78930
host1(config-rate-limit-profile)#?
  committed-action  Set the committed access rate action
  committed-burst   Set the committed access rate burst size in Bytes
  committed-rate    Set the committed access rate value in bits per second
  conformed-action  Set the conformed access rate action
  default           Set a command to its default(s)
  do                Run an exec mode command (alias command run)
  exceeded-action   Set the exceeded action
  exit              Exit from the current command mode
  help              Describe the interactive help system
```

```
log              Configure logging settings
macro            Run a CLI macro
mask-val         Set mask to be applied with mark values
no               Negate a command or set its default(s)
peak-burst       Set the peak burst size in Bytes
peak-rate        Set the peak access rate in bits per second
run              Run an exec mode command (alias command do)
sleep            Make the Command Interface pause for a specified duration
```

Redundancy Configuration Mode

In this mode, you can activate high availability (SRP switchover) by issuing the mode **high-availability** command.

From Global Configuration mode, type the **redundancy** command and press Enter.

```
host1(config-router)#redundancy
host1(config-redundancy)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  mode     Configure redundancy mode
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
```

Remote Neighbor Configuration Mode

In this mode, you can configure remote neighbor parameters for Routing Information Protocol (RIP), Protocol Independent Multicast (PIM), and Open Shortest Path First (OSPF).

From Global Configuration mode, type either **router rip, router pim,** or **router ospf** and the *processID*. Press Enter. You are now in Router Configuration mode.

From Router Configuration mode, type the **remote-neighbor** command and the appropriate attributes, and press Enter.

```
host1(config-router)#remote-neighbor 10.13.5.61
host1(config-router-rn)#?
  authentication        Configure authentication
  default               Set a command to its default(s)
  distribute-list       Specify an access list to be a distribute list
  do                    Run an exec mode command (alias command run)
  exit                  Exit from the current command mode
  exit-remote-neighbor  Exit the remote-neighbor configuration mode
  help                  Describe the interactive help system
  log                   Configure logging settings
  macro                 Run a CLI macro
  no                    Negate a command or set its default(s)
  receive               Set reception characteristics
  route-map             Specify a route map to apply to outgoing routes
  run                   Run an exec mode command (alias command do)
```

```
  send                Set transmit characteristics
  sleep               Make the Command Interface pause for a specified
                      duration
  split-horizon       Enable Split-horizon
  time-to-live        Configure ttl used to send to this neighbor
  update-source       Source address to be used for transmit
```

Route Map Configuration Mode

In this mode, you can create and modify route maps.

From Global Configuration mode, type the **route-map** command and the appropriate *routeMapNumber*, and press Enter.

```
host1(config)#route-map unis889
host1(config-route-map)#?
  default    Set a command to its default(s)
  do         Run an exec mode command (alias command run)
  exit       Exit from the current command mode
  help       Describe the interactive help system
  log        Configure logging settings
  macro      Run a CLI macro
  match      Identify this entry as requiring an attribute match
  match-set  Identify this entry to match and set attributes
  no         Negate a command or set its default(s)
  run        Run an exec mode command (alias command do)
  set        Configure this entry to set attributes
  sleep      Make the Command Interface pause for a specified duration
```

Router Configuration Mode

In this mode, you can configure a routing protocol using **router** commands.

From Global Configuration mode, type the **router** command and the appropriate router attributes, and press Enter.

```
host1(config)#router bgp 2378
host1(config-router)#?
  address-family                Enter address family configuration mode
  aggregate-address             Create an aggregate entry in BGP routing table
  auto-summary                  Automatic summarization of redistributed routes
                                to their natural network masks
  bgp                           Configure BGP
  default                       Set a command to its default(s)
  default-fields                Set default fields for show commands
  default-information           Configure the distribution of default routing
                                information
  disable-dynamic-redistribute  disable dynamic importing of routing
                                information with the latest policy
  distance                      Configure administrative distances for routes
  do                            Run an exec mode command (alias command run)
  exit                          Exit from the current command mode
  help                          Describe the interactive help system
  ip                            Configure the type of route to be contributed
                                by this BGP address family
  limits                        Configure limits on internal BGP tables
  log                           Configure logging settings
  macro                         Run a CLI macro
  maximum-paths                 Configure the maximum number of equal-cost paths
  neighbor                      Specify neighbor properties
```

```
  network                     Identify a network for BGP to announce
  no                          Negate a command or set its defaults
  overload                    Configure BGP behaviour when reaching overload
                              state (no more resources available)
  redistribute                Configure the redistribution of routing
                              information from another protocol
  rib-out                     Configure rib-out storage for all BGP peers
  run                         Run an exec mode command (alias command do)
  sleep                       Make the Command Interface pause for a
                              specified duration
  synchronization             Enable synchronization with the IGP
  table-map                   Specify a table map to map external entry
                              attributes into routing table
  timers                      Configure the keep-alive interval and the hold-time
```

RSVP Configuration Mode

In this mode, you can create and configure MPLS Resource Reservation Protocol (RSVP) parameters.

From Global Configuration mode, type **mpls rsvp interface profile** and the *profileName*, and press Enter.

```
host1(config)#mpls rsvp interface profile sprint
host1(config-rsvp)#?
  cleanup-timeout-factor  Configure the timeout factor
  default                 Set a command to its default(s)
  do                      Run an exec mode command (alias command run)
  exit                    Exit from the current command mode
  help                    Describe the interactive help system
  log                     Configure logging settings
  macro                   Run a CLI macro
  no                      Negate a command or set its default(s)
  refresh-period          Configure refresh period
  run                     Run an exec mode command (alias command do)
  sleep                   Make the Command Interface pause for a specified
                          duration
```

RTR Configuration Mode

In this mode, you can configure Response Time Reporter (RTR) parameters. The RTR feature allows you to monitor your network's performance and its resources by measuring response times and the availability of your network devices.

From Global Configuration mode, type **rtr** and the *mapNumber*, and press Enter.

```
host1(config)#rtr 784078348
host1(config-rtr)#?
  default                   Set a command to its default(s)
  do                        Run an exec mode command (alias command run)
  exit                      Exit from the current command mode
  frequency                 Specify the frequency interval
  help                      Describe the interactive help system
  hops-of-statistics-kept   Specify the hops capture
  log                       Configure logging settings
  macro                     Run a CLI macro
  max-response-failure      Specify the maximum number of consecutive failures
  no                        Negate a command or set its default(s)
  operations-per-hop        Specify a number of operations per hop
  owner                     Specify the owner of entry
```

```
request-data-size        Specify the request payload size
run                      Run an exec mode command (alias command do)
samples-of-history-kept  Specify the maximum history samples
sleep                    Make the Command Interface pause for a specified duration
tag                      Specify the user defined tag
timeout                  Specify the operation timeout
tos                      Specify a value for the ToS byte
type                     Specify the type of the entry
```

Scheduler Profile Configuration Mode

In this mode, you can configure a scheduler profile. You can then set the shaping rate value, enable the strict-priority scheduling for the scheduler node, or set the weighted-round-robin (WRR) value of the scheduler node or queue.

From Global Configuration mode, type **scheduler-profile** and the *scheduleProfileName* that you want to create or configure, and press Enter.

```
host1(config)#scheduler-profile A990
host1(config-scheduler-profile)#?
  default          Set a command to its default(s)
  do               Run an exec mode command (alias command run)
  exit             Exit from the current command mode
  help             Describe the interactive help system
  log              Configure logging settings
  macro            Run a CLI macro
  no               Negate a command or set its default(s)
  run              Run an exec mode command (alias command do)
  shaping-rate     Shape the node or queue to the specified rate
  sleep            Make the Command Interface pause for a specified duration
  strict-priority  Dequeue strict priority packets ahead of other packets
  weight           Set the relative weight of the node or queue
```

Service Session Profile Configuration Mode

In this mode, you can set and modify Service Manager service session profile attributes, such as time, volume, and statistics.

From Global Configuration mode, type the **service-management service-session-profile** command and the *profileName*, and then press Enter.

```
host1(confi)#service-management service-session-profile vodISP1
host1(config-service-session-profile)#?
  default     Set a command to its default(s)
  do          Run an exec mode command (alias command run)
  exit        Exit from the current command mode
  help        Describe the interactive help system
  log         Configure logging settings
  macro       Run a CLI macro
  no          Negate a command or set its default(s)
  run         Run an exec mode command (alias command do)
  sleep       Make the Command Interface pause for a specified duration
  statistics  Configure statistics
  time        Configure time
  volume      Configure volume
```

SNMP Event Manager Configuration Mode

In this mode, you can configure certain SNMP triggers for events, what occurs when an event is triggered, resource limits for triggers, and some trap notification options.

From Global Configuration mode, type the **snmp-server management-event** command and then press Enter.

```
host1(config)#snmp-server management-event
host1(config-mgmtevent)#?
  default   Set a command to its default(s)
  do        Run an exec mode command (alias command run)
  event     Specify what happens when an event is triggered
  exit      Exit from the current command mode
  help      Describe the interactive help system
  log       Configure logging settings
  macro     Run a CLI macro
  no        Negate a command or set its default(s)
  resource  Specify the resource limits
  run       Run an exec mode command (alias command do)
  sleep     Make the Command Interface pause for a specified duration
  trigger   Specify the conditions that lead to events
```

Statistics Profile Configuration Mode

In this mode, you can configure a statistics profile. You can then set the rate period during which statistics are gathered, enable statistics gathering, and enable the counting of drop and forwarding events.

From Global Configuration mode, type **statistics-profile** and the *statisticsProfileName* that you want to create or configure, and press Enter.

```
host1(config)#statistics-profile statpro-1
host1(config-statistics-profile)#?
  committed-drop-threshold   Set threshold for logging a committed-drop event
  conformed-drop-threshold   Set threshold for logging a conformed-drop event
  default                    Set a command to its default(s)
  do                         Run an exec mode command (alias command run)
  exceeded-drop-threshold    Set threshold for logging an exceeded-drop event
  exit                       Exit from the current command mode
  forwarding-rate-threshold  Set threshold for logging a forwarding-rate event
  help                       Describe the interactive help system
  log                        Configure logging settings
  macro                      Run a CLI macro
  no                         Negate a command or set its default(s)
  rate-period                Set the time period for calculating queue rates
  run                        Run an exec mode command (alias command do)
  sleep                      Make the Command Interface pause for a specified
                             duration
```

Subinterface Configuration Mode

In this mode, you can configure one or more virtual interfaces, called *subinterfaces*, on a single physical interface. The system supports this feature with ATM and Frame Relay.

Both ATM and Frame Relay provide permanent virtual circuits (PVCs) that can be grouped under separate subinterfaces configured on a single physical interface. Subinterfaces allow multiple encapsulations for a protocol on a single interface.

From Interface Configuration mode, indicate a subinterface by typing the **interface** command and an *interfaceSpecifier* in s*lot/port.subinterface* format, and then press Enter. For example:

```
host1(config-if)#interface atm 3/2.6
host1(config-subif)#
```

Subscriber Policy Configuration Mode

In this mode, you can configure a policy (a set of forwarding and filtering rules) that defines how a subscriber (client) bridge group interface should handle various packet types. After you define the policy, use the **bridge subscriber-policy** command (from Global Configuration mode) to associate the policy with a bridge group interface.

From Global Configuration mode, type the **subscriber-policy** command followed by an alphanumeric policy name of any character length, and press Enter.

```
host1(config)#subscriber-policy client1
host1(config-policy)#?
  arp                  Modify arp policy
  broadcast            Modify broadcast policy
  default              Set a command to its default(s)
  do                   Run an exec mode command (alias command run)
  exit                 Exit from the current command mode
  help                 Describe the interactive help system
  ip                   Modify ip policy
  log                  Configure logging settings
  macro                Run a CLI macro
  mpls                 Modify mpls policy
  multicast            Modify multicast policy
  no                   Negate a command or set its default(s)
  pppoe                Modify PPPoE policy
  relearn              Modify relearn policy
  run                  Run an exec mode command (alias command do)
  sleep                Make the Command Interface pause for a specified
                       duration
  unicast              Modify user-to-user (Unicast) policy
  unknown-destination  Modify unknown destination policy
  unknown-protocol     Modify unknown protocol policy
```

Traffic Class Configuration Mode

In this mode, you can create a traffic class and configure the level of service to packets assigned to the traffic class.

From Global Configuration mode, type the **traffic-class** command followed by a *trafficClassName*, and then press Enter.

```
host1(config)#traffic-class test123
host1(config-traffic-class)#?
  default                 Set a command to its default(s)
  do                      Run an exec mode command (alias command run)
  exit                    Exit from the current command mode
  fabric-strict-priority  Allow packets in this class to be dequeued out of the
                          fabric ahead of other traffic classes
  help                    Describe the interactive help system
  log                     Configure logging settings
  macro                   Run a CLI macro
```

```
no                    Negate a command or set its default(s)
run                   Run an exec mode command (alias command do)
sleep                 Make the Command Interface pause for a specified duration
```

Traffic Class Group Configuration Mode

In this mode, you can create and configure traffic-class groups, which can contain multiple traffic classes.

From Global Configuration mode, type the **traffic-class-group** command and a *trafficClassGroupName*, and press Enter.

```
host1(config)#traffic-class-group trafclasnameabcd
host1(config-traffic-class-group)#?
  default        Set a command to its default(s)
  do             Run an exec mode command (alias command run)
  exit           Exit from the current command mode
  help           Describe the interactive help system
  log            Configure logging settings
  macro          Run a CLI macro
  no             Negate a command or set its default(s)
  run            Run an exec mode command (alias command do)
  sleep          Make the Command Interface pause for a specified duration
  traffic-class  Set the traffic class belong to this group
```

Tunnel Group Configuration Mode

In this mode, you can define up to 31 tunnels for a tunnel group.

From Global Configuration mode, type **aaa tunnel-group** and the *groupName*, and press Enter.

```
host1(config)#aaa tunnel-group storm
host1(config-tunnel-group)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
  tunnel   Configure tunnel tag
```

Tunnel Group Tunnel Configuration Mode

In this mode, you can configure attributes for a tunnel group tunnel.

From Tunnel Group Configuration mode, type **tunnel** and the tag number (in the range 1–31) for the tunnel, and press Enter.

```
host1(config-tunnel-group)#tunnel 1
host1(config-tunnel-group-tunnel)#?
  address         Configure tunnel endpoint address
  client-name     Configure the client hostname of the tunnel
  default         Set a command to its default(s)
  do              Run an exec mode command (alias command run)
  exit            Exit from the current command mode
```

```
  help            Describe the interactive help system
  identification  Configure tunnel identification
  log             Configure logging settings
  macro           Run a CLI macro
  max-sessions    Configure maximum sessions for this tunnel
  medium          Configure tunnel medium
  no              Negate a command or set its default(s)
  password        Configure tunnel password
  preference      Configure tunnel preference
  receive-window  Configure the receive window size for this tunnel
  router-name     Configure the virtual-router for the domain name
  run             Run an exec mode command (alias command do)
  server-name     Configure the remote hostname for the tunnel
  sleep           Make the Command Interface pause for a specified duration
  source-address  Configure tunnel source address
  type            Configure tunnel type
```

Tunnel Profile Configuration Mode

In this mode, you can create and configure MPLS tunnel profiles.

From Global Configuration mode, type **mpls tunnels profile** and the *profileName*, and press Enter.

```
host1(config)#mpls tunnels profile storm
host1(config-tunnelprofile)#?
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
  tunnel   Configure tunnel interface parameters
```

Tunnel Server Configuration Mode

In this mode, you can configure (provision) the maximum number of tunnel-service interfaces to be used on a dynamic tunnel-server port.

From Global Configuration mode, type **tunnel-server** and the slot number and port number of the dynamic tunnel-server port, and press Enter.

```
host1(config)#tunnel-server 2/2
host1(config-tunnel-server)#?
  default         Set a command to its default(s)
  do              Run an exec mode command (alias command run)
  exit            Exit from the current command mode
  help            Describe the interactive help system
  log             Configure logging settings
  macro           Run a CLI macro
  max-interfaces  Configure maximum number of tunnel-server interfaces for
                  dynamic server port
  no              Negate a command or set its default(s)
  run             Run an exec mode command (alias command do)
  sleep           Make the Command Interface pause for a specified duration
```

VRF Configuration Mode

In this mode, you can create and configure VRF parameters for BGP/MPLS VPNs.

From Global Configuration mode, type **ip vrf** and the *vrfName*, and press Enter. Confirm the new VRF by pressing Enter.

```
host1(config)#ip vrf yankee
Proceed with new vrf creation? [confirm]
host1(config-vrf)#?
  default       Set a command to its default(s)
  description   Configure VRF specific description
  do            Run an exec mode command (alias command run)
  exit          Exit from the current command mode
  export        Specify VRF export characteristics
  help          Describe the interactive help system
  import        Specify VRF import characteristics
  ip            Configure IP characteristics
  log           Configure logging settings
  macro         Run a CLI macro
  maximum       Specify a maximum limit
  no            Negate a command or set its default(s)
  rd            Specify route distinguisher
  route-target  Specify VPN extended community Target
  run           Run an exec mode command (alias command do)
  sleep         Make the Command Interface pause for a specified duration
```

VR Group Configuration Mode

In this mode, you can add up to four virtual routers to the virtual router group. The accounting servers of the virtual routers in the group can receive AAA broadcast accounting records.

From Global Configuation mode, type **aaa accounting vr-group** and the *vrGroupName*, and press Enter.

```
host1(config)#aaa accounting vr-group westVrGroup38
host1(config-vr-group)#?
  aaa      Configure authentication, authorization, and accounting
           characteristics
  default  Set a command to its default(s)
  do       Run an exec mode command (alias command run)
  exit     Exit from the current command mode
  help     Describe the interactive help system
  log      Configure logging settings
  macro    Run a CLI macro
  no       Negate a command or set its default(s)
  run      Run an exec mode command (alias command do)
  sleep    Make the Command Interface pause for a specified duration
  support  Enter Support mode
```

Chapter 3

Installing JUNOSe Software

The JUNOSe software resides on a nonvolatile storage (NVS) card located in the switch route processor (SRP) module. Each SRP module is shipped with an NVS card that contains a software release. Each SRP module is shipped with an NVS card that contains a software release. New software releases are shipped on a set of CDs. You can also download software releases from the Juniper Networks Web site. This chapter provides information on how to install a new software release on a router and contains the following sections:

- Overview on page 113
- Platform Considerations on page 115
- Installing Software When a Firewall Exists on page 115
- Installing Software When a Firewall Does Not Exist on page 120
- Copying Release Files from One Router to Another on page 128
- Upgrading Systems That Are Operating with Two SRP Modules on page 129
- Upgrading from Release 5.1.1 or Lower-Numbered Releases on page 130
- Downgrading JUNOSe Software on page 133

CAUTION: See the *Release Notes* for extra information about installing and upgrading the software.

Overview

If the router contains only one SRP module, we recommend you divert traffic to another router before installing a new software release because the router is unavailable during the installation process. Depending on whether a firewall separates the router from the network host, you can then complete the appropriate software installation. (See *Installing Software When a Firewall Exists* on page 115 or *Installing Software When a Firewall Does Not Exist* on page 120.) However, if the router contains two SRP modules, you can upgrade the software while the system is operating. (See *Upgrading Systems That Are Operating with Two SRP Modules* on page 129.)

When installing new JUNOSe software, you must copy the contents of the release files to a network host and transfer the release files to at least one router in the network. Depending on the network configuration, you can copy the release files from either the network host or the first router to the other routers in the network. (See *Copying Release Files from One Router to Another* on page 128.)

NOTE: Some line modules and SRP modules on ERX-14xx models, ERX-7xx models, and the ERX-310 router require a minimum amount of memory to be used with JUNOSe Release 5.3.0 or a higher-numbered release. See the *ERX Module Guide* for module specifications.

Identifying the Software Release File

You can find the software release file on one of the following JUNOSe software CDs:

- JUNOSe <*release*> #1—Contains the release files for the ERX-7xx routers, the ERX-14xx routers, and the ERX-310 router
- JUNOSe <*release*> #2—Contains the release file for the E120 and the E320 router, the MIB directory, and the *Release Notes*

You can also download a compressed version of the software release by logging on to https://www.juniper.net/support/. The .zip file that you download contains the software release file.

The release is in the software directory, which is identified by the release number. For example, if the release number is x.y.z, the name of the directory is x-y-z. See Table 12.

Table 12: Software Release Files

Router	File Format (x-y-z is the release number)
E120 and E320	e320_x-y-z.rel
ERX-1440	erx40_x-y-z.rel
ERX-310	erx310_x-y-z.rel
All other E-series routers	erx_x-y-z.rel

To identify the software release file:

1. Access the software directory.
2. Find the files with the extension .rel.

The procedures outlined in the following sections provide detailed instructions for typical installations. For additional information about commands and troubleshooting, see *Chapter 2, Command-Line Interface* and *JUNOSe Command Reference Guide, About This Guide*

Platform Considerations

You can install JUNOSe software on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Installing Software When a Firewall Exists

When a firewall separates the router from the network host, you must use FTP to transfer the software release files from the network host to the router. In this case, you must configure the FTP server on the router and ensure that FTP client software is installed on the network host.

For this network configuration, you must install the software from the normal operational mode of the command-line interface (CLI). You can access the CLI through either the local console or a Telnet session. If you have not yet configured the router to support Telnet, then you must use the local console.

To install the software, perform the following tasks. (See Table 13.)

Table 13: Software Installation Procedure When a Firewall Exists

1. Obtain the required information for the installation.
2. For routers that are currently operating, divert network traffic to another router.
3. Access the Privileged Exec CLI command mode.
4. Configure IP on an interface.
5. Copy the release files on the network host.
6. Configure access to the network host.
7. Enable the FTP server on the router.
8. Identify the files to transfer.
9. Transfer the files to the user space on the router.
10. Install the software release file to the system space on the router.
11. Save the current configuration.
12. Reboot the system.

Task 1: Obtain the Required Information

Before you install the software, obtain the following information:

- The password (if one is configured) that enables you to access Privileged Exec mode on the router
- The IP address of the network host

- The IP address of the router
- The IP address of the next hop to reach the destination network (for example, a gateway)
- The login name and password for the vty line
- The procedure for copying the release files to the network host

Task 2: Divert Network Traffic to Another Router

The system will be unavailable during the installation process.

Task 3: Access Privileged Exec Mode

To access this mode via the CLI:

1. Issue the enable command.

   host1>**enable**

2. Type the password if the system prompts you.

Task 4: Configure IP on an Interface

Typically, you configure IP on the Fast Ethernet interface of the SRP module. To configure IP on an interface:

1. Determine the slot number of the module.

   host1#**show version**

2. Determine the port number of the module.
3. Determine whether the interface already has an IP address.

   - On ERX-7xx models, ERX-14xx models, and the ERX-310 router:

   host1#**show ip interface fastEthernet 6/0**

   - On the E120 router and the E320 router:

   host1#**show ip interface fastEthernet 6/0/0**

NOTE: If an IP interface is not configured, an Invalid interface message appears.

If the interface already has an IP address, go to Step 5. Otherwise, proceed with Step 4.

4. Configure an IP address on the interface.

   - On ERX-7xx models, ERX-14xx models, and the ERX-310 router:

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**interface fastEthernet 6/0**
   host1(config-if)#***ip address*** *ipAddress [mask]*

   - On the E120 router and the E320 router:

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**interface fastEthernet 6/0/0**
   host1(config-if)#***ip address*** *ipAddress [mask]*

5. Press Ctrl + z to return to Privileged Exec mode.

Task 5: Copy the Release Files to the Network Host

If you downloaded the software from the Juniper Networks Web site as a .zip file, uncompress the files to a directory, and copy the release files to the network host.

If you are accessing the release files from one of the software CDs, you must mount the CD. The way you mount the release files on the network host depends on the type of computer you use, the operating system, and the network configuration. To find out how to mount the release files on the network host, review the manual for the operating system, or contact your network administrator.

Task 6: Configure Access to the Network Host

To configure access to the network host:

1. Use the **ping** command to determine whether the router can reach the network host.

   host1#**ping** *hostname*

   If the router can reach the network host, go to the next section. Otherwise, go to Step 2.

2. Determine whether a route exists between the router and the network host.

   host1#**show ip route**

   If the appropriate route is displayed, go to Step 5. Otherwise, proceed with Step 3.

3. Configure a route to reach the network host.

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**ip route** *ipNetwork networkMask ipNextHop*

4. Press Ctrl + z to return to Privileged Exec mode.

5. Determine whether the router has been configured to recognize the network host.

   host1#**show host**

   If the network host is listed, go to Step 8. Otherwise, proceed with Step 6.

6. Add an entry to the Static Host Table so that the router can access the network host. Use the **host** command to specify the network hostname and IP address.

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**host** *hostName ipAddress ftp loginname password*

7. Press Ctrl + z to return to Privileged Exec mode.

8. Use the **ping** command to determine whether the router can now reach the network host.

   host1#**ping** *hostname*

   If the router cannot reach the network host, verify that you correctly performed the previous steps in this procedure and that the network host is operational.

Task 7: Enable the FTP Server on the Router

The router divides its vty resources among Telnet, SSH, and FTP services. Each FTP session requires one vty line, and the FTP service uses the authentication method configured for the vty line. If you configured more than one vty line for Telnet access, the FTP service uses one of those lines. If you configured only one line for Telnet access, configure another vty line.

To enable the FTP server, use the **ftp-server enable** command.

host1(config)#**ftp-server enable**

Task 8: Identify the Files to Transfer

To identify all the files for the release, use a text editor to open the software release (.rel) file on the JUNOSe software CD or from the directory in which you downloaded from the Juniper Networks Web site. The software release file contains a list of all the files associated with the release. You must transfer the software release file and all the files it contains to the user space.

Task 9: Transfer Files to the User Space

To transfer the files for the release to the user space, use the FTP client software on the network host to connect to the FTP server on the router. Transfer the files to a subdirectory within the incoming directory. If you specify a subdirectory that does not exist, the router creates the directory.

NOTE: Be sure to transfer the software release file and all the files it lists.

Task 10: Install Files on the System Space

Installing the software release file to the system space installs all files listed in the software release file. To install the software release file from the incoming directory in the user space to the router space, use the **copy** command.

Be sure to specify the correct software release (.rel) filename for the router you are using, as described in *Identifying the Software Release File* on page 114.

NOTE: The destination file must have a .rel extension.

For example:

host1#**copy /incoming/releases/erx_x-y-z.rel erx_x-y-z.rel**

The software release is copied from the user space to the system space. This process can take several minutes.

Task 11: Save the Current Configuration

To save the current configuration, use the **copy running-configuration** command:

host1#**copy running-configuration** *filename.cnf*

Task 12: Reboot the System

To reboot the system using the newly installed software:

1. Access Global Configuration mode.

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#

2. Run the **boot system** command, specifying the .rel filename of the software release.

   For example:

   host1(config)#**boot system erx_x-y-z.rel**

The following message appears when you issue this command:

WARNING: We recommend that you copy the current running-configuration to a file prior to reloading a different release of software.

3. Press Ctrl + z to return to Privileged Exec mode.

4. Verify that the router is ready to boot with the new software release.

   host1#**show boot**

   If the old software version is still listed, verify that you completed the previous steps correctly.

5. Run the **reload** command.

   host1#**reload**

   The following message appears when you issue this command:

   WARNING: Execution of this command will cause the system to reboot. Proceed with reload? [confirm]

   The system reboots. The reboot might take longer than normal because line modules initialize with the old version of the software, acquire the new version from the SRP module, and reinitialize. When you observe the LEDs on the line modules, the line modules appear to boot twice.

Installing Software When a Firewall Does Not Exist

If there is no firewall between the router and the network host to which you copied the release files, you can transfer the software release files from the network host to the router via the FTP server or by issuing the **copy** command. To transfer files via the FTP server, refer to the previous section, *Installing Software When a Firewall Exists*. This section describes how to transfer files by issuing the **copy** command.

If you use the **copy** command to transfer the files, the network host must be an FTP server. This command activates an FTP client on the router.

For this network configuration, you can install the software in the normal command line interface (CLI) operational mode or in boot mode.

Installing Software in Normal Operational Mode

For this procedure, you must access the CLI through either the local console or a Telnet session. If you have not yet configured the router to support Telnet, then you must use the local console.

To install the software, perform the following tasks. (See Table 14.)

Table 14: Software Installation Procedure When a Firewall Does Not Exist

1. Obtain the required information for the installation.
2. For routers that are currently operating, divert network traffic to another router.
3. Access the Privileged Exec CLI command mode.
4. Configure IP on an interface.
5. Configure access to the network host.
6. Copy the release files to the network host.
7. Copy the software release file to the router.
8. Save the current configuration.
9. Reboot the system.

Task 1: Obtain the Required Information

Before you install the software, obtain the following information:

- The password (if one is configured) that enables you to access Privileged Exec mode on the router
- The IP address of the network host
- The IP address of the router
- The IP address of the next hop to reach the destination network (for example, a gateway)
- The login name and password for the FTP server
- The procedure for copying the release files to the network host

Task 2: Divert Network Traffic to Another Router

The system will be unavailable during the installation process.

Task 3: Access Privileged Exec Mode

To access this mode via the CLI:

1. Issue the enable command.

   host1>**enable**

2. Type the password if the system prompts you.

Task 4: Configure IP on an Interface

Typically, you configure IP on the Fast Ethernet interface of the SRP module. To configure IP on an interface:

1. Determine the slot number of the module.

   host1#**show version**

2. Determine the port number of the module.

3. Determine whether the interface already has an IP address.

   - On ERX-7xx models, ERX-14xx models, and the ERX-310 router:

   host1#**show ip interface fastEthernet 6/0**

   - On the E120 router and the E320 router:

   host1#**show ip interface fastEthernet 6/0/0**

NOTE: If an IP interface is not configured, an Invalid interface message appears.

   If the interface already has an IP address, go to Step 5. Otherwise, proceed with Step 4.

4. Configure an IP address on the interface.

   - On ERX-7xx models, ERX-14xx models, and the ERX-310 router:

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**interface fastEthernet 6/0**
   host1(config-if)#***ip address*** *ipAddress [mask]*

   - On the E120 router and the E320 router:

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**interface fastEthernet 6/0/0**
   host1(config-if)#***ip address*** *ipAddress [mask]*

5. Press Ctrl + z to return to Privileged Exec mode.

Task 5: Configure Access to the Network Host

To configure access to the network host:

1. Use the **ping** command to determine whether the router can reach the network host.

   host1#**ping** *ipAddress*

   If the router can reach the network host, go to the next section. Otherwise, go to Step 2.

2. Determine whether a route exists between the router and the network host.

   host1#**show ip route**

   If the appropriate route is displayed, go to Step 4. Otherwise, proceed with Step 3.

3. Configure a route to reach the network host.

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**ip route** *ipNetwork networkMask ipNextHop*

4. Press Ctrl + z to return to Privileged Exec mode.

5. Determine whether the router has been configured to recognize the network host.

   host1#**show host**

   If the network host is listed, go to Step 8. Otherwise, proceed with Step 6.

6. Add an entry to the Static Host Table so that the router can access the network host. Use the **host** command to specify the network hostname and IP address.

   host1#**configure**
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#**host** *hostName ipAddress* **ftp** *loginname password*

7. Press Ctrl + z to return to Privileged Exec mode.

8. Use the **ping** command to determine whether the router can now reach the network host.

   host1#**ping** *hostname*

   If the router cannot reach the network host, verify that you correctly performed the previous steps in this procedure and that the network host is operational.

Task 6: Copy the Release Files to the Network Host

If you downloaded the software from the Juniper Networks Web site as a .zip file, uncompress the files to a directory, and copy the release files to the network host.

If you are accessing the release files from one of the software CDs, you must mount the CD. The way you mount the CD on the network host depends on the type of network host you use, the operating system, and the way your network is configured. To find out how to mount a CD on the network host, review the manual for the operating system, or contact your network administrator.

Task 7: Copy the Software Release File to the Router

To copy the software release file to the router, use the **copy** command.

Be sure to specify the correct software release (.rel) filename for the router you are using, as described in *Identifying the Software Release File* on page 114.

NOTE: The destination file must have a .rel extension.

For example:

host1#**copy** *hostname:/cdrom/x-y-z/erx_x-y-z.rel erx_x-y-z.re***l**

The software release is copied from the network host to the router. This process can take several minutes.

Task 8: Save the Current Configuration

To save the current configuration, use the **copy running-configuration** command:

host1#**copy running-configuration** *filename.cnf*

Task 9: Reboot the System

To reboot the system using the newly installed software:

1. Access Global Configuration mode.

   ```
   host1#configure
   Configuring from terminal or file [terminal]?
   Enter configuration commands, one per line. End with CNTL/Z.
   host1(config)#
   ```

2. Run the **boot system** command, specifying the .rel filename of the software release. For example:

   host1(config)#**boot system** *erx_x-y-z.rel*

   The following message appears when you issue this command:

   WARNING: We recommend that you copy the current running- configuration to a file prior to reloading a different release of software.

3. Press Ctrl + z to return to Privileged Exec mode.

4. Make sure that the router is ready to boot with the new software release.

   host1#**show boot**

   If the old software version is still listed, verify that you completed the previous steps correctly.

5. Run the **reload** command.

   host1#**reload**

   The following message appears when you issue this command:

   WARNING: Execution of this command will cause the system to reboot. Proceed with reload? [confirm]

   The system reboots. The reboot might take longer than normal because line modules initialize with the old version of the software, acquire the new version from the SRP module, and reinitialize. When you observe the LEDs on the line modules, the line modules appear to boot twice.

Installing Software in Boot Mode

To install the software in Boot mode, you must access the CLI via the local console.

To install the software, perform the following tasks. (See Table 15.)

Table 15: Software Installation Procedure in Boot Mode

1. Obtain the required information for the installation.
2. For routers that are currently operating, divert network traffic to another router.
3. Access the Boot mode.
4. Assign an IP address to the router.
5. Configure access to the network host.
6. Reset the SRP module.
7. Copy the release files to the network host.
8. Copy the software release file to the router.
9. Reboot the system.

Task 1: Obtain the Required Information

Before you install the software, obtain the following information:

- The IP address of the network host
- The IP address of the router
- The IP address of the next hop to reach the destination network (for example, a gateway)

- The login name and password for the FTP server
- The procedure for copying the release files to the network host

Task 2: Divert Network Traffic to Another System

The system will be unavailable during the installation process.

Task 3: Access the Boot Mode

To access Boot mode from the local console:

1. At the Privileged Exec prompt, type the **reload** command.

   Information on the reloading process appears.

2. When the countdown begins, press the key sequence **mb**.

   This action puts the CLI in Boot mode and the `:boot##` prompt appears.

NOTE: If you do not press the key sequence **mb** before the countdown ends, the reloading process continues and returns the CLI to the normal User Exec mode.

Task 4: Assign an IP Address

When you assign an IP address to the router in Boot mode, the address is configured on the Fast Ethernet port of the primary SRP module. To assign an Internet address to the router, use the **ip address** command.

:boot##**ip address** *ipAddress [mask]*

Task 5: Configure Access to the Network Host

To configure access to the network host:

1. Configure a gateway through which the router can reach the network host.

   :boot##**ip gateway** *ipAddress*

2. Determine whether the router has been configured to recognize the network host.

   :boot##**show host**

   If the network host is listed, go to the next section. Otherwise, proceed with Step 3.

3. Add an entry to the Static Host Table so that the router can access the network host.

   :boot##**host** *hostName ipAddress* **ftp** *login-name password*

   Use the **host** command to specify the network host name and IP address.

Task 6: Resetting the SRP Module

To ensure that the IP addresses are properly activated, you must reset the SRP module. To reset the SRP module, issue the **reload** command from the `:boot##` prompt or depress the recessed module reset button located on the front of the module.

Depressing the module reset button on the SRP module is equivalent to rebooting the router and causes all of the line modules to reboot.

Task 7: Copy the Release Files to the Network Host

If you downloaded the software from the Juniper Networks Web site as a .zip file, uncompress the files to a directory, and copy the release files to the network host.

If you are accessing the release files from one of the software CDs, you must mount the CD. The way you mount the CD on the network host depends on the type of network host you use, the operating system, and the way your network is configured. To find out how to mount a CD on the network host, review the manual for the operating system, or contact your network administrator.

Task 8: Copy the Software Release File to the Router

To copy the software release file to the router, use the **copy** command.

Be sure to specify the correct software release (.rel) filename for the router you are using, as described in *Identifying the Software Release File* on page 114.

NOTE: The destination file must have a .rel extension.

For example:

:boot##**copy** *hostname:/cdrom/x-y-z/erx_x-y-z.rel erx_x-y-z.rel*

The software release is copied from the network host to the router. This process can take several minutes.

Task 9: Reboot the System

To reboot the system using the newly installed software:

1. Run the **boot system** command, specifying the .rel filename of the software release. For example:

   :boot##**boot system** *erx_x-y-z.rel*

   The following message appears when you issue this command:

   WARNING: We recommend that you copy the current running-configuration to a file prior to reloading a different release of software.

2. Run the **reload** command.

   :boot##**reload**

   The following message appears when you issue this command:

   WARNING: Execution of this command will cause the system to reboot. Proceed with reload? [confirm]

   The system reboots. The reboot might take longer than normal because line modules initialize with the old version of the software, acquire the new version from the SRP module, and reinitialize. When you observe the LEDs on the line modules, the line modules appear to boot twice.

Copying Release Files from One Router to Another

When you have copied the release files from a network host to one router, you can transfer files from that router to other routers on the network. This feature is useful when:

- The other routers are unreachable from the network host but have network connectivity to the router on which you installed the new software.
- The connection between routers is faster than the connection between a router and the network host to which it is connected.

The procedures for transferring release files from a source router to a destination router are almost identical to transferring release files from a network host to a router on the same side of the firewall.

NOTE: You must enable the FTP server on the source router.

To transfer release files from a source router to a destination router, follow the instructions in *Installing Software When a Firewall Does Not Exist* on page 120, with the following changes:

- Substitute the source router for the network host.
- Omit the step about copying the release files to the network host.
- Copy the file to the system space of the second router from the user space of the first router.

  Be sure to specify the correct software release (.rel) filename for the router you are using, as described in *Identifying the Software Release File* on page 114.

  For example:

  host1#**copy** *boston:/outgoing/releases/erx_x-y-z.rel erx_x-y-z.rel*

Upgrading Systems That Are Operating with Two SRP Modules

Use this procedure when the system contains two SRP modules and is already operating with an earlier software release. Each SRP module keeps the system operational while you upgrade the software on the other, so that you can minimize service interruption.

CAUTION: You must upgrade the software on the redundant SRP module when you upgrade the software on the primary SRP module. This action prevents the redundant SRP module from overwriting the new software on the primary SRP module if the primary SRP module fails and the redundant SRP module takes control.

To upgrade the software on a system that is operational and contains two SRP modules:

1. Turn off autosynchronization.

   host1(config)#**disable-autosync**

2. Copy the new release of the software to NVS of the primary SRP module. Be sure to specify the correct software release (.rel) filename for the router you are using, as described in *Identifying the Software Release File* on page 114.

   - If a firewall separates the router from the network host, transfer files to the user space with the FTP client on the network host, and install files on the system space (See *Installing Software When a Firewall Exists* on page 115.) For example:

     host1#**copy** */incoming/releases/erx_x-y-z.rel erx_x-y-z.rel*

   - If no firewall separates the router from the network host, copy the files to the router (See *Installing Software When a Firewall Does Not Exist* on page 120.) For example:

     host1#**copy** *hostname:/cdrom/x-y-z/erx_x-y-z.rel erx_x-y-z.rel*

   - If you are transferring the files from one router to another, copy the file to the system space of the second router from the user space of the first router (See *Copying Release Files from One Router to Another* on page 128.) For example:

     host1#**copy** *boston:/outgoing/releases/erx_x-y-z.rel erx_x-y-z.rel*

3. Save the current configuration. For example:

   host1#**copy running-configuration** *system2.cnf*

4. Specify that the router should use the new software release when it reboots. For example:

   host1(config)#**boot system** *erx_x-y-z.rel*

5. Synchronize the NVS file system of the redundant module with that of the primary module.

   host1#**synchronize**

   The redundant SRP module automatically reboots because the software release that it is configured to run differs from the software release it is running.

CAUTION: The secondary SRP module does not run the new software until it reboots. If you issue the **srp switch** command or the primary SRP module fails before the redundant SRP module reboots, then the secondary SRP module runs with the old release when it takes control.

6. Wait for the redundant SRP module to boot, initialize, and reach the standby state. When the module is in standby state, the REDUNDANT LED is on and the ONLINE LED is off. The State field in the **show version** display indicates the module is in standby.

   After any type of reboot, the primary and redundant SRP module NVS file systems are unsynchronized again.

7. Synchronize the NVS file system of the redundant module with that of the primary module.

   host1#**synchronize**

8. Switch from the primary SRP module to the redundant SRP module.

   host1#**srp switch**

   The redundant SRP module becomes the primary. The former primary SRP module reboots and becomes the redundant.

9. Reenable autosynchronization.

   host1(config)#**no disable-autosync**

Upgrading from Release 5.1.1 or Lower-Numbered Releases

Release 5.1.1 or lower-numbered releases only support application images up to 172 MB. To install larger application images for Release 6.0.0 and higher-numbered releases, you must first install Release 5.1.2 (or the highest-numbered 5.x.x release). This enables the system to support application images greater than 172 MB. For example, you cannot go from Release 5.1.1 to Release 7.2.0 without first upgrading to Release 5.1.2. See Table 16.

Table 16: Release Compatibility

JUNOSe Release	Highest Release Able to Load	Cannot Load	Maximum Application Image
5.1.1 or lower-numbered release	5.3.5p0-2 or the highest-numbered 5.x.x release	6.x.x or higher-numbered release	~172 MB
5.1.2 or higher-numbered release	No limitation	Not applicable	~234 MB
7.2.0 or higher-numbered release	No limitation	Not applicable	~256 MB

Your software upgrades may be available remotely through Telnet or FTP, or may be delivered on a new NVS card. Depending on how you access the software updates, there are two different procedures to follow. See the appropriate section for instructions:

- *Upgrading Software Remotely Through Telnet or FTP*
- *Upgrading Software from an NVS Card*

Upgrading Software Remotely Through Telnet or FTP

Follow these steps to upgrade your system software remotely:

1. Copy the new release to your system (using Telnet of FTP).

NOTE: The release you are installing must be Release 5.1.2 or higher-numbered 5.x.x release.

2. Install and arm the release from the **config#** prompt using the normal upgrade procedures as described in this chapter.

3. Reload and configure the software.

After the system is configured with a 5.x.x release, newer releases are supported and can be installed.

Upgrading Software from an NVS Card

Follow these steps to upgrade your system software when the software is on an NVS card. The procedure you use depends on the number of SRP modules in the system.

Upgrading a System That Contains One SRP Module

If the system contains only one SRP module, you must power off the system before you upgrade the NVS card.

To upgrade the NVS card on a system that contains one SRP module:

1. Enter the **halt** command.
2. Connect your antistatic wrist strap to the ESD grounding jack on the router.
3. Power off the system.
4. Replace the NVS card on the SRP module.

NOTE: The release you are installing must be Release 5.1.2 or higher-numbered 5.x.x release.

5. Power on the system.

After the system is configured with a 5.x.x release, newer releases are supported and can be installed.

Upgrading a System That Contains Two SRP Modules

In a system that contains two SRP modules, you can upgrade the software without powering off the system.

To upgrade the software in a system that contains two SRP modules:

1. Connect your antistatic wrist strap to the ESD grounding jack on your router.
2. Turn off autosynchronization.

```
host1#enable
host1#configure
Configuring from terminal or file [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.

host1 (config)#disable-autosync
host1 (config)#exit
```

3. Halt the redundant SRP module.

```
host1#halt standby-srp

Remove the redundant SRP module from the chassis.
```

4. Replace the NVS card on this SRP module.

NOTE: The release you are installing must be Release 5.1.2 or higher-numbered 5.x.x release.

5. Reinsert the SRP module into the chassis.

6. Force the redundant SRP module to take over from the primary SRP module.

```
host1#srp switch
```

7. Turn on autosychronization.

```
host1#enable
host1#configure
Configuring from terminal or file [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.

host1 (config)#no disable-autosync
host1 (config)#exit
```

The software is updated on the other SRP module.

After the system is configured with a 5.x.x release, newer releases are supported and can be installed.

Downgrading JUNOSe Software

Downgrading JUNOSe software requires factory defaults installed on the router, and can cause NVS and configuration script incompatibilities.

CAUTION: We do not recommend that you attempt to downgrade JUNOSe software without the assistance of a Juniper Technical Assistance Center representative. Contact the Juniper Technical Assistance Center to obtain help.

Chapter 4

Configuring SNMP

This chapter provides information for configuring Simple Network Management Protocol (SNMP) on your E-series router.

This chapter contains the following sections:

- Overview on page 135
- Platform Considerations on page 144
- References on page 144
- Before You Configure SNMP on page 145
- SNMP Configuration Tasks on page 145
- Configuring Traps on page 153
- Configuring the SNMP Server Event Manager on page 162
- Collecting Bulk Statistics on page 178
- Using the Bulk Statistics Formatter on page 203
- Managing Virtual Routers on page 204
- Monitoring SNMP on page 204

Overview

SNMP is a protocol that manages network devices, such as your E-series router. The goal of SNMP is to simplify network management in two ways:

- By defining a single management protocol that can be used to manage any network device from any vendor.

  This feature reduces the complexity of the network management application because the application does not need to support a large number of proprietary management protocols for the mix of vendors' devices in the network.

- By defining a single, consistent representation of managed information that is commonly deployed in network devices.

  For example, SNMP uses a common form and semantics for interface statistics, a process that supports consistent interpretation and meaningful comparison.

SNMP is an application-level protocol that comprises the following three elements:

- An SNMP client (manager)
- An SNMP server (agent)
- A Management Information Base (MIB)

SNMP defines a client-server model in which a client (*manager*) obtains information from the server (*agent*) through two mechanisms:

- A request/response protocol by which the client configures and monitors the server. In this instance, the information is solicited.
- Asynchronous notifications (called *traps*) by which the server, on its own initiative, reports notable changes in the router's status to the client. In this instance, the information is unsolicited.

Terminology

Table 17 provides definitions for the basic SNMP terms.

Table 17: SNMP Terminology

Term	Meaning
agent	Also referred to as server; a managed device, such as a router, that collects and stores management information
client	Sometimes called a network management station (NMS) or simply a manager; a device that executes management applications that monitor and control network elements
community	A logical group of SNMP-managed devices and clients in the same administrative domain
entity	Refers to both a server and a client
event	A condition or state change that may cause the generation of a trap message
managed object	A characteristic of something that can be managed, such as a list of currently active TCP circuits in a device
group	SNMPv3 term; a set of users with the same access privileges to the router
MIB	Management Information Base; a collection of managed objects residing in a virtual information store
network element	Also known as a managed device; a hardware device, such as a PC or a router
notification	A message that indicates a status change (equivalent to a trap)
server	Also referred to as agent; a managed device, such as a router, that collects and stores management information

Table 17: SNMP Terminology (continued)

Term	Meaning
trap	Message sent by an SNMP server to a client to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached. Managed devices use traps to asynchronously report certain events to clients.
user	SNMPv3 term; an individual who accesses the router
view	SNMPv3 term; defines the management information available to the user: read, write, or notification

SNMP Features Supported

This SNMP implementation provides the following:

- Standard SNMP MIB support for services and interfaces as defined by the Internet Engineering Task Force (IETF)
- A set of AS number version 1 notated enterprise MIBs for all management functions not addressed by standard MIBs
- A multilingual SNMP server that supports SNMPv1, SNMPv2c, and SNMPv3 protocols
- Enhanced security and management features supported in SNMPv3
- Traps for alarm and state change events
- Bulk data collection and retrieval
- Management of virtual routers
- Secure audit logging for packet mirroring traps and Juni-PACKET-MIRROR MIB access

NOTE: You can disable the management interface through SNMP. But, if you disable the management interface, you can no longer access the router through SNMP.

NOTE: JUNOSe software supports SNMP packet mirroring traps; however, the packet mirroring-related SNMP commands, categories, and traps are visible in the CLI only to authorized users. See *JUNOSe Policy Management Configuration Guide, Chapter 10, Packet Mirroring Overview* for information about using SNMP with secure packet mirroring.

SNMP Client

The SNMP client runs on a network host and communicates with one or more SNMP servers on other network devices, such as routers, to configure and monitor the operation of those network devices.

SNMP Server

The SNMP server operates on a network device, such as a router, a switch, or a workstation. It responds to SNMP requests received from SNMP clients and generates *trap messages* to alert the client(s) about notable state changes in the network device.

The SNMP server implementation operates over UDP/IP only. It can receive requests directed to any IP address configured on the router. SNMP requests and responses are received or sent on UDP port 161. SNMP traps are sent from UDP port 162 by default or from a configurable port. For traps sent from UDP port 162, you can configure the destination UDP port for each recipient with the **snmp-server host** command.

SNMP MIBs

A MIB specifies the format of managed data for a device function. The goal of a MIB is to provide a common and consistent management representation for that function across networking devices.

Your router supports both standard and enterprise SNMP MIBs.

Standard SNMP MIBs

A standard MIB is defined by a body such as the IETF and fosters consistency of management data representation across many vendors' networking products.

Juniper Networks E-series Enterprise MIBs

An enterprise MIB is defined by a single vendor. In addition to providing consistency of management data representation across that vendor's product line, the enterprise MIB also accounts for proprietary functions and value-added features not addressed by standard MIBs.

For example, boot record extensions to the enterprise MIB enable configuration of the release (.rel) files for each router, slot, and subsystem. The extensions also enable booting through the factory defaults, the running configuration, or a configuration (.cnf) file.

Accessing Supported SNMP MIBs

For complete information about the SNMP MIBs supported by your router, see the *E-series System Software* CD, shipped with your router. In the MIBs folder you will find information about all supported standard and Juniper Networks E-series Enterprise (proprietary) MIBs.

SNMP Versions

This SNMP server implementation supports:

- SNMPv1 (defined in RFC 1157)
- SNMPv2c (Community-based SNMPv2, defined in RFC 1901 and RFC 3416)
- SNMPv3 (compliant with RFCs 3410–3418, STD 62)

The server encodes SNMP responses using the same SNMP version received in the corresponding request and encodes traps using the SNMP version configured for the trap recipient.

SNMPv2c supports the capabilities defined for SNMPv1 and provides greater power and flexibility through the addition of several features, including:

- More detailed error codes
- GetBulk operation for efficient retrieval of large amounts of data
- 64-bit counters

SNMPv3 is an extensible SNMP framework that supplements the SNMPv2c framework by supporting:

- Security for messages
- Explicit access control

Security Features

As users transfer more sensitive information, such as billing details, through the Internet, security becomes more critical for SNMP and other protocols. SNMPv3 provides the user-based security model (USM) to address authentication and data encryption.

Authentication provides the following benefits:

- Only authorized parties can communicate with each other. Consequently, a management station can interact with a device only if the administrator configured the device to allow the interaction.
- Messages are received promptly; users cannot save messages and replay them to alter content. This feature prevents users from sabotaging SNMP configurations and operations. For example, users can change configurations of network devices only if authorized to do so.

SNMPv3 authenticates users through the HMAC-MD5-96 or HMAC-SHA-96 protocols; CBC-DES is the encryption or privacy protocol. The SNMP agent recognizes up to 32 usernames that can have one of the following security levels:

- No authentication and no privacy (none)
- Authentication only (auth only)
- Authentication and privacy (priv)

In contrast, SNMPv1and SNMPv2c provide only password protection, through the community name and IP address. When an SNMP server receives a request, the server extracts the client's IP address and the community name. The SNMP community table is searched for a matching community. If a match is found, its access list, if nonzero, is used to validate the IP address. If the access list number is zero, the IP address is accepted. A nonmatching community or an invalid IP address causes an SNMP authentication error. Each entry in the community table identifies:

- An SNMP community name
- An SNMP view name
- A user's privilege level
  - Read-only (ro)
  - Read-write (rw)
  - Administrator (admin)
- An IP access list name

Management Features

Management features of SNMPv3 allow you to specify who will receive notifications and to define MIB views that users in different groups can access:

- Notification—Message that informs you of a status change; the equivalent of a trap in SNMPv1.
- View—Definition of the management information that is available: read, write, or notification. Predefined views are available for each group:
  - everything—Includes all MIBs associated with the router, except the packetMirror MIB
  - user—Includes all MIBs associated with the router, except the packetMirror MIB and standard and enterprise MIBs used to configure SNMP operation
  - nothing—Excludes all MIBs
  - mirrorAdmin—Includes the packetMirror MIB
- User—An individual who requires access to the router. The router may provide authentication and privacy for the user through SNMPv3. Each user is associated with a group.
- Group—A set of users with the same access privileges to the router. Three predefined groups are available: admin, public, and private. Table 18 shows the security levels and views associated with these groups.

Table 18: Relationship Among Groups, Security Levels, and Views

Group Name	Security Level	Read View	Write View	Notification/ Trap View
admin	authentication and privacy	everything	everything	everything
mirror	authentication and privacy	mirrorAdmin	mirrorAdmin	mirrorAdmin
public	none	user	nothing	nothing
private	authentication only	user	user	user

Virtual Routers

All SNMP-related CLI commands operate in the context of a virtual router, which means that you must configure users, traps, communities, and so on for *each* server. You must set the context using the **virtual-router** command and then configure SNMP.

The **show snmp** commands show only statistics and configuration information for the server/SNMP agent that corresponds to the current virtual router context.

The exceptions to this convention are the **snmp-server contact** and the **snmp-server location** commands. With these commands, single instances of the contact and the location are created regardless of the number of virtual routers.

Creating SNMP Proxy

Your JUNOSe software allows you to configure multiple virtual routers. Each virtual router has its own SNMP server. At router initialization, SNMP creates a server for each existing virtual router.

When router-specific data is required, the requestor can direct a request to a particular server for a virtual router through the base community string extension: for example, SNMP get public@megaRouter.

NOTE: In addition to the @ selector character, the system also supports the % selector character. For example, SNMP get public%megaRouter.

When any system server parses a request and detects an extended community string, it acts as proxy by forwarding the request to the server corresponding to the virtual router name in the extension (for example, *megaRouter)*. The target server then processes the request and generates a response, which is then returned to the proxy server and subsequently transmitted to the requester.

The JUNOSe implementation of SNMPv3 communicates with virtual routers by assigning each proxy agent an SNMP engine ID. This difference is unimportant to users of the CLI. However, if you use other SNMPv3 applications to manage the router, refer to the following section.

Disabling and Reenabling SNMP Proxy

The ability to proxy SNMP from a virtual router (VR) is enabled by default whenever you create a virtual router agent. However, you can disable or reenable the proxy feature on each virtual router agent to address any network security issues. To disable proxy on an agent (router), you must use SNMP or the CLI **snmp-server proxy disable** command.

NOTE: Disabling the proxy function on a particular virtual router disables the use of proxy through that virtual router. You can, however, use the proxy function to access a proxy-disabled virtual router through another virtual router that does have the proxy function enabled.

Communicating with the SNMP Engine

The SNMP engine performs the following tasks for SNMPv3:

- Sends and receives messages.
- Prepares messages and extracts data from messages.
- Authenticates, encrypts, and decrypts messages.
- Determines whether access to a managed task is allowed.

Each SNMP engine has an SnmpEngine ID, a hexadecimal number 15 octets long. Table 19 shows the structure of the SnmpEngine ID.

Table 19: SnmpEngineID Structure Object

Octet Assignment	Description
1 – 4	E-series router SNMP management private enterprise number
5	Indicates that octets 6–15 contain information determined by the E-series router
6 – 11	The MAC address for the device
12 – 15	The 32-bit (4 octet) router index (or routerUID)

Request protocol data units (PDUs) for the SNMP engine must contain the corresponding contextEngine ID and contextName for the SNMP engine. When the system receives a PDU, it examines the contextEngine ID and contextName, and forwards the request to the corresponding virtual router.

- The contextEngine ID is the same as the SnmpEngine ID.
- The contextName is an internally derived ASCII string associated with the router. It has the format *routerN*, where N is a number (with no leading zeros) in the range 1–16777215, corresponding to the least significant 24 bits of the 32-bit router index (or router UID). You can obtain the contextName for a specific router through the Juniper-ROUTER-MIB from the juniRouterContextName object in the juniRouterTable, which is indexed by the 32-bit router index (juniRouterIndex).

The following table shows examples of the E-series router SNMP engine objects that are associated with the default virtual router.

Object	Value
SnmpEngineID	0x80:00:13:0a:05:00:90:1a:00:04:6c:80:00:00:01
contextEngineID	0x80:00:13:0a:05:00:90:1a:00:04:6c:80:00:00:01
contextName	router1

SNMP Attributes

The software automatically maps predefined SNMPv1/v2c attributes to predefined SNMPv3 attributes, as shown in Table 20.

Table 20: Relationship Between SNMPv1/v2c and SNMPv3 Attributes

Attribute	SNMPv1/v2C Value	SNMPv3 Value
Community	admin	admin
View		everything
Privilege	rw	rw
Community	public	public
View		user
Privilege	ro	ro
Community	private	private
View		user
Privilege	rw	rw

SNMP Operations

SNMP has the five operations defined in Table 21.

Table 21: SNMP Operations

SNMP Operation	Definition
Get	Allows the client to retrieve an object instance from the server.
GetNext	Allows the client to retrieve the next object instance from a table or list within a server.
GetBulk	Makes it easier to acquire large amounts of related information without initiating repeated GetNext operations. GetBulk is not available in SNMPv1.
Set	Allows the client to set values for the objects managed by the server.
Notification	Used by the server to asynchronously inform the client of some event. (Called a trap in SNMPv1.)

SNMP PDU Types

SNMP offers the six types of PDUs defined in Table 22.

Table 22: SNMP PDU Types

SNMP PDU Type	Definition
Get Bulk	Transmitted by the client to the server to obtain the identifiers and the values of a group or collection of variables rather than one variable at a time. GetBulk is not available in SNMPv1.
Get Next Request	Transmitted by the client to the server to obtain the identifiers and the values of variables located *after* the designated variables.
Get Request	Transmitted by the client to the server to obtain the values of designated variables.
Get Response	Transmitted by the server to the client in response to a Get Request, a Get Next Request, or a Set Request PDU.
Set Request	Transmitted by the client to the server to modify the values of designated variables.
Notification	Transmitted by the server, on its own initiative, to inform the client of a special event noted on a network device. (Called a trap in SNMPv1.)

Platform Considerations

SNMP is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about SNMP, consult the following resources:

- RFC 1157—A Simple Network Management Protocol (SNMP) (May 1990)
- RFC 1901—Introduction to Community-based SNMPv2 (January 1996)
- RFC 2790—Host Resources MIB (March 2000)
- RFC 2864—The Inverted Stack Table Extension to the Interfaces Group MIB (June 2000)
- RFC 2493—Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals (January 1999)
- RFC 3014—Notification Log MIB (November 2000)

- RFC 3410—Introduction and Applicability Statements for Internet Standard Management Framework (December 2002)
- RFC 3411—An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (December 2002)
- RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (December 2002)
- RFC 3413—Simple Network Management Protocol (SNMP) Applications (December 2002)
- RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (December 2002)
- RFC 3415—View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) (December 2002)
- RFC 3416—Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) (December 2002)

Before You Configure SNMP

Before you configure SNMP, make sure that at least one IP address is configured on your router. See *ERX Hardware Guide, Chapter 7, Accessing ERX Routers* or *E120 and E320 Hardware Guide, Chapter 7, Accessing E-series Routers*.

Also make sure that you have the necessary configuration information for:

- Communities and their assigned privileges
- IP addresses of SNMP clients and trap recipients
- SNMPv3 users

SNMP Configuration Tasks

To configure the SNMP server:

1. Enable the SNMP server.

   host1(config)#**snmp-server**

2. Configure at least one authorized SNMP community (SNMPv1/v2c) or user (SNMPv3), which provides SNMP client access.

   host1(config)#**snmp-server community boston view everything rw**
   host1(config)#**snmp-server user fred group private auth sha fred-password priv des password**

3. (Optional) Set the server parameters—contact name and server location.

   host1(config)#**snmp-server contact Bob Smith**
   host1(config)#**snmp-server location 3rdfloor**

4. (Optional) Reconfigure the maximum SNMP packet size.

   host1(config)#**snmp-server packetsize 1000**

5. (Optional) Configure memory warning parameters.

   host1(config)#**memory warning 80 70**

6. (Optional) Configure the method the router uses to encode the ifDescr and ifName objects.

   host1(config)#**snmp interfaces description-format common**

7. (Optional) Manage the interface sublayers (compress interfaces and control interface numbering).

   host1(config)#**snmp-server interfaces compress atmAal5**
   host1(config)#**snmp-server interface compress-restriction ifadminstatusdown**
   host1(config)#**snmp interfaces rfc1213 55000 100000**

8. (Optional) Configure the dynamic group parameters.

   host1(config)#**snmp-server group grp1authpriv usm priv read grp1read write grp1write notify grp1notify**

9. (Optional) Configure the dynamic view parameters.

   host1(config)#**snmp-server view view1 1.3.6.1 included non-volatile**

You can also set up SNMP traps and set up the router to collect bulk statistics. See *Configuring Traps* on page 153 and *Collecting Bulk Statistics* on page 178.

Enabling SNMP

To enable the SNMP server, use the following command.

snmp-server

- Use to enable SNMP server operation.
- Example

  host1(config)#**snmp-server**

- Use the **no** version to disable the SNMP server operation.

Configuring SNMP v1/v2c Community

For SNMPv1/v2c, access to an SNMP server by an SNMP client is governed by a proprietary SNMP community table that identifies those communities that have read-only, read-write, or administrative permission to the SNMP MIB stored on a particular server.

When an SNMP server receives a request, the server extracts the client's IP address and the community name. The SNMP community table is searched for a matching community. If a match is found, its access list name is used to validate the IP address. If the access list name is null, the IP address is accepted. A nonmatching community or an invalid IP address results in an SNMP authentication error.

Each entry in the community table identifies:

- An SNMP community name
- A user's privilege level
- An IP access list

Community Name

The community name acts as a password and is used to authenticate messages sent between an SNMP client and a router containing an SNMP server. The community name is sent in every packet between the client and the server.

Privilege Levels

SNMP has three privilege levels:

- Read-only—Read-only access to the entire MIB except for SNMP configuration objects
- Read-write—Read-write access to the entire MIB except for SNMP configuration objects
- Admin—Read-write access to the entire MIB

IP Access List

The IP access list identifies those IP addresses of SNMP clients permitted to use a given SNMP community.

snmp-server community

- Use to configure an authorized SNMP community for access to the SNMP MIBs and to associate SNMPv1/v2c communities with SNMP MIB views.
- The community name serves as a password and permits access to an SNMP server. The name can be up to 31 characters, and it must be enclosed in quotation marks.
- The maximum number of communities in each virtual router is 32.
- By default, an SNMP community permits only read-only access.
- The view name allows configuration with available dynamic views.

- Example

  host1(config)#**snmp-server community “boston” view view1 rw**

- Use the **no** version to delete a community from the SNMP community table.

Configuring SNMPv3 Users

To configure SNMPv3 users, use the following command.

snmp-server user

- Use to create and modify SNMPv3 users.
- Example

  host1(config)#**snmp-server user fred auth sha fred-password priv des password group user**

- Use the **no** version to delete users.

Configuring SNMP Dynamic Groups and Views

With dynamic configurable views and groups you can fine-tune application features to a specific group, You can have 32 view entries (with distinct names) per virtual router. Because there is no limit to the number of entries within a distinct view name, you can configure complex views. You can also have 32 access entries (with distinct names) per virtual router. All views are on a per-virtual-router basis; although static views are on a per-virtual-router basis, they cannot be altered. If you modify a view, the system deletes the original entry and creates the new view. Therefore, if the new view fails, the original view is no longer available.

SNMP v3 configurations are allowed only at the maximum CLI privilege level (15).

snmp-server group

- Use to dynamically configure server groups. You must access the CLI at privilege level 15 to view or use this command.
- Example

  host1(config-profile)#**snmp-server group grp1authpriv usm priv read grp1read write grp1write notify grp1notify**

- Use the **no** version to remove the dynamically created group.

snmp-server view

- Use to dynamically configure an SNMP server view. You must access the CLI at privilege level 15 to view or use this command.
- Example

  host1(config)#**snmp-server view view1 1.3.6.1 included non-volatile**

- Use the **no** version to remove the dynamically created view.

Setting Server Parameters

Setting the server's contact person and location provides helpful identifiers for the SNMP server. These identifiers are arbitrary and do not affect the server's function, but they are useful to have.

snmp-server contact
snmp-server location

- Use these commands to configure the SNMP server's contact person and the server's location.
- The contact is the person who manages the server.
- The location is the server's physical location.
- Each of these parameters can be up to 64 characters.
- Example

  host1(config)#**snmp-server contact Bob Smith**
  host1(config)#**snmp-server location 3rdfloor**

- Use the **no** version of these commands to clear the contact or location identifier from the SNMP configuration.

Configuring SNMP Packet Size

The SNMP server must support a PDU with an upper limit of 484 bytes or greater. There is no need to coordinate the maximum packet size across the entire network. Many requests and responses tend to be smaller than the maximum value.

snmp-server packetsize

- Use to set the SNMP server's maximum packet size.
- Increase this value to improve the efficiency of the GetBulk operation.
- Example

  host1(config)#**snmp-server packetsize 1000**

- Use the **no** version to set the SNMP packet size to the default maximum size, 1500 bytes.

Configuring Memory Warning

You can set up the router to send memory warning messages when memory utilization reaches a specified value.

memory

- Use to configure memory warning parameters. You set a high memory utilization value and an abated memory utilization value. When the system reaches the high utilization value, it sends warning messages. When memory usage falls to the abated utilization value, the system stops sending warning messages.

- Example

  host1(config)#**memory warning 80 70**

- Use the **no** version to return to the default values, 85 for high utilization and 75 for abated memory utilization.

Configuring Encoding Method

You can control how the router encodes the ifDescr and ifName objects in the SNMP agent's interface table and in the bulkstats application.

There are two choices of encoding schemes: an E-series router proprietary method and a conventional industry method.

- The proprietary method identifies each interface sublayer with its type.
- The industry method bases the type information for each interface sublayer on the lowest layer 1 or layer 2 interface type.

For example a PPP interface configured on top of an ATM interfaces is:

- PPP3/0.1—Proprietary method
- ATM3/0.1—Industry method

snmp-server interfaces description-format

- Use to set the encoding scheme of the ifDescr and ifName objects. Include one of the following keywords:
  - **common**—Sets the encoding scheme to the conventional industry method and provides compatibility with software that uses the industry encoding scheme.
  - **legacy**—Sets the encoding scheme for legacy E-series routers.
  - **proprietary—**Sets the encoding scheme to the E-series router proprietary method.
- Example

  host1(config)#**snmp-server interfaces description-format common**

- Use the **no** version to return to the default, the legacy encoding scheme.

Managing Interface Sublayers

You can set up the SNMP agent to compress the number of interface instances in the standard interface and stack tables. You can also control the interface numbering method used in the interface tables.

Compressing Interfaces

You can compress interfaces by interface type and by the administrative status of the interface. Compressing interfaces removes them from the ifTable, the ifStackTable, and the ipAddrTable, which increases table retrieval performance. For example, if you want statistics kept only on IP interfaces, then you can compress all interfaces except IP; subsequently, only IP interfaces will appear in the ifTable, the ifStackTable, and the ipAddrTable.

To compress interfaces that have an administrative status of down, use the **snmp-server interfaces compress-restriction** command.

To compress interfaces according to type, use the **snmp-server interfaces compress** command. To see the list of interfaces that you can remove, use the CLI help:

```
host1(config)#snmp-server interfaces compress ?
  Atm           Atm interface layer
  Atm1483       Atm1483 interface layer
  AtmAal5       AtmAal5 interface layer
  . . .
  SonetVT       SonetVT interface layer
  VlanMajor     VlanMajor interface layer
  VlanSub       VlanSub interface layer <cr>
```

If you enter the **snmp-server interfaces compress** command without keywords, the following interface types are removed from the interface tables:

- ip
- ppp
- ethernetSubinterface
- hdlc
- ipLoopback
- ipVirtual
- pppLinkInterface
- pppoeInterface
- slepInterface/ciscoHdlc

snmp-server interfaces compress

- Use to remove interface sublayers from the ifTable, the ifStackTable, and the ipAddrTable.
- Example

  host1(config)#**snmp-server interfaces compress atmAal5**

- Use the **no** version to add interface sublayers to the ifTable, the ifStackTable, and the ipAddrTable.

snmp-server interfaces compress-restriction

- Use to exclude interfaces from the ifTable, the ifStackTable, and the ipAddrTable if the administrative status of the interface is down.
- Example

  host1(config)#**snmp-server interfaces compress-restriction ifadminstatusdown**

- Use the **no** version to remove the restriction and allow interfaces with an administrative status of down in the ifTable, the ifStackTable, and the ipAddrTable.

Controlling Interface Numbering

Each interface in the ifTable is assigned an ifIndex number. RFC 1213 required that ifIndexes use contiguous integers and that the ifIndex be less than the value of the total number of interfaces (ifNumber). More recent RFCs—1573, 2232, and 2863—removed these restrictions to accommodate interface sublayers. The E-series router implementation of SNMP derives index numbers in 32-bit values that are unique on a given router. This numbering scheme can result in large gaps in the ifIndex.

Legacy network management software that was designed to work with RFC 1213 implementations expects contiguous integers and can fail when the software encounters large gaps in the ifIndex.

By default, the router uses a numbering scheme based on RFC 2863. For compatibility with RFC 1213, you can set up the router to use contiguous numbers and to limit the values of the ifIndex and the ifNumber.

snmp-server interfaces rfc1213

- Use to set up the interface numbering method in the IfTable to use contiguous integers, which provides compatibility with versions of SNMP that are based on RFC 1213.
- The *maxIfIndex* option sets the maximum value of the ifIndex field that the system will allocate.
- The *maxIfNumber* option sets the maximum number of interfaces allowed in the interface tables.

CAUTION: Reducing the value of the maxIfIndex and/or maxIfNumber causes the router to automatically reboot to factory default settings.

- When the IfIndex and IfNumber maximums are reached, the system logs the event and ignores the creation of additional interfaces, which means that new interfaces are not visible in the interface table.
- Example

  host1(config)#**snmp-server interfaces rfc1213 55000 100000**
  WARNING: Execution of this command will cause all configuration settings to revert to factory defaults upon the next system reboot.
  Proceed with 'snmp interfaces rfc1213'? [confirm]

- Use the **no** version to return to the default method of interface numbering.

Monitoring Interface Tables

Use the following command to view the configuration of your interface tables.

show snmp group

- Use to display a list of interface types that are compressed in the interface tables and the interface numbering method configured on the router.
- Field descriptions
  - Compressed(Removed) Interface Types—List of interface types that are removed from the ifTable and ifStackTable
  - Armed Interface Numbering Mode—Interface numbering method configured on the router: RFC1213, RFC2863
  - maxIfIndex—Maximum value that the system will allocate to the ifIndex field
  - maxIfNumber—Maximum number of interfaces allowed in the ifTable
  - Interface Description Setting—Method used to encode the ifDescr and ifName objects: common, legacy, proprietary
- Example

```
host1#show snmp interfaces
Compressed(Removed) Interface Types:
HDLC, FT1, ATM, ATM1483
Armed Interface Numbering Mode:
RFC1213, maxIfIndex=65535, maxIfNumber=65535
Interface Description Setting: proprietary
```

Configuring Traps

This section provides information for:

- Enabling trap generation
- Setting up filtering of traps by severity
- Configuring trap destinations
- Setting a source address for traps
- Enabling link-status traps
- Specifying an egress point for traps
- Configuring trap queues
- Configuring trap notification logs
- Recovering lost traps

The system generates SNMP traps according to operating specifications defined in supported MIBs.

IP Hosts

Traps are sent to IP hosts. The IP hosts are configured in a proprietary trap host table maintained by the router (the server). Each entry in the table contains:

- IP address of the trap destination
- Community name (v1 or v2c) or username (v3) to send in the trap message
- SNMP format (v1 or v2) of the notification (trap) PDU to use for that destination
- Types of traps enabled to be sent to that destination
- Trap filters configured for the destination

The maximum number of entries in the SNMP trap host table in each virtual router is eight.

Trap Categories

The router supports the following trap categories:

- addrPool—Local address pool traps
- atmPing—E-series router proprietary ATM ping traps
- bfdmib—BFD MIB traps
- bgp—BGP state change traps
- bulkstats—Bulk statistics file full and nearly full traps
- cliSecurityAlert—Security alert traps
- dhcp—Dynamic Host Configuration Protocol traps
- dismanEvent—Distributed management (disman) event traps
- dosProtectionPlatform—DoS protection platform traps
- dvmrp—Distance Vector Multicast Routing Protocol traps
- dvmrpProp—E-series router proprietary DVMRP traps
- environment—Power, temperature, fan, and memory utilization traps
- fileXfer—File transfer status change traps
- haRedundancy—High availability and redundancy traps
- inventory—System inventory and status traps
- ip—Internet Protocol traps
- ldp—LDP traps

- link—SNMP linkUp and linkDown traps
- log—System log capacity traps
- mobileIpv4—Mobile IPv4 traps
- mplste—Mplste traps
- mrouter—Mrouter traps
- ntp—E-series router proprietary traps
- ospf—Open Shortest Path First traps
- packetMirror—Packet mirroring traps; packet mirroring–related SNMP categories and traps are visible only to authorized users. See *JUNOSe Policy Management Configuration Guide, Chapter 10, Packet Mirroring Overview* for information about using secure packet mirroring traps.
- pim—Protocol Independent Multicast traps
- ping—Ping operation traps in disman remops (remote operations) MIB
- radius—RADIUS servers fail to respond to accounting and authentication requests traps, or servers return to active service traps
- routeTable—Maximum route limit and warning threshold traps; when this trap is generated, the actual value of the exceeded warning threshold is displayed.
- snmp—SNMP coldStart, warmStart, authenticationFailure; the trap option. The **snmp-server enable traps snmp authentication** command allows customized treatment for SNMP authentication failure traps.
- sonet—SONET traps
- traceroute—Traceroute operation traps (in disman remops MIB)
- trapFilters—Global filters for SNMP trap recipients
- vrrp—Virtual Router Redundancy Protocol traps

To enable global trap categories, use the **snmp-server enable traps** command. To enable trap categories for a specific host, use the **snmp-server host** command.

Trap Severity Levels

The router provides a method of filtering traps according to severity. Table 23 describes the supported severity levels.

Table 23: Trap Severity Descriptions

Severity Number	Severity Name	System Response
0	Emergency	System unusable
1	Alert	Immediate action needed
2	Critical	Critical conditions exist
3	Error	Error conditions exist
4	Warning	Warning conditions exist
5	Notice	Normal but significant conditions exist
6	Informational	Informational messages
7	Debug	Debug messages

You can set up a global filter to filter all traps and/or set up a filter for each host. Trap filters work as follows:

1. An event is posted to the SNMP agent.
2. The system determines whether the corresponding trap category is globally enabled and whether the trap meets the minimum global severity level.
   a. If the trap does not meet these criteria, the system discards the trap.
   b. If the trap does meet these criteria, the trap is handed to the trap host processor.
3. The trap host processor determines whether the trap category is enabled on the host and whether the trap meets the minimum severity level set for the host.
   a. If the trap does not meet these criteria, the system discards the trap.
   b. If the trap does meet these criteria, the trap is sent to the trap recipient.

To set up global severity filters, use the **snmp-server enable traps** command. To set up a severity filter for a specific host, use the **snmp-server host** command.

snmp-server enable traps

- Use to enable and configure SNMP trap generation on a global basis.
- Traps are unsolicited messages sent from an SNMP server (agent) to an SNMP client (manager).
- You can enable the traps listed in *Trap Categories* on page 154.
- You can filter traps according to the trap severity levels described in Table 23 on page 156.

- If you do not specify a trap option, all options are enabled or disabled for the trap type.
- Example

  host1(config)#**snmp-server enable traps atmPing trapfilters critical**

- Use the **no** version to disable SNMP trap generation.

snmp-server host

- Use to configure an SNMP trap host to refine the type and severity to traps that the host receives.
- A trap destination is the IP address of a client (network management station) that receives the SNMP traps.
- You can configure up to eight trap hosts on each virtual router.
- You can enable the traps listed in *Trap Categories* on page 154.
- You can filter traps according to the trap severity levels described in Table 23 on page 156.
- Example

  host1(config)# **snmp-server host 126.197.10.5 version 2c westford udp-port 162 snmp link trapfilters alert**

- Use the **no** version to remove the specified host from the list of recipients.

snmp-server trap-source

- Use to specify the interface whose IP address is used as the source address for all SNMP traps.

NOTE: When there are multiple IP addresses configured on the IP interface that is chosen as the SNMP trap source, the SNMP agent automatically uses the primary IP address of the interface as the SNMP source address on SNMP traps.

- Example

  host1(config)#**snmp-server trap-source fastethernet 0/0**

- Use the **no** version to remove the interface from the trap configuration.

snmp trap ip link-status

- Use to enable link-status traps on an IP interface.
- Example

  host1(config-if)#**snmp trap ip link-status**

- Use the **no** version to disable link-status traps on an IP interface.

snmp trap link-status

- Use to configure the SNMP link-status traps on a particular interface.
- A *link-up* trap recognizes that a previously inactive link in the network has come up.
- A *link-down* trap recognizes a failure in one of the communication links represented in the server's configuration.
- Example

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

- Use the **no** version to disable these traps for the interface.

NOTE: This command operates in Controller Configuration mode. It is supported only by the DS3, DS1, and FT1 interface layers.

traps

- Use to specify traps for OSPF.
- Example

  host1(config-router-rn)#**traps all**

- Use the **no** version to delete the specified trap, group of traps, or all traps.

NOTE: For additional information about configuring OSPF-specific traps, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 5, Configuring OSPF*.

Specifying an Egress Point for SNMP Traps

You can enable SNMP trap proxy, which allows you to specify a single SNMP agent as the egress point for SNMP traps from all other virtual routers. This feature removes the need to configure a network path from each virtual router to a single trap collector.

You can enable SNMP trap proxy from either SNMP or the CLI. Only one SNMP trap proxy can exist for a physical router.

The SNMP trap proxy does not forward global traps that it receives from other virtual routers. The corresponding SNMP agent handles global traps locally and does not forward them to the SNMP trap proxy.

To configure the SNMP trap proxy:

1. Access the virtual router context.
2. Enable or disable the SNMP trap proxy.

snmp-server trap-proxy

- Use to enable or disable the SNMP trap proxy.
- Example

  host1(config)#**snmp-server trap-proxy enable**

- Use the **no** version to disable the SNMP trap proxy.

Configuring Trap Queues

You can control the SNMP trap egress rate, specify the method of handling a full queue, and specify the maximum number of traps kept in the queue.

snmp-server host

- Use to control the SNMP trap egress rate for the host that is receiving SNMP traps. Use one or more of the following keywords:
  - **drainRate**—Specifies the maximum number of traps per second sent to the host
  - **full**—Specifies the method for handling the queue full condition
  - **size**—Specifies the maximum number of traps kept in the queue
- Example

  host1(config)#**snmp-server host 10.10.10.10 trapqueue drainrate 600 full droplastin size 50**

- Use the **no** version to remove the SNMP host.

Configuring Trap Notification Logs

SNMP uses the User Datagram Protocol (UDP) to send traps. Because UDP does not guarantee delivery or provide flow control, some traps can be lost in transit to a destination address. The Notification Log MIB provides flow control support for UDP datagrams.

You should set up your management applications to periodically request the recorded traps to ensure that the host is up and the management applications have received all the generated traps.

To identify the location of traps logged in the notification log, the system assigns a consecutive index number to each SNMP trap message transmitted from the E-series router. Clients can use the index to detect missing traps.

To configure trap notification logs:

1. Configure the notification log.

   host1(config)**snmp-server notificationlog log 10.10.4.4 adminStatus includeVarbinds**

2. (Optional) Specify when the notification log ages out.

   host1(config)#**snmp-server notificationlog ageout 5**

3. (Optional) Specify the maximum number of entries kept in the notification log.

   host1(config)#**snmp-server notificationlog entrylimit 210**

4. (Optional) Enable the snmpTrap log to severity level info.

   host1(config)#**log severity info snmpTrap**

NOTE: Enabling the snmpTrap log provides the same information in the router log as appears in the snmp-server notification log. However, long trap strings may appear truncated.

log severity

- Use to set the severity level for a selected category or for systemwide logs.

NOTE: For more information about this command, see the *JUNOSe System Event Logging Reference Guide, Chapter 1,* .

- Example

  host1(config)#**log severity info snmptrap**

- Use the **no** version to return to the default severity value (error) for the selected category. To return all logs to their default severity setting, include an * (asterisk) with the **no** version.

snmp-server notificationLog ageOut

- Use to set the ageout for traps in the notification log tables. The range is 0–214748364 minutes.
- Example

  host1(config)#**snmp-server notificationLog ageout 5**

- Use the **no** version to return the ageout limit to the default value, 1440 minutes.

snmp-server notificationLog entryLimit

- Use to set the maximum number of notifications kept in all notification log tables.
- The range is 1–500, which means that you can allocate up to 500 notifications across all virtual routers on the router. As you allocate the entry limits for virtual routers, the available range changes to reflect the number of notifications that you have allocated.
- Example

  host1(config)#**snmp-server notificationLog entrylimit 210**

- Use the **no** version to return the limit to the default value, 500.

snmp-server notificationLog log

- Use to configure SNMP notification log tables.
- Use the **adminStatus** keyword to enable administrative status.
- Use the **includeVarbinds** keyword to include log names and log indexes in the trap's variable bindings.
- Example

  host1(config)**snmp-server notificationLog log 10.10.4.4 adminStatus includeVarbinds**

- Use the **no** version to remove the notification log configuration.

Recovering Lost Traps

SNMP traps can be lost during startup of the E-series router for one of the following reasons:

1. The SNMP agent begins sending SNMP traps to the host before the line module is initialized.

2. If the SNMP proxy virtual router is initialized after other virtual routers, traps generated by the other virtual routers and sent to the proxy router are lost.

To recover SNMP traps that are lost during system startup, the SNMP agent pings the configured trap host to identify that there is a communication path between E-series router and host. On successful ping acknowledgment, the lost traps are reconstructed for each virtual router. In the case of scenario 1, the reconstructed traps are sent to the proxy virtual router to be routed to the appropriate hosts. In the case of scenario 2, the traps are sent directly to the appropriate hosts.

You can configure the ping timeout window with the **snmp-server host** command. The following are guidelines for setting the maximum ping window:

- If you are losing traps because of scenario 1, base the maximum ping window time on the estimated time that it takes to establish connectivity in a particular network. (For some configurations it can take more than 30 minutes to establish connectivity.)

- If you are losing traps because of scenario 2, we recommend that you use the default value for the maximum ping window time, which is one minute.

snmp-server host

- Use to set the ping timeout for the host that is receiving SNMP traps.
- Use the **pingtimeout** keyword to set the ping timeout window; the range is 1–90 minutes.
- Example

  host1(config)#**snmp-server host 10.10.4.4 pingtimeout 2**

- Use the **no** version to remove the SNMP host.

Configuring the SNMP Server Event Manager

The SNMP server event manager works in conjunction with the Event MIB (RFC 2981). The purpose of this application is to allow many management functions (for example, fault detection, configuration management, accounting management, and performance management). These functions are traditionally performed by the network management station. However, by using the SNMP server event manager, you can distribute some of these functions to E-series routers and automate them.

Event MIB Purpose

The rapid growth of networks has made it impractical to directly manage networks from a single network management station (NMS). This brought about a need for a model that both automated and distributed event management. The goal was to allow devices to monitor themselves and other devices, and to take action under certain conditions.

The Event MIB (RFC 2981) defines a method for creating trigger conditions, testing those conditions, and determining which action to take when a trigger meets those conditions.

The Event MIB allows you to define test conditions for object integers that are accessible in the agent, making it possible to monitor any aspect of a device without defining specific notifications and complicating the agent definition. In this model, because devices have the ability to monitor themselves or other devices, the processing is distributed throughout the network. Also, sending the information only to the NMS that uses an event model reduces both network overhead and processing drain on the NMS.

Event MIB Structure

The Event MIB has three major parts: the trigger table, the objects table, and the event table. These tables also contain subordinate MIB tables that contain more detailed information about the trigger tests.

Trigger Table

The trigger table (mteTriggerTable) lists any currently-defined trigger conditions. Triggers fall into three categories—existence, Boolean, and threshold.

An *existence* trigger tests for the existence of a MIB object instance; you can specify that the trigger occur by either the appearance, disappearance, or change in value of a MIB instance.

A *Boolean* trigger tests whether the value of a MIB object (base syntax integer) is equal, unequal, greater than, less than, less than or equal to, or greater than or equal to some defined value.

A *threshold* trigger verifies a MIB object (base syntax integer) in relation to either a rising threshold value, falling threshold value, or both.

You can configure both Boolean and threshold tests to trigger on an *absolute value* or a *delta value* over a determined polling interval.

Subordinate MIB tables exist within the trigger section of each type of trigger test. In other words, each type of trigger (existence, threshold, and Boolean) contains a table that stores added information about that type of trigger test.

For example, a trigger entry of a specific type of test in the mteTriggerTable creates a linked entry in the appropriate subtable. In turn, this subtable contains more specific information about the specific test.

A *delta* table also exists within the trigger tables. This table stores information about any delta values based on any Boolean and threshold triggers. The delta table stores a MIB object that indicates whether any discontinuities occurred for any delta trigger (for example, a router reset).

NOTE: When determining discontinuity, the MIB object must be a time-based counter or number. When a polling interval expires and the event agent (router) needs to perform a delta calculation, it first checks the discontinuity MIB object for that trigger. If a discontinuity occurs, the agent does not perform the test for that trigger until the next polling interval.

Objects Table

The objects table (mteObjectsTable) defines objects that you want to add to event messages. In other words, you can create a list of user-specified objects and bind them to a trigger event. This can provide a snapshot of other values on a router when the trigger occurs. You can bind objects to a specific trigger, a type of test (for example, existence or Boolean tests), or a type of event (for example, rising or falling events).

NOTE: This release does not support the objects table.

Event Table

The event table (mteEventTable) defines what action you want the device to take when a trigger occurs. This action can be in the form of a notification, setting a specified MIB object, or both. The results of these actions are controlled within two subordinate MIB tables—notification and set.

Notifications (mteNotifications), or traps, define what the router sends when an event occurs. These traps include the following:

- When a Boolean or existence trigger occurs, the router sends an mteTriggerFired trap.
- When a rising threshold trigger occurs, the router sends an mteTriggerRising trap.
- When a falling threshold trigger occurs, the router sends an mteTriggerFalling trap.

- If a trigger fails to complete a test for any reason, the router sends a global mteTriggerFailure trap.
- If an event fails to set, the router sends an mteEventSetFailure trap.

Sets define certain modifications to other MIB objects based on a particular event.

Configuration Tasks

To configure the SNMP server event manager:

1. Access the SNMP server management event application.

   host1(config)#**snmp-server management-event**
   host1(config-mgmtevent)#

NOTE: You must create a management event instance for each virtual router.

2. (Optional) Specify the maximum number of trigger entries that you want the virtual router to support.

   host1(config-mgmtevent)#**resource 275**

3. Create an event for each trap notification (mteTriggerFailure, mteTriggerFalling, or mteTriggerRising) that you want to use by specifying an event owner and event name.

   host1(config-mgmtevent)#**event sysadmin failuretrigger**
   host1(config-mgmtevent-event)#**exit**
   host1(config-mgmtevent)#**event sysadmin fallingtrigger**
   host1(config-mgmtevent-event)#**exit**
   host1(config-mgmtevent)#**event sysadmin risingtrigger**
   host1(config-mgmtevent-event)#**exit**

NOTE: You must create a separate event for each trap notification that you want to use. However, you can specify the trap notification and enable the trap before exiting the event context.

4. Define each event to send a trap notification (mteTriggerFailure, mteTriggerFalling, and mteTriggerRising).

   host1(config-mgmtevent)#**event sysadmin failuretrigger**
   host1(config-mgmtevent-event)#**notification id mteTriggerFailure**
   host1(config-mgmtevent-event)#**exit**
   host1(config-mgmtevent)#**event sysadmin fallingtrigger**
   host1(config-mgmtevent-event)#**notification id mteTriggerFalling**
   host1(config-mgmtevent-event)#**exit**
   host1(config-mgmtevent)#**event sysadmin risingtrigger**
   host1(config-mgmtevent-event)#**notification id mteTriggerRising**
   host1(config-mgmtevent-event)#**exit**

NOTE: The mteTriggerFailure notification is a global value. Once you create a failure event notification, it is automatically bound to every trigger with the same owner. If a failure occurs, and the trigger owner and the event owner are the same, the router sends the trap.

5. Enable the event, and exit the event configuration level.

```
host1(config-mgmtevent)#event sysadmin failuretrigger
host1(config-mgmtevent-event)#enable
host1(config-mgmtevent-event)#exit
host1(config-mgmtevent)#event sysadmin fallingtrigger
host1(config-mgmtevent-event)#enable
host1(config-mgmtevent-event)#exit
host1(config-mgmtevent)#event sysadmin risingtrigger
host1(config-mgmtevent-event)#enable
host1(config-mgmtevent-event)#exit
host1(config-mgmtevent)#
```

NOTE: Once enabled, you cannot edit an event or trigger configuration. To change an enabled event or trigger, you must delete it and re-create it.

6. Define the trigger that you want to use for an event by specifying a trigger owner and trigger name.

```
host1(config-mgmtevent)#trigger george trigger1
host1(config-mgmtevent-trigger)#
```

7. Specify a MIB object to sample.

```
host1(config-mgmtevent-trigger)#sample value-id 1.3.6.1.2.1.60.1.2.1.1.7
```

8. Specify the frequency (in seconds) at which you want the sampling to occur.

```
host1(config-mgmtevent-trigger)#frequency 100
```

NOTE: Unless you specify that you want to perform delta sampling, the values are absolute.

9. (Optional) Specify that you want to perform delta sampling on the sample value ID.

```
host1(config-mgmtevent-trigger)#delta-sampling
```

- (Optional) Enter the discontinuity MIB value ID that you want to test.

  host1(config-mgmtevent-trigger)#**delta-sampling discontinuity-id 1.3.6.1.2.1.31.1.1.1.19.9**

- (Optional) Enter the discontinuity type (timeStamp or timeTicks) that you want the test to use.

  host1(config-mgmtevent-trigger)#**delta-sampling discontinuity-id-type timeStamp**

10. (Optional) Configure the desired SNMP security level for the agent that you want to poll.

    host1(config)#**snmp security read**

11. Define the test values that you want this trigger to use.

    You can define a Boolean test, existence test, or threshold test. See the following sections for procedures.

Defining a Boolean Test

You can configure a Boolean trigger to test whether the value of an integer object is equal, unequal, greater than, less than, less than or equal to, or greater than or equal to some defined value.

To define a Boolean test:

1. Define the Boolean-test comparison that you want this trigger to use.

   host1(config-mgmtevent-trigger)#**boolean-test comparison greater**

2. (Optional) Specify that you do not want the Boolean test to perform a comparison when this trigger first becomes active.

   host1(config-mgmtevent-trigger)#**boolean-test startup**

3. Specify the events that you want the Boolean-test trigger to use by entering an event owner name and event name.

NOTE: You do not need to bind a failure event to a trigger. If you create a failure event and a failure occurs, the router sends the trap if the event owner is the same as the trigger owner.

   host1(config-mgmtevent-trigger)#**boolean-test event george trigger1**

   When specifying an event, use the exact owner name and event name.Specify the Boolean value to which the test compares.

   host1(config-mgmtevent-trigger)#**boolean-test value 5175438**

4. Specify the agent on which the object resides.

   host1(config-mgmtevent-trigger)#**agent context-name router1**

You can obtain the agent context name for a virtual router from the **show snmp agent** command. The agent context name is independent of the virtual router name.Enable the trigger.

host1(config-mgmtevent-trigger)#**enable**

Once enabled, you cannot edit an event or trigger configuration. To change an enabled event or trigger, you must delete it and re-create it.

Defining an Existence Test

An existence test looks for the existence of a MIB object. The appearance, disappearance, or a change in value of the object can trigger the existence test.

To define an existence test:

1. Define the existence test test-type value that you want this trigger to use.

   host1(config-mgmtevent-trigger)#**existence-test test-type changed**

2. Define the startup threshold condition—absent or present—that you want this trigger to use.

   host1(config-mgmtevent-trigger)#**existence-test startup absent**

3. Specify the events that you want the existence-test trigger to use by entering an event owner name and event name.

NOTE: You do not need to bind a failure event to a trigger. If you create a failure event, if a failure occurs, and if the trigger owner and the event owner are the same, the router sends the trap.

   host1(config-mgmtevent-trigger)#**boolean-test event george trigger1**

   When specifying an event, make sure to use the exact owner name and event name.

4. Specify the agent on which the object resides.

   host1(config-mgmtevent-trigger)#**agent context-name router1**

   You can obtain the agent context name for a virtual router from the **show snmp agent** command. The agent context name is independent of the virtual router name.

5. Enable the trigger.

   host1(config-mgmtevent-trigger)#**enable**

   Once enabled, you cannot edit an event or trigger configuration. To change an enabled event or trigger, you must delete it and re-create it.

Defining a Threshold Test

To define a threshold test:

1. Define the threshold-test values that you want this trigger to use.

NOTE: The rising value must always be larger than the falling value. Entering a lower rising value than a falling value will provide invalid results or errors.

   - absolute-value—Use when defining absolute threshold values

     host1(config-mgmtevent-trigger)#**threshold-test absolute-value rising 2000 falling 1900**

   - delta-value—Use when defining delta threshold values

     host1(config-mgmtevent-trigger)#**threshold-test delta-value rising 2000 falling 1900**

2. Define the startup threshold condition that you predict the sample to initially follow—falling, rising, risingorfalling. For example, if you are sampling a MIB value that you know will start from zero and rise, you would specify a rising startup condition.

   host1(config-mgmtevent-trigger)#**threshold-test startup rising**

3. Specify the events (rising or falling) that you want the threshold-test trigger to use by entering an event owner name and event name.

NOTE: You do not need to bind a failure event to a trigger. If you create a failure event, if a failure occurs, and if the trigger owner and the event owner are the same, the router sends the trap.

   host1(config-mgmtevent-trigger)#**threshold-test event falling sysadmin fallingtrigger**
   host1(config-mgmtevent-trigger)#**threshold-test event rising sysadmin risingtrigger**

   When specifying an event, make sure to use the exact owner name and event name.

4. Specify the agent on which the object resides.

   host1(config-mgmtevent-trigger)#**agent context-name router1**

   You can obtain the agent context name for a virtual router from the **show snmp agent** command. The agent context name is independent of the virtual router name.

5. Enable the trigger.

   host1(config-mgmtevent-trigger)#**enable**

   Once enabled, you cannot edit an event or trigger configuration. To change an enabled event or trigger, you must delete it and re-create it.

agent context-name

- Use to specify the virtual router SNMP agent on which you want to poll MIB objects.
- The default is the current context (virtual router).
- The *contextName* value is the virtual router number in the order the virtual router was created (for example, router1, router2, and so on). Use the **show snmp agent** command to obtain the context name for the virtual router.
- Use the **wildcard** keyword to specify that the context name is a wildcard value.

NOTE: Use caution when assigning wildcards. Wildcards can rapidly use up trigger resources.

- Use the **limit** keyword to specify the maximum number of agents to be polled.
- Example 1

  host1(config-mgmtevent-trigger)#**agent context-name router1 wildcard**

- Example 2

  host1(config-mgmtevent-trigger)#**agent context-name router1 wildcard limit 15**

NOTE: SNMP server security defaults to “no access.” When using a separate virtual router, you must use the **snmp-server security** command and provide “read” or “read-write” access to other virtual routers.

- Use the **no** version to return to the default context (virtual router).

boolean-test

- Use to define Boolean test values for the trigger that you are configuring, including comparison settings, a Boolean value, a startup condition, and binding an event to the Boolean-test trigger.
- Example 1—Specifying a comparison setting

  host1(config-mgmtevent-trigger)#**boolean-test comparison less**

- Example 2—Specifying a Boolean value to which the test compares

  host1(config-mgmtevent-trigger)#**boolean-test value 5175438**

- Example 3—Binding an event to the Boolean-test trigger

  host1(config-mgmtevent-trigger)#**boolean-test event sysadmin booleanTrigger**

- Example 4—Setting the trigger to not perform a Boolean test on startup

  host1(config-mgmtevent-trigger)#**boolean-test startup**

- Use the **no** version to delete the Boolean-test values for this trigger or to remove either the startup condition or event binding.

delta-sampling

- Use to specify delta sampling for the trigger you are configuring.
- Example

  host1(config-mgmtevent-trigger)#**delta-sampling**

- (Optional) Use the **discontinuity-id** option to specify a discontinuity MIB ID for the sample. The discontinuity MIB ID monitors the sample for any discontinuity errors during the sample frequency. If a discontinuity error occurs, the router removes the sampling for that interval.
- (Optional) Use the **discontinuity-id-type** option to specify a discontinuity ID type (either timeStamp or timeTicks). The discontinuity ID type indicates the time value that you expect for a specific sample.
- Use the **no** version to turn off delta sampling and use absolute sampling (the default).

enable

- Use to enable an event configuration or trigger configuration.
- Example 1—Event Configuration Mode

  host1(config-mgmtevent-event)#**enable**

- Example 2—Trigger Configuration Mode

  host1(config-mgmtevent-trigger)#**enable**

- Once enabled, you cannot edit an event or trigger configuration (even when it is disabled). To change an enabled event or trigger, you must delete it and re-create it.
- There is no **no** version.

event

- Use to create an event and access the event configuration mode of the SNMP server event manager.
- Example

  host1(config-mgmtevent)#**event sysadmin failuretrigger**
  host1(config-mgmtevent-event)#

- To leave the event configuration mode, use the **exit** command.
- Use the **no** version to remove the event.

existence-test

- Use to define existence test values for the trigger that you are configuring, including binding an event to the existence-test trigger, specifying a startup condition, and defining an existence-test type.
- You can specify one or both startup conditions in the same command. You can specify one, two, or all three test types in the same command.
- Example 1—Binding an event to the Boolean-test trigger

  host1(config-mgmtevent-trigger)#**existence-test event sysadmin existenceTrigger**

- Example 2—Specifying a startup condition

  host1(config-mgmtevent-trigger)#**existence-test startup present**

- Example 3—Specifying an existence test type

  host1(config-mgmtevent-trigger)#**existence-test test-type absent**

- Use the **no** version to delete the existence-test values for this trigger or to remove either the startup condition or event binding.

frequency

- Use to set the frequency (in seconds) at which you want MIB sampling to occur.
- Example

  host1(config-mgmtevent)#**frequency 100**

- Use the **no** version to restore the default frequency value (600 seconds).

notification id

- Use to specify a trap notification for an event.
- Example

  host1(config-mgmtevent-event)#**notification id mteTriggerFailure**

- Use the **no** version to remove the notification from the event. Removal returns the notification value to its default (0.0)

resource

- Use to specify the total number of triggers that the virtual router allows.

CAUTION: When assigning wildcards, make sure to allow for enough trigger resources.

- Example

  host1(config-mgmtevent-event)#**resource 250**

- Use the **no** version to restore the default resource value (50).

sample

- Use to specify the MIB object that you want to sample for the trigger that you are configuring.
- Example

  host1(config-mgmtevent)#**sample value-id 1.3.6.1.2.1.60.1.2.1.1.7**

- Use the **no** version to remove the MIB object from the trigger. Removal returns the sample value-id to its default (0.0).

set

- Use to perform an SNMP set operation under certain event conditions.
- Example—Sets the administrative status of interface 123 to down (2)

  host1(config-mgmtevent-event)#**set context-name router1**
  host1(config-mgmtevent-event)#**set id 1.3.6.1.2.1.2.2.1.7.123**
  host1(config-mgmtevent-event)#**set value 2**

- Use the **no** version to remove the set operation.

snmp-server management-event

- Use to launch the SNMP server event manager mode on each virtual router on which you plan to manage events.
- Example

  host1(config)#**snmp-server management-event**
  host1(config-mgmtevent)#

- To leave the SNMP server event manager, use the **exit** command.
- Use the **no** version to delete all the management events.

snmp-server security

- Use to specify a security access level for the SNMP agent.
- Example

  host1(config)#**snmp-server security read**

- Use the **no** version to return to the SNMP security level to its default (no-access).

threshold-test

- Use to define the threshold values for the trigger that you are configuring, including specifying rising and falling values, a startup threshold condition, and binding an event to the threshold-test trigger.
- Example 1—Specifying absolute values

  host1(config-mgmtevent-trigger)#**threshold-test absolute-value rising 2000 falling 1900**

- Example 2—Specifying a startup threshold condition

  host1(config-mgmtevent-trigger)#**threshold-test startup rising**

- Example 3—Binding an event to the threshold-test trigger

  host1(config-mgmtevent-trigger)#**threshold-test event sysadmin failureTrigger**

- Use the **no** version to delete the threshold-test values for this trigger or remove either the threshold startup condition or event binding.

trigger

- Use to create a trigger and access the trigger configuration mode of the SNMP server event manager.
- Example

  host1(config-mgmtevent)#**trigger fred trigger1**
  host1(config-mgmtevent-trigger)#

- To leave the trigger configuration mode, use the **exit** command.
- Use the **no** version to remove the trigger.

Monitoring Events

To view the status of the SNMP agent, use the following **show snmp agent** command. To view statistics associated with events, resources, and triggers, use the **show snmp management-event** command.

show snmp agent

- Use to view SNMP MIB agent information.
- Field descriptions
  - context name—Router that contains the MIB agent
  - access permission level—Access permission level for other virtual routers that may want to access the agent
- Example

```
host1#show snmp agent
context name: router1
access permission level: no access
snmp proxy: enabled
```

show snmp management-event

- Use to view statistical SNMP event information for event table entries, router resources, and trigger table entries.
- Omit the **events**, **resource**, **statistics**, or **triggers** options to obtain a full output.
- Field descriptions
  - Resource
    - SampleMinimum—Minimum number of samples to be taken
    - SampleInstanceMaximum—Maximum number of samples to be taken
    - SampleInstances—Number of sample instances being monitored

- SampleInstancesHigh—Highest number of samples taken for any of the sample instances
- SampleInstancesLacks—Number of times this system could not take a new sample because that allocation would have exceeded the limit set by mteResourceSampleInstanceMaximum

- Triggers
  - Owner—Owner value assigned to the trigger
  - Name—Name value assigned to the trigger
  - Test—Type of trigger test to perform
  - SampleType—Type of sampling (absolute or delta) to perform
  - ValueID—Object ID of the MIB sample for this trigger
  - ValueIDLimit—Not supported in this release; reads as zero
  - ValueIDWildcard—Not supported in this release; reads as False
  - ContextName—Management context (for example, router1) from which to obtain mteTriggerValueID
  - ContextNameRgulrExprssn—Not supported in this release
  - ContextNameLimit—Not supported in this release; reads as zero
  - ContextNameWildcard—Not supported in this release; reads as False
  - Frequency—Frequency at which this trigger is sampled
  - ObjectsOwner—Not supported in this release
  - Objects—Not supported in this release
  - Enabled—State (False [disabled] or True [enabled]) of the trigger
  - EntryStatus—Active/inactive status of the instance
- Boolean
  - Comparison—Comparison value for this trigger
  - Value—Object ID value to which this trigger compares
  - Startup—Whether or not this trigger performs a Boolean test on startup
  - ObjectsOwner—Owner of this object
  - Objects—Name of this object
  - EventOwner—Owner of this event
  - Event—Name of this event
- Existence
  - Test—Test type for this trigger
  - Startup—Startup condition for this trigger
  - ObjectsOwner—Owner of this object
  - Objects—Name of this object
  - EventOwner—Owner of this event
  - Event—Name of this event

- Statistics
  - trigger owner—Owner value assigned to the trigger
  - trigger name—Name value assigned to the trigger
  - current time—Current UTC time
  - started sampling—UTC time sampling started
  - last sampled—UTC time event last sampled
  - sample instances—Number of sample instances being monitored
  - times sampled—Number of times events sampled
  - event traps—Number of traps sent
  - event sets—Number of events set
  - failures—Number of event failures
  - sample overrun—Number of times the event manager missed sampling for the current value within the given time period
  - failure traps—Number of failure traps sent as a result of event failures
- Threshold
  - Startup—Startup threshold condition for this trigger
  - Rising—Rising threshold condition for this trigger
  - Falling—Falling threshold condition for this trigger
  - DeltaRising—Delta rising threshold condition for this trigger
  - DeltaFalling—Delta falling threshold condition for this trigger
  - ObjectsOwner—Not supported in this release
  - Objects—Not supported in this release
  - RisingEventOwner—Rising event owner value for this trigger
  - RisingEvent—Rising event name value for this trigger
  - FallingEventOwner—Falling event owner value for this trigger
  - FallingEvent—Falling event name value for this trigger
  - DeltaRisingEventOwner—Delta rising event owner value for this trigger
  - DeltaRisingEvent—Delta rising event name value for this trigger
  - DeltaFallingEventOwner—Delta falling event owner value for this trigger
  - DeltaFallingEvent—Delta falling event name value for this trigger
- Delta
  - DiscontinuityID—Discontinuity MIB ID for this trigger
  - DiscontinuityIDWildcard—Not supported in this release
  - DiscontinuityIDType—Discontinuity ID type for this trigger

- Events
  - Owner—Owner value for this event
  - Name—Name of this event
  - Actions—Action (for example, notification) that takes place when this event is triggered
  - Enabled—Enabled state (True [enabled] or False [disabled]) of this event
  - EntryStatus—Entry status for this event
- Notification
  - Notification—Notification trap setting for this event
  - ObjectsOwner—Not supported in this release
  - Objects—Not supported in this release
- Set
  - Object—Object ID that the trigger is setting
  - ObjectWildcard—Whether or not the object is a wildcard
  - Value—Value to which you are setting the object ID when the trigger fires
  - ContextName—Management context (for example, router1) from which to obtain mteTriggerValueID
  - ContextNameWildcard—Whether or not the context name is a wildcard

- Example

```
host1#show snmp management-event
                                  Resource
------------------------------------------------------------------------------
SampleMinimum: 1
SampleInstanceMaximum: 50
SampleInstances: 14
SampleInstancesHigh: 14
SampleInstancesLacks: 0

                                   Triggers
------------------------------------------------------------------------------
Owner: unitTest
Name: booleantest1
Test: boolean
SampleType: absoluteValue
ValueID: 1.3.6.1.2.1.92.1.1.2.0
ValueIDLimit: 0
ValueIDWildcard: False
ContextName: router1
ContextNameLimit: 0
ContextNameWildcard: False
Frequency: 40
ObjectsOwner: unitTest
Objects: test3
Enabled: False
EntryStatus: createAndWait
----------------------- Boolean
Comparison: equal
```

```
Value: 300
Startup: False
ObjectsOwner:
Objects:
EventOwner: unitTest
Event: eventTest1
-------------------------------- Trigger
Owner: unitTest
Name: booleantest2
Test: boolean
SampleType: absoluteValue
ValueID: 1.3.6.1.2.1.92.1.1.2.0
ValueIDLimit: 0
ValueIDWildcard: False
ContextName: router1
ContextNameLimit: 0
ContextNameWildcard: False
Frequency: 40
ObjectsOwner: unitTest
Objects: test3
Enabled: False
EntryStatus: createAndWait
------------------------ Existence
Test: absent
Startup: absent
ObjectsOwner: unitTest
Objects: test3
EventOwner: unitTest
Event: eventTest3
------------------------ Threshold
Startup: falling
Rising: 200
Falling: 100
DeltaRising: 0
DeltaFalling: 0
ObjectsOwner:
Objects:
RisingEventOwner: unitTest
RisingEvent: eventTest2
FallingEventOwner: unitTest
FallingEvent: eventTest3
DeltaRisingEventOwner:
DeltaRisingEvent:
DeltaFallingEventOwner:
DeltaFallingEvent:
------------------------ Delta
DiscontinuityID: 1.3.6.1.2.1.92.1.1.2
DiscontinuityIDWildcard: True
DiscontinuityIDType: timeTicks

                                    Objects
--------------------------------------------------------------------------------
Owner: unitTest Name: test1
Index: 1
ID: 1.3.6.1.2.1.11.1.0
IDWildcard: False
EntryStatus: active
Index: 2
ID: 1.3.6.1.2.1.11.2.0
IDWildcard: False
EntryStatus: active
Index: 5
ID: 1.3.6.1.2.1.11.30.0
```

```
IDWildcard: False
EntryStatus: active

                                    Events
--------------------------------------------------------------------------------
Owner: unitTest
Name: eventTest1
Actions: notification set
Enabled: True
EntryStatus: active
------------------------ Notification
Notification: mteTriggerFired
ObjectsOwner: unitTest
Objects: test3
------------------------ Set
Object: 1.3.6.1.2.1.11.1.0
ObjectWildcard: False
Value: -20
ContextName: router
ContextNameWildcard: True
```

Collecting Bulk Statistics

The router offers an efficient data collection and transfer facility for accounting applications. The E-series router SNMP MIBs extend the accounting data collection mechanism defined in the Accounting-Control-MIB (RFC 2513) to include support for connectionless networks.

Service providers need reasonably accurate data about customers' use of networks. This data is used for billing customers and must be available at a customer's request. Accounting applications based on SNMP polling models consume significant network bandwidth because they poll large volumes of data frequently.

Unfortunately, SNMP is not well suited for gathering large volumes of data, especially over short time intervals. It is inadequate for use by accounting applications because:

- The SNMP PDU layout has a low payload-to-overhead ratio.
- Processing SNMP PDUs is expensive because objects and tables need to be sorted in lexicographic order.

The router avoids the need for continuous polling of SNMP statistics by using applications known as *collectors* to retrieve data. You can configure up to six collectors. The router sends collected statistics through FTP to assigned hosts, known as *receivers*. You must assign a primary receiver to each collector, and you can assign a secondary receiver for redundancy.

NOTE: The basic-encoding-rules (BER)–encoding choice is not supported.

You can collect interface bulk statistics based on sets of virtual router groups. If sets of virtual router groups generally correspond to ISPs, you can then forward the relevant data to a particular ISP.

To configure a collector to include data from a specific list of virtual routers, you must first configure a collector and then associate a router set with it. A collector can have up to 64 virtual routers associated with it.

To collect bulk statistics for a subset of all configured subinterfaces, you can define the subinterfaces using the following syntax:

Slot/Port[.*subInterfaceId*]

Per virtual router collection is supported on the if-stats and igmp schemas. It is supported on all interface types supported by BulkStats. Collectors modified to use per virtual router collection or configured after a collector has started have a time delay (up to the configured time in seconds) until an active collector starts again.

The maximum number of interfaces for each type of interface and line module can differ. Bulk statistics can collect these statistics when you configure the slots with their respective interfaces to the corresponding maximum values. For information about maximum values see *JUNOSe Release Notes*, *Appendix A*, *System Maximums*.

NOTE: Define all interface types before you map a collector to the if-stats schema to ensure that you display statistics for all configured interfaces in the first interval.

The name of the bulk statistics file that is transferred to the host when there is a collectorSequence attribute in the remote name is as follows:

fileName-z-mmddHHMM-s.sts

where:

- *fileName*—Name of the file, which includes sysName, sysUpTime, depending on the attributes specified
- *-z*—Receiver index value
- *mmddHHMM*—Timestamp when the receiver is created in month/day/hour/minute format
- *-s*—Actual sequence number

Interface Strings

Bulk statistics provides interface strings as described in Table 24.

Table 24: Interface Strings

Type of Interface	Common Description Format-Mode Disabled	Common Description Format-Mode Enabled
IP interfaces	IP	Ip
PPP interfaces	PPP	Ppp
DS0 interfaces	Ds0	Ds0
DS1 interfaces	SERIAL	Ds1
DS3 interfaces	SERIAL	Ds3

Table 24: Interface Strings (continued)

Type of Interface	Common Description Format-Mode Disabled	Common Description Format-Mode Enabled
Frame Relay Major interfaces	FR	FrameRelayMajor
Ethernet interfaces	ENET	Ethernet
Sonet interfaces	SONET	Sonet
Sonet Path interfaces	SONET	SonetPath
ATM interfaces	ATM	Atm
ATM AAL5 interfaces	ATM	AtmAal5
ATM 1483 interfaces	ATM	Atm1483
Ft1 interfaces	SERIAL	Ft1
HDLC interfaces	HDLCIntf	HDLC
IpLoopback interfaces	Loopback	IpLoopback
IpVirtual interfaces	IpVirtual	IpVirtual
Frame Relay Sub interfaces	FR	FrameRelaySub
PppOE Major interfaces	PPPoE	PppoeMajor
PppOE Sub interfaces	PPPoE	PppoeSub
Bridged Ethernet	BRG-ET	BridgedEthernet
L2TP Tunnel	L2TP	L2tpTunnel
L2TP Session	L2TP	L2tpSession
PppLink interfaces	MLPPP	PppLink
HDLC interfaces	HDLCEncaps	Hdlc
L2TP Destinataion	L2TP	L2tpDestination
MPLS Major interfaces	MplsIfMajor	MplsMajor
MPLS Minor interfaces	MplsIfMinor	MplsMinor
Ppp Network interfaces	MLPPP	PppNetwork
Ethernet Sub interfaces	ENET	EthernetSub
MultiLink Frame Relay interfaces	MLFR	MultilinkFrameRelay
Ip Tunnel Interfaces	IP-TUNNEL	IpTunnel
Server Port Interfaces	ServerPort	ServerPort
Sonet VT interfaces	SONET	SonetVT
Vlan major interfaces	VLAN-MAJ	VlanMajor
Vlan sub interfaces	VLAN-SUB	VlanSub
Gtp interfaces	Gtp	Gtp
L2fTunnel interfaces	L2fTunnel	L2fTunnel
L2fSession interfaces	L2fSession	L2fSession
L2fDestination interfaces	L2fDestination	L2fDestination
IpSec Tunnel interfaces	IpSecTunnel	IpsecTunnel
Sg interfaces	SgInterface	SgInterface
MPLS L2 Shim interfaces	MplsL2Shim	MplsL2Shim
MPLS VC Sub interfaces	MplsL3Shim	MplsVcSub

Table 24: Interface Strings (continued)

Type of Interface	Common Description Format-Mode Disabled	Common Description Format-Mode Enabled
LacGen interfaces	LacGen	LacGen
Bridge interfaces	BridgeIf	Bridge
IpSec Transport interfaces	IPSecTransportIf	IpsecTransport
IPv6 interfaces	IPv6If	Ipv6
IPv6 Tunnel interfaces	IPv6TunnelIf	Ipv6Tunnel
IPv6 loopback interfaces	IPv6LoopbackIf	Ipv6Loopback
OSI interfaces	Osi	Osi
LAG interfaces	Lag	Lag
Ip Tunnel MDT interfaces	IpTunnelMdt	IpTunnelMdt

Understanding Counter Discontinuity

Interface counter discontinuity can occur when a counter wraps or after a line module is reloaded or reset. If one of these actions occurs, applications that utilize the counters in expressions or calculations generate erroneous values and misleading graphs.

Because counters are 64 bits long, the possibility of a counter's wrapping naturally would occur so infrequently (for example, in many hundreds of years) that this scenario is not recognized as an issue.

Counter discontinuity does occur, however, when you reload or reset a line module. To indicate reloading or resetting, bulk statistics files contain a record similar to the following:

```
{Controller down slot 3, TUE OCT 29 2004 14:25:10.370 UTC}
```

This record provides a mechanism by which applications can detect discontinuity events. To take advantage of this detection capability, the bulk statistics parsing entity should use the record to terminate expression or formula calculations for the indicated slot and to establish a new baseline.

Configuring Collectors and Receivers

To configure the router to collect statistics:

1. Add names to the FTP host table for the primary and secondary (optional) receivers.

   See *Copying and Redirecting Files* in *Chapter 5, Managing the System*, for information about adding names to the host table.

2. Specify the type of interface on which you want to collect statistics.

   host1(config)#**bulkstats interface-type ppp collector 2**

3. Specify the parameters for the receivers.

   host1(config)#**bulkstats receiver 1 remote-name js:/ftptest/bulk%s%s.sts sysName sysUpTime**

4. Assign the data collector.

   host1(config)#**bulkstats collector 2**

5. Specify the method for data collection.

   host1(config)#**bulkstats collector 2 collect-mode auto**

6. Assign the primary receiver.

   host1(config)#**bulkstats collector 2 primary-receiver 1**

7. (Optional) Assign the secondary receiver.

   host1(config)#**bulkstats collector 2 secondary-receiver 5**

8. (Optional) Specify the time for which the system transfers data.

   host1(config)#**bulkstats collector 2 interval 1000**

9. (Optional) Set the maximum size of the bulk statistics file.

   host1(config)#**bulkstats collector 2 max-size 20480**

10. (Optional) Add descriptive information to the bulk statistics file.

    host1(config)#**bulkstats collector 2 description customer xyz**

11. (Optional) Set the encoding scheme of the ifDescr and ifName objects.

    host1(config)#**bulkstats interfaces description-format common**

12. (Optional) Set the system to retrieve bulk statistics once only.

    host1(config)#**bulkstats collector 2 single-interval**

13. (Optional) Configure bulk statistics traps.

    host1(config)#**bulkstats traps nearly-full**

14. (Optional) Collect bulk statistics per virtual router.

    host1(config)#**bulkstats virtual-router-group collector 2 routerISP3**

NOTE: The bulk statistics feature supports generating files on a per interface basis.

bulkstats collector

- Use to assign the data collector.
- Example

  host1(config)#**bulkstats collector 2**

- Use the **no** version to delete the collector.

bulkstats collector collect-mode

- Use to specify the way the collector retrieves bulk statistics.
- Example

  host1(config)#**bulkstats collector 2 collect-mode auto**

- Use the **no** version to specify that either the user or the system will initiate transfers manually.

bulkstats collector description

- Use to add descriptive information to the bulk statistics file.
- Example

  host1(config)#**bulkstats collector 2 description customer xyz**

- Use the **no** version to remove descriptive text from the bulk statistics file.

bulkstats collector interval

- Use to specify the time interval in seconds for which the collector transfers data to the receivers.
- Example

  host1(config)#**bulkstats collector 2 interval 1000**

- Use the **no** version to set this time to the default, 360 seconds (6 minutes).

bulkstats collector max-size

- Use to set the maximum size of the bulk statistics file for all collectors combined. Even when you configure more than one collector, the first maximum file size configured is the combined size of all collectors.
- The maximum file size that you can configure is 20971520 bytes. However, if you do not configure a maximum size, then the maximum file size defaults to 5767168 bytes.
- Although the CLI accepts the commands, you cannot unconfigure or modify the configuration of the maximum file size until the router is rebooted.
- Example

  host1(config)#**bulkstats collector 2 max-size 20480**

- Use the **no** version to set the size of the bulk statistics file to the default, 5767168 bytes.

bulkstats collector primary-receiver

- Use to assign the primary receiver to which the system transfers data.
- The index for the receiver must match the index that you specified with the **bulkstats receiver remote-name** command.
- Example

  host1(config)#**bulkstats collector 2 primary-receiver 7**

- Use the **no** version to clear the primary receiver and disable the collector.

bulkstats collector secondary-receiver

- Use to assign the secondary (that is, the backup) receiver to which the system transfers data.
- The index for the receiver must match the index you specified with the **bulkstats receiver remote-name** command.
- Example

  host1(config)#**bulkstats collector 2 secondary-receiver 5**

- Use the **no** version to clear the secondary receiver.

bulkstats collector single-interval

- Use to set the system to retrieve bulk statistics once only, rather than periodically.
- Example

  host1(config)#**bulkstats collector 2 single-interval**

- Use the **no** version to set the system to retrieve bulk statistics periodically, the default situation.

bulkstats interfaces description-format common

- Use to set the encoding scheme of the ifDescr object that the bulk statistics application reports to the conventional industry method.
- This command provides compatibility with software that uses the industry encoding scheme.
- For more information, see *Configuring Encoding Method* on page 150.
- Example

  host1(config)#**bulkstats interfaces description-format common**

- Use the **no** version to return to the proprietary method of encoding.

bulkstats interface-type

- Use to configure the interface or subinterface type on which you want to collect statistics.
- You can provide an interface specifier (location) to identify a specific interface on which you want to collect statistics.
- If you define more than one collector, you must specify a unique collector index, in the range 1–65535.
- The supported interface types are:
  - **atm**—Collects statistics on ATM interfaces
  - **atm1483**—Collects statistics on ATM 1483 interfaces
  - **ethernet**—Collects statistics on Ethernet interfaces
  - **frame-relay**—Collects statistics on Frame Relay interfaces
  - **frame-relay-sub**—Collects statistics on Frame Relay subinterfaces
  - **hdlc**—Collects statistics on Cisco HDLC interfaces
  - **ip**—Collects statistics on IP interfaces
  - **mplsMajor**—Collects statistics on MPLS major interfaces
  - **mplsMinor**—Collects statistics on MPLS minor interfaces
  - **mplsL2shim**—Collects statistics on MPLS shim interfaces
  - **ppp**—Collects statistics on PPP
  - **vlan**—Collects statistics on VLAN subinterfaces

NOTE: You cannot collect statistics on the SRP Ethernet interface.

- Example 1

  host1(config)#**bulkstats interface-type ppp 3/1 collector 2**

- Example 2

  host1(config)#**bulkstats interface-type vlan 2/3:1 collector 1**

- Example 3

  host1(config)#**bulkstats interface-type mplsMajor 2/3:1 collector 1**

- Use the **no** version to delete the interface type from bulk statistics collection. Deletion of a particular interface type takes effect at the next collection interval.

bulkstats receiver remote-name

- Use to configure the parameters for receivers.
- Bulk statistics transfers require the configuration of a remote FTP server.
- The receivers must appear in the FTP host table. The name of the host must match the name you specify with this command. The hostname is relative to the virtual router's context when you issue this command.
- When specifying the remote filename for bulk statistics, you must precede the filename with the hostname followed by the :/ characters.
- Example

  host1(config)#**bulkstats receiver 1 remote-name js:/ftptest/bulk%s%s.sts sysName sysUpTime**

NOTE: The % variables in the remote name are replaced at runtime with the sysName and sysUpTime parameters to produce variable filenames on the remote host.

- Use the **no** version to delete the receiver.

bulkstats traps

- Use to configure bulk statistics traps.
- You must configure SNMP correctly and specify a valid trap source. Otherwise, the system will not send SNMP traps.
- Example

  host1(config)#**bulkstats traps nearly-full**

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

bulkstats virtual-router-group

- Use to collect interface statistics for each virtual router.
- A collector can have a maximum of 64 virtual routers associated with it.
- Routers are identified by their assigned name or router index.
- Supported only on if-stats and igmp schemas.
- Supported on all interface types supported by the bulk statistics application.
- Collectors modified to use per virtual router collection or configured after a collector has started have a time delay until an active collector starts again.

- Example

  host1(config)#**bulkstats virtual-router-group collector *2* routerISP3**

- Use the **no** version to prevent bulkstats from being reported for virtual router groups.

Deleting All Bulkstats Configurations

Although individual bulkstats commands allow you to disable or delete a specific bulkstats parameter, the CLI also allows you to remove all bulkstats configurations from the router at one time.

no bulkstats

- Use to remove all bulkstats configurations from the router at one time.
- Example

  host1(config)#**no bulkstats**

Monitoring Collection Statistics

To view the parameters the router uses to collect statistics, use the following **show bulkstats** commands.

To include or exclude lines of output based on a text string that you specify, use the output filtering feature for **show** commands. For details, see *Chapter 2, Command-Line Interface*.

show bulkstats

- Use to display the bulk statistics data collection configuration.
- Field descriptions
  - AdminStatus—Administrative status of the bulk statistics application
  - OperStatus—Operational status of the bulk statistics application, enabled or disabled
  - Interface Description Setting—Method used to encode the ifDescr object: common, proprietary, industry-common
  - File Format—End of the line format in bulkstats files, carriage return and line feed (CR + LF) or LF
  - Current Time—Current system time used to compare with the collection stop/start time
  - Intervals—Number of times the bulk statistics collector has cycled through a collection
  - PrimaryXfers—Number of times the bulk statistics collector has attempted a data file transfer to a primary server
  - PrimaryFails—Number of primary server transfer failures
  - SecondaryXfers—Number of times the bulk statistics collector has attempted a data file transfer to a secondary server
  - SecondaryFails—Number of secondary server transfer failures

- BulkStats Collector Information:
  - Index—Bulk statistics collector index number
  - CurrSize—Current size of the bulk statistics file in bytes
  - MaxSize—Maximum size configured for the bulk statistics file in bytes
  - Intrvl—Time interval between bulk collections in seconds
  - Mode—How often the collector is set up to collect statistics:
    - periodic—Collects statistics periodically
    - single-interval—Collects statistics once only
  - XferMode—Collect mode configured for the collector:
    - auto—Agent transfers file when interval expires
    - manual—Network management system or the user initiates transfers
    - onFull—Agent transfers file when it reaches the maximum size
  - State
    - inProg—Collector is properly configured and currently active
    - notInSvc—Collector has been decommissioned by a management client
    - notReady—Collector does not have enough configuration information to go active
    - error—Configuration or operational error
  - Index—Bulk statistics collector index number
  - Primary-Receiver—Index number of the primary receiver to which the system transfers data, if defined
  - Second-Receiver—Index of the secondary receiver to which the system transfers data
  - Last Transfer Failure—Last time that the collector attempted to retrieve statistics and was unsuccessful
  - Interval Start Time—Start of current interval of bulk collections. The collector began collecting bulk statistics at this time.
  - Interval Stop Time—End of current interval of bulk collections.
- Schema Information:
  - Index—Index number of the schema
  - Subtree—Type of bulk statistics schema configured on the collector: if-stack, if-stats, or system
  - CollectorIndex—Bulk statistics collector index number
  - Create-Delete Time Stats—State of final statistics collection (enabled or disabled)

- Create-Delete Interface Type—Interface type associated with final statistics collection (ATM 1483, IP, PPP)
- State
  - active—Schema is properly configured and currently active
  - notInSvc—Schema has been decommissioned by a management client
  - notReady—Schema does not have enough configuration information to go active
  - error—Configuration or operational error
- Subtree List—Types of statistics the schema is configured to receive

- Interface Types:
  - Index—Index number of the interface type entry
  - Type—Interface type for which bulk statistics collection is configured
  - CollectorIndex—Index number of the collector to which the interface type applies
  - State
    - active—Interface type is properly configured and currently active
    - notInSvc—Interface type has been decommissioned by a management client
    - notReady—Interface type does not have enough configuration information to go active
    - error—Configuration or operational error

- Receiver Information:
  - Index—Index number of the receiver
  - RemoteFileName—Hostname, path, and filename of the remote FTP server
  - State
    - active—Receiver is properly configured and currently active
    - notInSvc—Receiver has been decommissioned by a management client
    - notReady—Receiver does not have enough configuration information to go active
    - error—Configuration or operational error
  - Status
    - Success
    - Copy source does not exist or is unreachable

        - Copy failed
        - File in use
    - Virtual Router Groups:
        - Collector—Number that identifies the particular data collector, in the range 1–65535
        - Virtual-Routers—Set of virtual router names (up to 64 names)
- Example

```
host1#show bulkstats

  AdminStatus:  enabled
  OperStatus:   enabled
  Interface Description Setting: industry-common
  File Format: CR+LF
Current Time: TUE AUG 15 2002 15:54:20 UTC

  Intervals PrimaryXfers PrimaryFails SecondaryXfers SecondaryFails
  --------- ------------ ------------ -------------- --------------
  0         0            0             0              0

  BulkStats Collector Information:
  Index  CurrSize  MaxSize   Intrvl  Mode      XferMode  State
  -----  --------  --------  ------  --------- --------  -------
  1      490       3670016   600     periodic  manual    inProg
  2      0         3670016   360     periodic  manual    notReady

  Index  Primary-Receiver  Second-Receiver  Last Transfer Failure
  -----  ----------------  ---------------  --------------------
  1      1                 not defined
  2      not defined       not defined

  Index Interval Start Time          Interval Stop Time
  ----- ---------------------------- -------------------------
  1     TUE AUG 15 2000 15:52:33 UTC TUE AUG 15 2000 16:02:33 UTC
  2     Not started                  N/A

Schema Information:
  Index  Subtree
  -----  -------------------------------------------------
  1      ifStats

  Index  CollectorIndex  State
  -----  --------------  --------
  1      1               active

  Index  Create-Delete Time Stats  Create-Delete Interface Types
  -----  ------------------------  -----------------------------
  1      enabled                   IP

  Index  Subtree List
  -----  ------------------------------------------------------------------
  1      all
```

```
  Interface Types:
  Index         Type             CollectorIndex  State
  -----  ----------------------  --------------  --------
  1      Ppp                     1               active
  6      Ethernet                1               active
  11     Atm1483                 1               active

  Receiver Information:
  Index  RemoteFileName
  -----  ------------------------------------------------------
  1      host:/upload/bulkStas.sts

  Index  State     Status
  -----  --------  ---------------------------------------------
  1      notReady  Copy source does not exist or is unreachable

Collector  Virtual-Routers
---------  ---------------
33              serviceProviderABC
655              default
```

show bulkstats collector description

- Use to display information about the collector's file description.
- Field descriptions
  - Index—Index number of the bulk statistics collector
  - FileDescription—Descriptive information added to the bulk statistics file with the **bulkstats collector description** command
- Example

```
host1#show bulkstats collector description
  Index  FileDescription
  -----  -----------------------
  1      Bulk SNMP Statistics Collection
```

show bulkstats collector interval

- Use to display information about the collector transfer interval configuration.
- Field descriptions
  - Index—Index number of the bulk statistics collector
  - Interval—Amount of time, in seconds, that the collector transfers data to the receiver
- Example

```
host1#show bulkstats collector interval
Index  Interval
-----  --------
1      360
```

show bulkstats collector max-size

- Use to display information about the bulk statistics maximum file size configuration.
- Field descriptions
  - Index—Index number of the bulk statistics collector
  - MaxSize—Maximum size of the bulk statistics file in bytes
- Example

```
host1#show bulkstats collector max-size
Index  MaxSize
-----  ------------
1      2097152
```

show bulkstats collector transfer-mode

- Use to display information about the bulk statistics transfer mode configuration.
- Field descriptions
  - Index—Index number of the bulk statistics collector
  - Transfer-Mode:
    - auto-xfer—Server automatically transfers the bulk statistics files to a remote FTP server
    - manual-xfer—Server expects the user to transfer bulk statistics files
    - on-file-full—Server transfers the bulk statistics file when the file reaches its maximum size
  - Primary-Receiver—Receives the bulk statistics sent by the collector
  - Secondary-Receiver—Serves as a backup to the primary receiver
- Example

```
host1#show bulkstats collector transfer-mode
Index  Transfer-Mode  Primary-Receiver  Secondary-Receiver
-----  -------------  ----------------  ------------------
1      auto-xfer      1                 2
```

show bulkstats interface-type

- Use to display information about the bulk statistics interface types configuration.
- Field descriptions
  - Interface Types:
  - Index—Index number of the interface type entry
  - Type—Interface type for which bulk statistics collection is configured

- CollectorIndex—Index of the collector to which the interface type applies
- State
  - active—Interface type is properly configured and currently active
  - notInSvc—Interface type has been decommissioned by a management client
  - notReady—Interface type does not have enough configuration information to go active
  - error—Configuration/operational error

- Example

```
host1#show bulkstats interface-type

Interface Types:
  Index         Type             Collector  State
  -----  ----------------------  ---------  --------
  1      ppp                     1          active
```

show bulkstats receiver

- Use to display information about the remote file configuration of the bulk statistics receiver.
- Field descriptions
  - Index—Index number of the receiver
  - RemoteFileName—Hostname, path, and filename of the remote FTP server
  - Index—Index number of the receiver
  - State
    - active—Receiver is properly configured and currently active
    - notInSvc—Receiver has been decommissioned by a management client
    - notReady—Receiver does not have enough configuration information to go active
    - error—Configuration/operational error
  - Status
    - Success
    - Copy source does not exist or is unreachable
    - Copy failed
    - File in use

- Example

```
host1#show bulkstats receiver

  Index  RemoteFileName
  -----  ---------------------------------------------
  1      f:/upload/bulkStas.sts

  Index  State     Status
  -----  --------  ---------------------------------------------
  1      notReady  Copy source does not exist or is unreachable
```

show bulkstats statistics

- Use to display bulk statistics counters.
- Field descriptions
  - AdminStatus—Administrative status of the bulk statistics application
  - OperStatus—Operational status of the bulk statistics application
  - HdwDetects—Number of times the bulk statistics application detected a line module bulkstat collector's presence
  - HdwCollectorCreates—Number of line module collectors created
  - CollectorCreateReqs—Number of times the bulk statistics application requested the creation of a line module collector
  - CollectorStopReqs—Number of times the bulk statistics application requested the line module collectors to stop
  - CollectorDeleteReqs—Number of times the bulk statistics application requested the deletion of a line module collector
  - CollectorStarts—Number of times the bulk statistics collector has started
  - CollectorIncompleteCfgs—Number of times the bulk statistics collector attempted to start a collector, but failed because the collector's configuration was incomplete
  - CollectorStopFailures—Number of times the bulk statistics collector failed during a collector stop request
  - DriverErrors—Number of bulk statistics driver errors
  - FileSizeFulls—Number of times the bulk statistics application ran out of storage space
  - CollectorFileNearlyFullTraps—Number of nearly full events posted to the SNMP agent on this router
  - CollectorFileFullTraps—Number of file full events posted to the SNMP agent on this router
  - Intervals—Number of times the bulk statistics collector has cycled through a collection
  - PrimaryXfers—Number of times the bulk statistics collector has attempted a data file transfer to a primary server
  - PrimaryFails—Number of primary server transfer failures
  - SecondaryXfers—Number of times the bulk statistics collector has attempted a data file transfer to a secondary server

- SecondaryFails—Number of secondary server transfer failures
- BulkStats Collector Statistics:
  - Index—Bulk statistics collector index
  - CurrSize—Current size of the bulk statistics storage file in bytes
  - CreateErrs—Number of bulk statistics collector create errors
  - Last Transfer Failure—Last time that the collector attempted to retrieve statistics and was unsuccessful
  - Interval Start Time—Start of current interval or bulk collections. The collector began collecting bulk statistics at this time.
  - Interval Stop Time—End of current interval of bulk collections
- Dynamic Interface Collector statistics:
  - Collector Index—Bulk statistics collector index
  - Slot#—Slot number from which the statistics were obtained
  - Received—Number of records for dynamic interfaces that were reported by the specified interface
  - Transferred—Number of record for dynamic interface that were written to the bulk statistics (.sts) file.
  - Dropped—Number of records for dynamic interfaces that were dropped (that is, not written to the bulk statistics [.sts] file)

- Example

```
host1#show bulkstats statistics

AdminStatus:                  enabled
OperStatus:                   enabled
HdwDetects:                   4
HdwCollectorCreates:          8
CollectorCreateReqs:          2
CollectorStopReqs:            0
CollectorDeleteReqs:          0
CollectorStarts:              25
CollectorIncompleteCfgs:      3
CollectorStopFailures:        0
DriverErrors:                 0
FileSizeFulls:                0
CollectorFileNearlyFullTraps: 0
CollectorFileFullTraps:       0

  Intervals PrimaryXfers PrimaryFails SecondaryXfers  SecondaryFails
  --------- ------------ ------------ --------------  --------------
  24         18            5             0               0

  BulkStats Collector Statistics:
  Index  CurrSize  CreateErrs  Last Transfer Failure
  -----  --------  ----------  ----------------------------
  1      331       0           MON JAN 24 2001 17:21:33 UTC
  2      0         0

  Index Interval Start Time          Interval Stop Time
  ----- ---------------------------- -------------------------
  1     MON JAN 24 2001 19:09:33 UTC MON JAN 24 2001 19:15:33 UTC
  2     Not started                  N/A
```

```
Dynamic Interface Collector statistics:
  CollectorIndex  Slot#  Received    Transferred  Dropped
  --------------  -----  ----------  -----------  ----------
  1               1      0           0            0
```

show bulkstats traps

- Use to display information about the bulk statistics traps configured to collect statistics.
- Field descriptions
  - Trap Type
    - nearly-full—Trap will be posted to the SNMP entity on this system when the threshold is reached
    - file-full—Trap will be posted to the SNMP entity on this system when the trap reaches 100 %
  - State—Configuration setting: enabled, disabled
  - Threshold—Nearly full trap will be posted to the SNMP entity on this system when this percentage is reached
  - Traps Sent—Number of times this event was posted to the SNMP entity on this system
- Example

```
host1#show bulkstats traps
Trap Type    State   Threshold    Traps Sent
-----------  -------  ----------  ----------
file-full    enabled  N/A         0
nearly-full  enabled  5           0
```

show bulkstats virtual-routers

- Use to display information about the bulk virtual router group configuration.
- Field descriptions
  - Collector—Number that identifies the particular data collector, in the range 1–65535
  - Virtual-Routers—Set of virtual router names (up to 64 names)
- Example

```
host1#show bulkstats virtual-routers

Collector  Virtual-Routers
---------  ---------------
33             serviceProviderABC
655             default
```

Configuring Schemas

You can also set a management schema for bulk statistics. A schema is a group of attributes or counters that provide an efficient way to retrieve specific types of information about the router. The bulk statistics application supports five schema configurations: *igmp, if-stack, if-stats*, *policy,* and *system*.

NOTE: There are no explicit schema objects for the if-stack and system schemas.

Table 25 shows the type of data each schema retrieves.

Table 25: Data Retrieved According to Schema

Schema	Retrieves
igmp	Statistics associated with various IGMP components.
if-stack	The interface and interface column configuration. It is a complete retrieval of the ifStackTable, and using it can dramatically reduce the time to discover the configured interfaces and their stacking relationship on a router.
if-stats	Usage data on sets of interface types. The interface usage data is the ifTable/ifXTable counters. Note that the ifXTable supports 64-bit counters and the data written into the bulk statistics file supports the 64-bit counters.
policy	Statistics associated with a specified policy, a policy type, or traffic tagged by a policy with a color tag.
system	Global system and per-module statistics and information. The global system statistics retrieved are the sysUpTime and nvsUtilPct. The per-module statistics and information retrieved include the intPhysicalDesc, the cpuUtilPct, and the memUtilPct.

igmp Objects

Table 26 presents igmp objects you can configure using the **bulkstats schema subtree** command.

Table 26: Schema igmp Objects

Object	Definition
all	Configure IGMP schema for all attributes
dest-address	Configure IGMP schema for destination address
igmp-cmd	Configure IGMP schema for IGMP command
lower-interface	Configure IGMP schema for lower interface
multicast-group	Configure IGMP schema for multicast group
router-index	Configure IGMP schema for router index
source-address	Configure IGMP schema for source address
time-stamp	Configure IGMP schema for time stamp

if-stats Objects

Table 27 presents if-stats objects you can configure using the **bulkstats schema subtree** command.

Table 27: Schema ifStats Objects

Object	Definition
all	Configure IfStats schema for all stats
correlator	Configure IfStats schema for correlator
in-bcast-pkts	Configure IfStats schema for in-bcast-pkts
in-discards	Configure IfStats schema for in-discards
in-errors	Configure IfStats schema for in-errors
in-mcast-octets	Configure IfStats schema for in-mcast-octets
in-mcast-pkts	Configure IfStats schema for in-mcast-pkts
in-octets	Configure IfStats schema for in-octets
in-policed-octets	Configure IfStats schema for in-policed-octets
in-policed-pkts	Configure IfStats schema for in-policed-pkts
in-spoofed-pkts	Configure IfStats schema for in-spoofed-pkts
in-ucast-pkts	Configure IfStats schema for in-ucast-pkts
in-unknown-protos	Configure IfStats schema for in-unknown-protos
lower-interface	Configure IfStats schema for lower-interface
out-bcast-pkts	Configure IfStats schema for out-bcast-pkts
out-discards	Configure IfStats schema for out-discards
out-errors	Configure IfStats schema for out-errors
out-mcast-octets	Configure IfStats schema for out-mcast-octets
out-mcast-pkts	Configure IfStats schema for out-mcast-pkts
out-octets	Configure IfStats schema for out-octets
out-policed-octets	Configure IfStats schema for out-policed-octets
out-policed-pkts	Configure IfStats schema for out-policed-pkts
out-sched-octets	Configure IfStats schema for out-sched-octets
out-sched-pkts	Configure IfStats schema for out-sched-pkts
out-ucast-pkts	Configure IfStats schema for out-ucast-pkts
time-offset	Configure IfStats schema for time-offset

All the schema if-stats objects in Table 27 apply to both layer 2 and layer 3 interfaces, except usdAcctngSpoofedPkts, which is specific to layer 3.

Defining all interface types before you map a collector to the if-stats schema ensures that you display statistics for all configured interfaces in the first interval.

You can get more accurate rate statistics by using the **time-offset** parameter. To use this parameter you must navigate to the **if-stats subtreelist**. The **time-offset** parameter is included in each bulk statistics interface record and is the offset from the master interval at which the record was collected.

policy Objects

Table 28 presents policy objects you can configure using the **bulkstats schema subtree** command.

Table 28: Schema Policy Objects

Object	Definition
all	Configure policy schema for all statistics
green-bytes	Configure policy schema for green bytes
green-packets	Configure policy schema for green packets
red-bytes	Configure policy schema for red bytes
red-packets	Configure policy schema for red packets
upper-green-bytes	Configure policy schema for upper green bytes
upper-green-packets	Configure policy schema for upper green packets
upper-red-bytes	Configure policy schema for upper red bytes
upper-red-packets	Configure policy schema for upper red packets
upper-yellow-bytes	Configure policy schema for upper yellow bytes
upper-yellow-packets	Configure policy schema for upper yellow packets
yellow-bytes	Configure policy schema for yellow bytes
yellow-packets	Configure policy schema for yellow packets

bulkstats schema

- Use to create the schema for collecting bulk statistics.
- Example

  host1(config)#**bulkstats schema 4**

- Use the **no** version to delete the specified schema.

NOTE: If you create a collector but there is no schema for that collector, the collector will not be active, and a schema will be created automatically for that collector to collect if-stats for all subtree attributes.

bulkstats schema subtree

- Use to set the schema for collecting data. Specify one of the following keywords:
  - **if-stack**—Retrieves the interface and interface column configuration.
  - **if-stats**—Retrieves interface usage data on sets of interface types; using the **subtreelist** keyword along with the **if-stats** keyword lets you specify specific counters and lets you set the **time-offset** parameter; using the **if-create-delete-time-stats** keyword along with the **if-stats** keyword retrieves interface final statistics (interface statistics that may be lost during higher create or delete frequency) on a per-interface basis.
  - **igmp**—Retrieves IGMP usage data; using the **subtreelist** keyword along with the **igmplist** keyword lets you obtain statistics for one or more specific IGMP lists.
  - **policy**—Retrieves policy usage data.
  - **system**—Retrieves global system and per-module statistics and information.
- Example 1

  host1(config)#**bulkstats schema 1 subtree if-stats subtreelist lower-interface**

- Example 2

  host1(config)#**bulkstats schema 5 subtree if-stats if-create-delete-time-stats interfaceType ?**

```
atm1483     Configure bulkstats for ATM 1483 sub-interfaces
ip          Configure bulkstats for IP interfaces
mplsL2Shim  Configure bulkstats for MPLS shim Interfaces
mplsMajor   Configure bulkstats for MPLS major Interfaces
mplsMinor   Configure bulkstats for MPLS minor Interfaces
ppp         Configure bulkstats for PPP interfaces
vlan        Configure bulkstats for VLAN Sub-Interfaces
```

- Use to collect statistics on a specified policy, a policy type, or based on color-coded tags applied by a policy. Specify one of the following keywords:
  - **policy-name—**Collects statistics for a specified policy
  - **policy-type**—Collects data on input policies, local input policies, output policies, or secondary output policies
  - **policy-subtreelist**—Collects statistics based on color-coded tags applied by a policy
- You create policies using the **policy-list** command. See *JUNOSe Policy Management Configuration Guide, Chapter 1, Managing Policies on the E-series Router*.
- Example

  host1(config)#**bulkstats schema 4 subtree policy policy-name XMYpolicy**

- Use the **no** version to delete the specified schema.

Monitoring Schema Statistics

You are able to display your configuration and monitor the data generated by schemas.

show bulkstats schema

- Use to display data on the bulk statistics schema.
- Field descriptions
  - Schema Information:
  - Index—Index number of the schema
  - Subtree—Type of bulk statistics schema configured on the collector: igmp, if-stack, if-stats, policy, or system
  - CollectorIndex—Bulk statistics collector index (same as the SNMP table index)
  - State
    - active—Schema is properly configured and currently active
    - notInService—Schema has been decommissioned by a management client
    - notReady—Schema does not have enough configuration information to go active
    - error—Configuration/operational error
  - Subtree List—Type(s) of statistics the schema is configured to receive
- Example 1

```
host1#show bulkstats schema

  Schema Information:
  Index  Subtree            CollectorIndex  State
  -----  -----------------  --------------  --------
  1      ifStack            1               active
  2      system             2               active

  Index  Subtree List
  -----  ------------------------------------------------
  1      N/A
  2      N/A
```

- Example 2

```
host1#show bulkstats schema

  Schema Information:
  Index  Subtree            CollectorIndex  State
  -----  -----------------  --------------  --------
  1      ifStats            1               active
  2      system             2               active

  Index  Subtree List
  -----  ------------------------------------------------
  1      ifOutErrors; ifLowerInterface; ifTimeOffset
  2      N/A
```

Configuring Interface Numbering Mode

E-series routers support the RFC 1213 interface numbering mode on bulkstats. This mode is contrasted with the default interface numbering mode.

The RFC 1213 numbering mode is based on a 32-bit contiguous integer value starting from 1 and ranging to ifNumber. This mode differs from the default interface numbering mode, which encodes a type field in the upper 8 bits of a 32-bit integer. The use of the upper 8 bits creates large gaps in the ifIndex numbering scheme.

There is no re-use of ifIndex values in RFC 1213 mode, whereas in the default interface numbering mode, ifIndex values can be re-used. In the default interface numbering mode, re-use of ifIndex values across reboots is permitted and is basically known as ifIndex re-numbering.

In RFC 1213 mode, however, the interface numbers are not re-used during a single initialization of the device and renumbering of ifIndexes occurs after a system reboot. In the default interface numbering mode, ifIndexes are persistent across system reboots and can be reused without resetting the value of sysUpTime.

In RFC 1213 mode, two parameters control the size of the ifIndex range and the total number of interfaces in the standard interface tables—maxIfIndex and maxIfNumber. There is no such control in the default interface numbering mode.

In RFC 1213 mode, interface creations should not result in gaps in the ifIndex range. A gap that results from the deletion of an interface is acceptable because it is handled by older network management applications. The gaps are eliminated after the router is rebooted. However, in the default interface numbering mode, large gaps occur from the creation of interfaces due to the use of the upper 8 bits of the ifIndex for interface type encoding. Gaps are not eliminated after a system reboot.

In RFC 1213 mode, small gaps can occur in the creation of IP interfaces when virtual routers are used. These gaps are minimized but not eliminated when the router is rebooted.

Rather than seeing an ifIndex value of 1 and 10066329, for example, a management client would see ifIndex values of 1 and 2.

bulkstats interfaces rfc1213

- Use to enable the RFC 1213 interface numbering mode on bulkstats.
- Example

  host1(config)#**bulkstats interfaces rfc 1213**

- Use the **no** version to disable the RFC 1213 interface numbering mode on bulkstats.

Using the Bulk Statistics Formatter

The bulk statistics formatter allows you to set a remote filename dynamically and specify the format for the end of each line in the bulkstats file.

Setting Remote Filenames

The router supports the following special characters for remote filenames:

- %x—An integer in hexadecimal format (base 16)
- %s—A character string
- %u—An unsigned integer in decimal (base 10)
- %d—An integer in decimal (base 10)

The % variables in the remote name are replaced at runtime with the sysName and sysUpTime parameters to produce variable filenames on the remote host.

See the **bulkstats receiver remote-name** command.

```
host1(config)#bulkstats receiver 1 remote-name “bulk%s%d.sts” sysName
collectorSequence
```

Guidelines

The current capabilities and limitations of the bulk statistics formatter are:

- If you add %d or any numeric formatter for a string value (such as sysName), the attribute name will be used (for instance, sysName). The opposite is also true, except for sysUptime, which will use %s as a %u.
- You can use %% if you want a % character to be part of the parsed name.
- You can use the same attribute multiple times. For example, you may want a name that has %x and %u of collectorSequence.
- Currently, there is no control over sequence numbers, except for the guarantee that the formatter will:
  1. Use sequential values, beginning from 1
  2. Persist through system reboot
- If you need the sequential number to restart, remove and then add the bulk statistics receiver again.
- You can use up to 128 characters for the remote file name. Anything beyond that is truncated when the filename is stored in nonvolatile memory, but this truncation is not visible until the next time the system reboots.

Specifying End of Line Format

By default, the bulk statistics application generates a DOS-compatible file that contains both a carriage return (CR) and line feed (LF) at the end of each line. The existence of a carriage return at the end of a line may cause formatting issues with some applications that do not ignore or remove carriage returns.

You can set up the system to remove the carriage return and leave only a line feed at the end of each line.

bulkstats file-format endOfLine-LF

- Use to strip the carriage return from the end of each line in the bulkstats file.
- Example

  host1(config)#**bulkstats file-format endOfLine-LF**

- Use the **no** version to return to the default, CR and LF.

Managing Virtual Routers

Your router supports SNMP management of virtual routers. This support is based on an SNMP community string proxy to select particular instances of virtual routers. The entity MIB is used to model the physical container to the logical relationship of the virtual router implementation. See *Chapter 13, Configuring Virtual Routers*.

Monitoring SNMP

To monitor the status of SNMP operations on your network, enter Privileged Exec mode. You can then establish a baseline and use the **show** commands to view statistics.

Establishing a Baseline

SNMP statistics are stored in system counters. The only way to reset the system counters is to reboot the router. You can, however, establish a baseline for SNMP statistics by setting a group of reference counters to zero.

baseline snmp

- Use to establish a baseline for SNMP statistics.
- The system 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.
- To display statistics relative to the current baseline, use the **delta** keyword with SNMP **show** commands.
- SNMP operations (such as Get and Set) continue to use and report statistics from the system counters.
- See *Viewing SNMP Status* on page 205 for a sample display when you enter the **show snmp** command. If you establish a baseline and then enter **show snmp**, the statistics now have zero or low values.

- Example

```
host1#baseline snmp
host1#show snmp
Contact: Joe Administrator
Location: Network Lab, Bldg 3 Floor 1
2 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    1 Get-request PDUs
    1 Get-next PDUs
    0 Set-request PDUs
    0 Unknown security models
    0 Unavailable contexts
2 SNMP packets out
    0 Too big errors (Maximum packet size 1500)
    1 No such name errors
    0 Bad values errors
    0 General errors
    2 Get-response PDUs
    0 SNMP trap PDUs
    0 Invalid Message Report PDUs
    0 Unknown PDU Handler Report PDUs
    0 Unknown Context Report PDUs
    0 Unsupported Security Level Report PDUs
    0 Not in time Window Report PDUs
    0 Unknown Username Report PDUs
    0 Unknown Engine ID Report PDUs
    0 Wrong Digest Report PDUs
    0 Decryption Error Report PDUs
```

- There is no **no** version.

Viewing SNMP Status

To view SNMP status on your network, use the following **show** commands.

show snmp

- Use to display all the information about SNMP status.
- To display statistics relative to the current baseline, use the **delta** keyword.
- Field descriptions
  - Contact—Router's contact person
  - Location—Router's location
  - SNMP packets input—Total number of SNMP packets received by the router
    - Bad SNMP version errors—Number of SNMP PDUs with a bad version number
    - Unknown community name—Number of SNMP PDUs that had an unrecognized community name
    - Illegal operation for community name supplied—Number of access violations based on the configured privilege level for community strings

- Encoding errors—Number of AS number version 1 encoding and decoding errors
- Number of requested variables—Number of variable bindings processed by the SNMP agent
- Number of altered variables—Number of variable bindings processed successfully in SNMP **set** commands
- Get-request PDUs—Number of get-exact SNMP PDUs processed
- Get-next PDUs—Number of get-next SNMP PDUs processed
- Set-request PDUs—Number of set SNMP PDUs processed
- Unknown security models—Number of SNMP PDUs with unrecognized security
- Unavailable contexts—Number of SNMP proxy requests to unknown entities

- SNMP packets out—Total number of SNMP packets sent by the router
  - Too big errors—Number of processed PDUs that resulted in SNMP PDUs too large to encode
  - No such name errors—Number of requests that resulted in noSuchName errors. If interfaces configured on modules that do not support 64-bit counters are accessed, the system returns a noSuchName message.
  - Bad values errors—Number of requests that resulted in badValues errors
  - General errors—Number of general errors
  - Get-response PDUs—Number of requests that resulted in getResponse PDUs
  - SNMP trap PDUs—Number of SNMP trap PDUs generated by this agent
  - SNMP trap proxied—Number of traps generated by this agent that are sent via trap-proxy
  - Invalid Message Report PDUs—Number of packets received by the SNMP engine that were dropped because there were invalid or inconsistent components in the SNMP message
  - Unknown PDU Handler Report PDUs—Number of packets received by the SNMP engine that were dropped because the PDU in the packet could not be passed to an application responsible for handling the PDU type; for example, no SNMP application had registered for the proper combination of the context engine ID and PDU type
  - Unknown Context Report PDUs—Number of packets received by the SNMP engine that were dropped because the context contained in the message was unknown
  - Unsupported Security Level Report PDUs—Number of packets received by the SNMP engine that were dropped because they requested a security level that was unknown to the SNMP engine or otherwise unavailable

- Not in time Window Report PDUs—Number of packets received by the SNMP engine that were dropped because they appeared outside the authoritative SNMP engine window
- Unknown Username Report PDUs—Number of packets received by the SNMP engine that were dropped because they referenced a user that was not known to the SNMP engine
- Unknown Engine ID Report PDUs—Number of packets received by the SNMP engine that were dropped because they referenced an snmpEngineID that was not known to the SNMP engine
- Wrong Digest Report PDUs—Number of packets received by the SNMP engine that were dropped because they did not contain the expected digest value
- Decryption Error Report PDUs—Number of packets received by the SNMP engine that were dropped because they could not be decrypted

- Example

```
host1#show snmp
Contact: Joe Administrator
Location: Network Lab, Bldg 3 Floor 1
538 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    695 Number of requested variables
    0 Number of altered variables
    26 Get-request PDUs
    512 Get-next PDUs
    0 Set-request PDUs
    0 Unknown security models
    0 Unavailable contexts
538 SNMP packets out
    0 Too big errors (Maximum packet size 1500)
    10 No such name errors
    0 Bad values errors
    0 General errors
    538 Get-response PDUs
    0 SNMP trap PDUs
    0 Invalid Message Report PDUs
    0 Unknown PDU Handler Report PDUs
    0 Unknown Context Report PDUs
    0 Unsupported Security Level Report PDUs
    0 Not in time Window Report PDUs
    0 Unknown Username Report PDUs
    0 Unknown Engine ID Report PDUs
    0 Wrong Digest Report PDUs
    0 Decryption Error Report PDUs
```

show snmp access

- Use to display information about the groups you configured.
- Field descriptions
  - Group Name—Name of the group
  - Model—Security model; for example, user-based security model (USM)
  - Level—Method for authentication and privacy
    - none—No authentication and no privacy
    - auth—Authentication only
    - priv—Authentication and privacy
  - Read—Name of the view for read access
  - Write—Name of the view for write access
  - Notify—Name of the view for notification
  - Storage—SNMP storage type, volatile or nonvolatile
- Example

```
host1#show snmp access
Group Name          Model  Level  Read         Write        Notify
------------------  -----  -----  -----------  -----------  ---------
admin               usm    priv   everything   everything   everything
mirror              usm    priv   mirrorAdmin  mirrorAdmin  mirrorAdmin
public              usm    none   user         none         none
private             usm    auth   user         user         user
```

show snmp community

- Use to display information about the SNMP communities.
- Field descriptions
  - Community—Name of the community and the associated virtual router
  - View—Name of the view
  - Priv—Access privilege for the view
    - ro—Read-only access
    - rw—Read-write access
    - admin—All privileges
  - AccList—Number of access lists associated with this community
- Example

```
host1#show snmp community

Community                    View           Priv  AccList
-------------------------------------------  ----  -------
admin@default                everything     rw          0
private@default              user           rw          0
public@default               user           ro          0
```

show snmp group

- Use to display the list of available groups. Detailed information is available through the **show snmp access** command.
- Field descriptions
  - groupName—Name of the group
  - *securityModel*—SNMP security model
    - v1—SNMPv1
    - v2c—SNMPv2c
    - usm—SNMPv
  - authenticationLevel—Method for authentication and privacy
    - none—No authentication and no privacy
    - auth—Authentication only
    - priv—Authentication and privacy
  - readView—Name of the view for read access
  - writeView—Name of the view for write access
  - notifyView—Name of the view for notification
  - storageType—SNMP storage type
    - volatile—Loses contents when power is lost
    - nonVolatile—Does not lose contents when power is lost
- Example

```
host1#show snmp group
Group Name                                Storage Type
----------------------------------------  ---------------
group1                                    Volatile
group2                                    NonVolatile
admin                                     Permanent
mirror                                    Permanent
public                                    Permanent
private                                   Permanent
```

show snmp notificationLog

- Use to display the configuration of the SNMP notification log.
- Field descriptions
  - Global Age Out Value—Ageout for traps in the notification log tables
  - Global Entry Limit Value—Maximum number of notifications kept in all notification log tables
- Example

```
host1#show snmp notificationLog
Global Age Out Value:      1440 minutes
Global Entry Limit Value : 500
No notification log name information is available
```

show snmp trap

- Use to display configuration information about SNMP traps and trap destinations.
- Field descriptions
  - Enabled Categories—Trap categories that are enabled on the router
  - SNMP authentication failure trap—Enabled or disabled
  - Trap Source—Interface whose IP address is used as the source address for all SNMP traps
  - Trap Source Address—IP address used as the source address for all SNMP traps
  - Trap Proxy—Enabled or disabled
  - Global Trap Severity Level—Global severity level filter; if a trap does not meet this severity level, it is discarded
  - Address—IP address of the trap recipient
  - Security String—Name of the SNMP community
  - Ver—SNMP version (v1 or v2) of the SNMP trap packet
  - Port—UDP port on which the trap recipient accepts traps
  - Trap Categories—Types of traps that the trap recipient can receive
  - TrapSeverityFilter—Severity level filter for this SNMP host
  - Ping TimeOut—Configured ping timeout in minutes
  - Maximum QueueSize—Maximum number of traps to be kept in the trap queue
  - Queue DrainRate—Maximum number of traps per second to be sent to the host
  - Queue Full discard method—Method used to discard traps when the queue is full:
    - dropFirstIn—Oldest trap in the queue is dropped
    - dropLastIn—Most recent trap is dropped
- Example

```
host1#show snmp trap

Enabled Categories: Ping, TraceRoute
SNMP authentication failure trap is disabled
Trap Source: FastEthernet 0/0, Trap Source Address:10.10.5.61
Trap Proxy: disabled
Global Trap Severity Level: 6 - informational

Address          Security String                   Ver  Port   Trap Categories
---------------  --------------------------------  ---  -----  ----------------
10.10.0.200       private                           v2c 162
SnmpLinkInvEnvBstFxfBgpLogCliPingOspfTraceDvmrpDvmrpUniAdrPAtmPingVrrpSonetNtp


Address         TrapSeverityFilter  Ping    Maximum    Queue    Queue Full
                                   TimeOut QueueSize DrainRate discrd methd
--------------- ------------------ ------- --------- --------- -------------
10.10.0.200      5 - notice         1       32        0         dropLastIn
```

show snmp trap statistics

- Use to display statistics for all SNMP traps on the virtual router, as well as statistics for each SNMP host configured on the virtual router.
- Field descriptions
  - Trap request(s)—Number of local traps requested
  - Proxy trap request(s)—Number of proxy traps requested
  - Trap(s) discarded—Total number of traps discarded
    - No system memory—Traps discarded because there was not enough system memory
    - No queue resources—Traps discarded because there were no queue resources available
    - SNMP agent disabled—Traps discarded because the SNMP agent was disabled
    - Global trap category disabled—Traps discarded because they were filtered by the **snmp enable trap** command
    - Global minimum severity level—Traps discarded because they did not match the severity level set with the **snmp enable traps trapfilters** command.
  - Trap(s) out—Total number of traps sent by the virtual router
  - Trap(s) proxied—Total number of traps proxied by the virtual router
  - Address—IP address of the host
  - TrapsDiscarded Severity/Category—Severity level and category of the discarded traps
  - TrapsDiscrded bad encoding—Traps discarded because of bad encoding
  - TrapsDiscrded Queue Full—Traps discarded because the queue was full
  - TrapsDiscrded NoHostRespons—Traps discarded because the host did not respond to pings sent to the host
  - Trap PDUs sentOut—Number of trap PDUs sent by this host

```
host1#show snmp trap statistics
Trap request(s):3112
Proxy trap request(s):0
Trap(s) discarded:4
    No system memory:0
    No queue resources:0
    SNMP agent disabled:0
    Global trap category disabled:4
    Global minimum severity level:0
Trap(s) out:3108
Trap(s) proxied:0
Address         TrapsDiscarded    TrapsDiscrded TrapsDiscrded TrapsDiscrded
                Severity/Category bad encoding  Queue Full    NoHostRespons
--------------- ----------------- ------------- ------------- -------------
1.1.1.1         1081              0             511           32
10.10.132.137   0                 0             0             0
```

```
Address         Trap PDUs
                sentOut
--------------- ---------
1.1.1.1         536
10.10.132.137   3108
```

show snmp user

- Use to display information about users.
- Field descriptions
  - User—Name of the user
  - Auth—Authorization protocol for this user
    - no—No authorization protocol
    - md5—HMAC-MD5-96 authorization protocol
    - sha—HMAC-SHA-96 authorization protocol
  - Priv—Privacy protocol for this user
    - no—No privacy protocol
    - des—DES encryption algorithm for privacy
  - Group—Name of the group to which the user belongs
- Example SNMPv3 display.

```
host1#show snmp user

User                    Auth  Priv  Group
----------------------- ----  ----  ------------------
josie                   md5   des   admin
nightfly                md5   no    private
steelydan               no    no    public
```

show snmp view

- Use to display information about the views you created.
- Field descriptions
  - View Name—Name of the view
  - View Type—Access privilege for the view
    - included—Specified object identifier (OID) trees are available in this view
    - excluded—Specified OID trees are not available in this view
  - Oid Tree—OID of the AS number version 1 subtree
  - Storage—SNMP storage type, volatile or nonvolatile
- Example

```
host1#show snmp view

View Name       View Type  Oid Tree
--------------  ---------  --------------------------
user            included   1.3.6.1.
user            excluded   1.3.6.1.4.1.4874.2.2.16.
user            excluded   1.3.6.1.6.3.11.
user            excluded   1.3.6.1.6.3.12.
```

```
user            excluded   1.3.6.1.6.3.13.
user            excluded   1.3.6.1.6.3.14.
user            excluded   1.3.6.1.6.3.15.
user            excluded   1.3.6.1.6.3.16.
user            excluded   1.3.6.1.6.3.18.
nothing         excluded   1.3.6.1.
everything      included   1.3.6.1.
everything      excluded   1.3.6.1.4.1.4874.2.2.77.
mirrorAdmin     included   1.3.6.1.4.1.4874.2.2.77.
```

Output Filtering

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

Chapter 5

Managing the System

This chapter describes general tasks associated with managing the E-series router.

This chapter contains the following sections:

- Overview on page 216
- Platform Considerations on page 216
- Naming the System on page 217
- Configuring the Switch Fabric Bandwidth on page 217
- Configuring Timing on page 217
- Using the CLI on page 219
- Managing vty Lines on page 222
- Clearing Lines on page 224
- Monitoring the Current Configuration on page 225
- Configuring the System Automatically on page 234
- Saving the Current Configuration on page 235
- Customizing the User Interface on page 237
- Sending Messages on page 244
- Managing Memory on page 245
- Managing Files on page 245
- Transferring Files on page 254
- Configuring the NFS Client on page 269
- Using a Loopback Interface on page 271
- Using the Telnet Client on page 271

- Configuring DNS on page 272
- Troubleshooting the System on page 275
- Managing and Monitoring Resources on page 286
- Monitoring the System on page 288

Overview

Managing the E-series router involves a variety of tasks. This chapter covers those tasks associated with the router in general rather than specific networking protocols. Each section in the chapter covers a different topic; where appropriate, a section contains an overview of the topic, configuration tasks, and information about monitoring the associated settings.

For additional management information, CLI commands, and procedures, refer to the following table.

Task	Reference
Find detailed information about commands described in this chapter.	*JUNOSe Command Reference Guide A to M* and *JUNOSe Command Reference Guide N to Z*
Configure the system as an SNMP agent.	*Chapter 4, Configuring SNMP*
Set system passwords.	*Chapter 9, Passwords and Security*
Write CLI macros.	*Chapter 10, Writing CLI Macros*
Boot the system.	*Chapter 11, Booting the System*
Manage line modules and SRP modules.	*Chapter 6, Managing Modules*

Platform Considerations

System management is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 and E320 router.

Naming the System

When you receive the router, it has a factory default host name. To rename the router, use the **hostname** command.

hostname

- Use to rename the router.
- The assigned name is displayed in the command-line interface (CLI) prompts.
- Example

  router1(config)#**hostname host1**
  host1(config)#

- There is no **no** version.

Configuring the Switch Fabric Bandwidth

By default, the switch fabric for the ERX-1440, ERX-310, E120, and E320 routers uses a bandwidth weighting ratio of 15:2 for multicast-to-unicast weighted round robin (WRR). In the absence of strict-priority traffic, and when both unicast and multicast traffic compete for switch fabric bandwidth, the switch fabric allocates 15/17ths of the available bandwidth to multicast traffic and 2/17ths of the available bandwidth to unicast traffic.

The **fabric weights** command enables you to specify a ratio for multicast-to-unicast traffic on the router switch fabric. The **no** version of the command reverts the weighting ratio back to its default.

fabric weights

- Use to define the multicast-to-unicast traffic ratio for the switch fabric for the ERX-1440, ERX-310, E120, and E320 routers
- Example

  host1# **fabric weights multicast 2 unicast 1**

- Use the **no** version to return the switch fabric to its default multicast-to-unicast ratio (15:2).

Configuring Timing

You can use the **timing source** command to configure three timing sources for the system. These sources are known as the primary, secondary, and tertiary sources. The system periodically polls the status of the current timing source. If the system discovers that the current source has become unavailable, it polls the timing source you specified as next in line. If this source is available, it switches to this source; if not, it then polls the next source in line. If the lowest source is unavailable, the system maintains the SRP clock as the source.

If you enable auto-upgrade, in the event of a source failure, the system—after switching to a lower source—polls all higher configured sources and automatically switches back to the highest timing source when that source becomes available.

The **timing select** command enables you to specify which source (primary, secondary, or tertiary) the system is to use by default. The system will never attempt to upgrade to a source higher than the selected source.

timing disable-auto-upgrade

- Use to disable the auto-upgrade feature of the system's timing selector.
- The system starts out by setting the operational timing selector to the administratively configured selector. See the **timing select** command.
- Example

  host1(config)#**timing disable-auto-upgrade**

- Use the **no** version to restore the factory default, which is auto-upgrade enabled.

timing select

- Use to specify which of the configured timing sources is used by default.
- Primary timing source is preferred over secondary, and secondary is preferred over tertiary. See the **timing source** command.
- If you enable the auto-upgrade feature, the system does not try to upgrade beyond the administratively configured selector.
- Example

  host1(config)#**timing select secondary**

- There is no **no** version.

timing source

- Use to specify how the SRP module exchanges timing signals with an interface.
- You can specify primary, secondary, and tertiary timing sources.
- You can specify one external source received on an I/O module or IOA other than the SRP I/O module or SRP IOA.
- You can specify two or more internal sources or external sources received through the SRP I/O module or SRP IOA external timing ports.
- On the E120 and E320 routers, you can specify sonet for only two of the available three timing sources (primary, secondary, or tertiary).
- The available sources to choose are:
  - ds1—DS1 interface
  - ds3—DS3 interface
  - e1—E1 interface
  - e3—E3 interface
  - sonet—SONET interface
  - internal—Internal system controller (SC) oscillator
  - line—External timing input on SRP module

- Example

  host1#**timing source secondary sonet 3/0**

- There is no **no** version.

Monitoring Timing

Use the **show timing** command to view the timing settings for the system.

show timing

- Use to display the timing settings and the operational status of the system timing.
- If a timing source fails, the system uses the next time source in the hierarchy, and a message appears in the system log at the *warning* level. If auto-upgrade is enabled, the system upgrades to a higher-priority timing source when one becomes available, and a message appears in the system log at the *notice* level.
- Example

```
host1#show timing
timing: tertiary (failover from primary)
        primary: external SC E1 (A) (ERROR)
        secondary: ds3 3/0 (ERROR)
        tertiary: internal SC oscillator (ok)
        auto-upgrade enabled
```

Using the CLI

Use the commands described in this section to navigate the CLI. For a complete description of the CLI, see *Chapter 2, Command-Line Interface*.

configure

- Use to enter Global Configuration mode.
- Global Configuration mode provides access to other configuration modes, such as Interface Configuration mode. See *Chapter 2, Command-Line Interface*.
- This command allows other commands to be executed from a terminal or a file.
- This command is not allowed for a short time after a warm restart (warm switchover) occurs. This delay allows some applications time to complete their warm-restart initialization. However, if the warm restart is not complete in 5 minutes, the warm start is cancelled and configuration access is restored.
- Example 1

  host1#**configure**
  Configuring from terminal or file [terminal]?
  Enter configuration commands, one per line. End with CNTL/Z.
  host1(config)#

- Example 2

  ```
  host1#configure
  Configuring from terminal or file [terminal]? file
  File name: system1.scr
  Proceed with configure? [confirm]
  host1(config)#
  ```

- There is no **no** version.

disable

- Use to exit Privileged Exec mode and return to User Exec mode.
- Use to move to a lower Privileged Exec mode level without returning to User Exec mode. Specifying a privilege level after the **disable** command changes the Privileged Exec mode to the lower level that you specify; you do not return to User Exec mode.
- Example 1

  ```
  host1#disable
  host1>
  ```

- Example 2

  ```
  host1#show privilege
  Privilege level is 10
  host1#disable 5
  host1#show privilege
  Privilege level is 5
  ```

- There is no **no** version.

do

- Use to issue an Exec mode command from any CLI configuration command mode.
- Example

  ```
  host1(config)#do show configuration | begin interface
  ```

- The **do** command functions the same as the **run** command.
- There is no **no** version.

enable

- Use to move from User Exec to Privileged Exec mode.
- Privileged Exec mode allows you to access all other user interface modes. From here you can configure, monitor, and manage all aspects of the router.
- You can access the Privileged Exec commands using one of 16 levels of command privilege. If you do not enter a privilege level and you are not accessing the router through a RADIUS authentication account, the default CLI access level is 10. For information about CLI levels of access, see *Privileged-Level Access* in *Chapter 2, Command-Line Interface*.

- Set a password for this mode by using either the **enable password** or the **enable secret** command in Global Configuration mode. This protects the system from any unauthorized use.
- Once a password is set, anyone trying to use Privileged Exec mode will be asked to provide the password.
- Example 1 (accessing Privileged Exec mode at the default level 10)

  host1>**enable**
  password:*******
  host1#

- Example 2 (accessing Privileged Exec mode at the highest level 15; a password is not set for this example)

  host1>**enable 15**
  host1#

- There is no **no** version.

end

- Use to exit Global Configuration mode or any of the other Configuration modes. You may also use Ctrl + z to exit these modes.
- Executing this command returns you to the User Exec mode.
- Example

  host1(config)#**end**
  host1#

- There is no **no** version.

exit

- Use to exit the current command mode or the system when issued from the User Exec mode.
- Example

  host1#**exit**
  host1>

- There is no **no** version.

help

- Use to display basic information about the interactive help system.
- Example

```
host1#help
Use the help options as follows:

?, or command<Space>? - Lists the set of all valid next keywords or
                        arguments
partial-keyword?      - Lists the keywords that begin with a certain
                        character string
partial-keyword<Tab>  - Completes the partial keyword
```

- There is no **no** version.

run

- Use to issue an Exec mode command from any CLI configuration command mode.
- Example

```
host1(config)#run show configuration | begin interface
```

- The **run** command functions the same as the **do** command.
- There is no **no** version.

sleep

- Use to make the CLI pause for a specified period of time (in seconds).
- Pausing is very useful in configuration script files.
- Example

```
host1#sleep 60
```

- There is no **no** version.

Managing vty Lines

The system supports 30 virtual tty (vty) lines for Telnet, SSH, and FTP services. Each Telnet, SSH, or FTP session requires one vty line. When you connect to the router through a vty line, the number of the vty line is not assigned sequentially; instead, the system assigns the first vty line that passes the host access list check rules.

Configuring vty Lines

By default five vty lines (0–4) are open. You can open additional lines using the **line vty** command. Once lines are open, login is enabled by default. Before users can access the lines, you must configure a password, disable login using the **no login** command, or configure AAA authentication on the lines.

line vty

- Use to open or configure vty lines.
- You can specify a single line or a range of lines. The range is 0–29.
- Example

  host1(config)#**line vty 6 10**
  host1(config-line)#

- Use the **no** version to remove a vty line or a range of lines from the configuration. Lines that you remove will no longer be available for use by Telnet, FTP, or SSH. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

password

- Use to specify a password on a single line or a range of lines.
- If you enable login but do not configure a password, the system will not allow you to access virtual terminals.
- Specify a password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted.
- You can use the following keywords:
  - **0** (zero)—Specifies an unencrypted password
  - **5**—Specifies a secret
  - **7**—Specifies an encrypted password
- Example 1 (unencrypted password)

  host1(config-line)#**password 0 mypassword**

- Example 2 (secret)

  host1(config-line)#**password 5 y13_x**

- Example 3 (encrypted password)

  host1(config-line)#**password 7 x13_2**

- Use the **no** version to remove the password. By default, **no password** is specified.

For more information about configuring security for vty lines, see *Chapter 9, Passwords and Security*.

Monitoring vty Lines

Use the **show line vty** command to monitor vty lines.

show line vty

- Use to display the configuration of a vty line.
- Field descriptions
  - access-class—Access class associated with the vty line
  - data-character-bits—Number of bits per character
    - 7—Setting for the standard ASCII set
    - 8—Setting for the international character set
  - exec-timeout—Time interval that the terminal waits for expected user input
    - Never—Indicates that there is no time limit
  - exec-banner—Status for the exec banner: enabled or disabled. This banner is displayed by the CLI after user authentication (if any) and before the first prompt of a CLI session.
  - motd-banner—Status for the MOTD banner: enabled or disabled. This banner is displayed by the CLI when a connection is initiated.
  - login-timeout—Time interval during which the user must log in.
    - Never—Indicates that there is no time limit
- Example

```
host1#show line vty 0
no access-class in
data-character-bits 8
exec-timeout 3w 3d 7h 20m 0s
exec-banner enabled
motd-banner enabled
login-timeout 30 seconds
```

Clearing Lines

Use the **clear line** command to clear any line on the system (vty or console). Using this command terminates any service, such as an FTP session, on this line and closes any open files.

clear line

- Use to remove any services on a line and close any files opened as a result of services on that line.
- You can specify the absolute number to clear any line. For each line on the system, the absolute number is listed in the line number field of the **show users** command output.
- You can specify the line type and the relative number to clear a specific type of line. For each line on the system, the relative number is listed in the line name field of the **show users** command output.

- Example 1

  host1#**clear line 2**

- Example 2

  host1#**clear line console 0**

- There is no **no** version.

Monitoring the Current Configuration

Use the commands described in this section to monitor the current (running) configuration of the system.

You can use the **show configuration** command to display information when the router is in Automatic Commit mode. In Automatic Commit mode, the system automatically saves any change to the system configuration to nonvolatile storage (NVS).

You can use the **show running-configuration** command to display information when the router is in Manual Commit mode. In Manual Commit mode, any configuration change affects only the current (running) system configuration.

For more information about saving the current configuration in Automatic Commit mode or Manual Commit mode, see *Saving the Current Configuration* on page 235.

Defining the Configuration Output Format

The JUNOSe **show configuration** command displays the entire system configuration. For very large configurations, the show configuration report can take a long time to generate and display.

The **service show-config format** command enables you to run the **show configuration** command using one of two formats—original format (format 1; the default) and a format that provides a much faster output (format 2). Using format 2 can significantly reduce the amount of time it takes to generate and display configurations that contain three or more virtual routers and a large number of interfaces.

The primary difference between format 1 and format 2 output is the way in which each displays layer 2 and layer 3 interface configurations. Table 29 indicates where layer 2 and layer 3 interface configurations appear within the **show configuration** command output when the system is using format 1 or format 2.

Table 29: Output Locations for Layer 2 and Layer 3 Interface Configurations

Format	Layer 2 Only Interfaces	Layer 3 Only Interfaces	Layer 2 and Layer 3 Combination Interfaces
Format 1	Entire configuration appears in the default router output	Entire configuration appears in the layer 3 virtual router output	Layer 2 configuration appears in the default router the layer 3 virtual router output
Format 2	Entire configuration appears in the default router output	Entire configuration appears in the layer 3 virtual router output	Layer 2 configuration appears in the default router output; layer 3 configuration appears in the layer 3 virtual router output

The following examples show the differences between format 1 and format 2 output:

Example 1 Format 1 output

```
virtual-router default
…
interface null 0
interface loopback 0
 ip address 127.0.0.1 255.0.0.0
!
interface ip shAtm50126
 ip share-interface atm 5/0.126
!
interface ip MikeShare2
 ip share-interface atm 5/1.1
!
interface atm 5/0
interface atm 5/0.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/0.100.1
 encapsulation ppp
 ppp authentication chap
 ip address 102.0.1.1 255.255.255.0
!
interface atm 5/0.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
 ip address 102.0.2.1 255.255.255.0
!
interface atm 5/0.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 ip address 100.0.0.1 255.255.255.0
 pppoe
!
pppoe subinterface atm 5/0.103.1
 encapsulation ppp
 ppp authentication pap
 ip address 100.0.1.1 255.255.255.0
!
```

```
interface atm 5/0.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
 ip address 150.0.1.1 255.255.255.0
 ipv6 address 2000:0:17::1/60
!
interface atm 5/0.126 point-to-point
!
interface atm 5/1
interface atm 5/1.1 point-to-point
interface atm 5/1.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/1.100.1
 encapsulation ppp
 ppp authentication chap
!
interface atm 5/1.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
!
interface atm 5/1.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 pppoe
!
pppoe subinterface atm 5/1.103.1
 encapsulation ppp
 ppp authentication pap
!
interface atm 5/1.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
!
interface atm 5/1.125 point-to-point
!
interface fastEthernet 0/0
 ip address 10.13.5.196 255.255.128.0
!
interface mlppp joe
!
ip route 0.0.0.0 0.0.0.0 10.13.5.1
ip route 40.0.0.0 255.0.0.0 atm5/0.104
ip route 172.28.32.70 255.255.255.255 10.13.5.1
no ip source-route
!
!
ipv6
!
!
===============================================================================
virtual-router foo
…
interface null 0
interface loopback 0
 ip address 127.0.0.2 255.0.0.0
!
interface atm 5/1.100.1
 ip address 102.0.1.2 255.255.255.0
!
interface atm 5/1.102
 ip address 102.0.2.2 255.255.255.0
```

```
!
interface atm 5/1.103
 ip address 100.0.0.2 255.255.255.0
!
interface atm 5/1.103.1
 ip address 100.0.1.2 255.255.255.0
!
interface atm 5/1.104
 ip address 150.0.1.2 255.255.255.0
 ipv6 address 2000:0:17::2/60
!
ip route 30.0.0.0 255.0.0.0 atm5/1.104
no ip source-route
!
!
ipv6
```

Example 2 Format 2 output

```
service show-config format 2
…
virtual-router default
…
interface atm 5/0
interface atm 5/0.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/0.100.1
 encapsulation ppp
 ppp authentication chap
!
interface atm 5/0.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
!
interface atm 5/0.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 pppoe
!
pppoe subinterface atm 5/0.103.1
 encapsulation ppp
 ppp authentication pap
!
interface atm 5/0.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
!
interface atm 5/0.126 point-to-point
!
interface atm 5/1
interface atm 5/1.1 point-to-point
interface atm 5/1.100 point-to-point
 atm pvc 100 0 100 aal5snap 0 0 0
 encapsulation pppoe
 pppoe sessions 1
!
interface atm 5/1.100.1
 encapsulation ppp
 ppp authentication chap
```

```
!
interface atm 5/1.102 multipoint
 atm pvc 1021 0 1021 aal5snap 0 0 0
 atm pvc 1022 0 1022 aal5snap 0 0 0
 atm pvc 1023 0 1023 aal5snap 0 0 0
!
interface atm 5/1.103 point-to-point
 atm pvc 103 0 103 aal5snap 0 0 0
 encapsulation bridge1483
 pppoe
!
pppoe subinterface atm 5/1.103.1
 encapsulation ppp
 ppp authentication pap
!
interface atm 5/1.104 point-to-point
 atm pvc 104 0 104 aal5snap 0 0 0
!
interface atm 5/1.125 point-to-point
!
interface fastEthernet 0/0
interface null 0
interface loopback 0
 ip address 127.0.0.1 255.0.0.0
!
interface ip shAtm50126
 ip share-interface atm 5/0.126
!
interface ip MikeShare2
 ip share-interface atm 5/1.1
!
interface mlppp joe
interface fastEthernet 0/0
 ip address 10.13.5.196 255.255.128.0
!
interface atm 5/0.100.1
 ip address 102.0.1.1 255.255.255.0
!
interface atm 5/0.102
 ip address 102.0.2.1 255.255.255.0
!
interface atm 5/0.103
 ip address 100.0.0.1 255.255.255.0
!
interface atm 5/0.103.1
 ip address 100.0.1.1 255.255.255.0
!
interface atm 5/0.104
 ip address 150.0.1.1 255.255.255.0
 ipv6 address 2000:0:17::1/60
!
ip route 0.0.0.0 0.0.0.0 10.13.5.1
ip route 40.0.0.0 255.0.0.0 atm5/0.104
ip route 172.28.32.70 255.255.255.255 10.13.5.1
no ip source-route
!
!
ipv6
!
```

```
!
================================================================================
virtual-router foo
…
interface null 0
interface loopback 0
 ip address 127.0.0.2 255.0.0.0
!
interface atm 5/1.100.1
 ip address 102.0.1.2 255.255.255.0
!
interface atm 5/1.102
 ip address 102.0.2.2 255.255.255.0
!
interface atm 5/1.103
 ip address 100.0.0.2 255.255.255.0
!
interface atm 5/1.103.1
 ip address 100.0.1.2 255.255.255.0
!
interface atm 5/1.104
 ip address 150.0.1.2 255.255.255.0
 ipv6 address 2000:0:17::2/60
!
ip route 30.0.0.0 255.0.0.0 atm5/1.104
no ip source-route
!
```

Customizing the Configuration Output

You can customize the configuration information by including or excluding lines of output based on the keywords described in this section.

Using a keyword with the **show configuration** command might be more effective than using **show configuration | begin**. When **show configuration** is used with a specific keyword, the current configuration is quickly determined and displayed for *only* that specified keyword. Executing **show configuration | begin** causes all output of **show configuration** to be generated, but the output is not displayed until the **begin** criterion is met.

Use the **virtual-router** keyword to display the current configuration of a specified virtual router. You can combine the **virtual-router** keyword with the **category** keyword to display the current configuration of specific settings for a virtual router.

Use the **interface** keyword to display the current configuration of a particular interface. Use the **type** keyword to target specific interface types. You can exclude information about particular types of interfaces using the **exclude-category interface** keyword.You can exclude information about particular types of interfaces using the **exclude-category interface** keyword.

Use the **category** keyword to display the current configuration of a specific group of router settings. The settings are organized in categories by function.

Use the **tag-group** keyword with the **category interfaces** keywords to tag interfaces as belonging to a specific group and display all interfaces within a group.

Use the **tag-group** command to configure an interface tag group. Any number of interfaces can be in a tag group. The following interface types cannot be added to tag groups: tunnel, lag, mlppp, and mlframe-relay. An interface can be in only one tag group.

Table 30 describes the categories of router settings and the type of information displayed for each category.

Table 30: Categories of Router Settings

Category	Configuration Displayed
aaa	Authentication, authorization, and accounting (AAA) settings, such as the default authentication protocol and the RADIUS accounting server
address-assignment	Address assignment settings for Dynamic Host Configuration Protocol (DHCP) and the local address server
flow-management	Flow management settings, such as firewalls, Network Address Translation (NAT), and IP flow statistics
interfaces	Physical interfaces (types and specifiers); this is the only category that displays information about interfaces
ip-protocols	Internet protocols, such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF)
link-layer-forwarding	Link-layer settings, such as bridged interfaces and link-layer interface types
management	Router management settings, such as the CLI, bulk statistics, and Telnet
physical-layer-protocols	Physical layer protocols, such as DS1, DS3, and SONET/SDH
policy	Policy settings, such as policy lists, classifier groups, and rate-limit profiles
qos	Quality of service (QoS) settings, such as traffic class, drop profile, and scheduler profile
system	System-level settings, such as timing, logging, and redundancy
tunneling	Tunneling protocols, such as IP Security (IPSec), Multiprotocol Label Switching (MPLS), and Layer Two Tunneling Protocol (L2TP)

Many of the categories described in Table 30 contain subcategories of router settings. For example, you can specify **show configuration category management cli** to display only the configuration for the CLI. To display the names of subcategories that you can specify for each category, issue the **show configuration category *categoryName* ?** command.

You can combine the **category** keyword with the **virtual-router** keyword to display the current configuration of specific settings for a virtual router.

NOTE: When you specify categories with the **show configuration** command, the output might display additional configuration data that is not explicitly associated with the categories that you specified.

service show-config

- Use to define the **show configuration** command display output.
- Specify format 1 to display the show configuration command output in its original format.
- Specify format 2 to significantly reduce the amount of time it takes to generate and display output for configurations that contain three or more virtual routers and a large number of interfaces.
- Example

  host1#**service show-config format 2**

- Use the **no** version to revert the **show configuration** command output format to its default (format 1).

show configuration

- Use to display the current configuration of the system, a specified virtual router, a specified interface, or a specified category of router settings.
- This command was formerly documented as **show config**; that abbreviation is still supported.
- You can create a configuration script from the output by saving it as a file with the .scr extension.
- This command provides configuration information based on the privilege level of the session (user). The output does not display any configuration data for commands that have privilege levels higher than that of the session. For example, if the session is enabled at level 5, issuing the **show configuration** command displays only output for commands at level 5 and below. For more information, see *CLI Command Privileges* on page 50.
- 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 *Chapter 2, Command-Line Interface*, for details.
- Example

```
host1#show configuration
! Configuration script being generated on TUE JAN 29 200X 00:31:12 UTC! Juniper Networks Edge Routing
Switch ERX-700
! Version: x.y.z (January 18, 200X 15:01)
! Copyright (c) 1999-200X Juniper Networks, Inc. All rights reserved.

Commands displayed are limited to those available at privilege level 10

! Juniper Networks Edge Routing Switch ERX-700
boot config running-configuration
boot system erx_x-y-z.rel
no boot backup
no boot subsystem
no boot backup subsystem
no boot force-backup
!
! Note:  The following commands are here to ensure that all virtual routers and
! vrfs are created before other commands that may need to reference them.
! These commands will be repeated further on as each virtual router and vrf
! has its configuration presented.
!
virtual-router default
```

```
virtual-router boston
!
ip vrf vpna
virtual-router vrA
!
hostname host1
exception protocol ftp anonymous null
!
controller t1 6/0
 channel-group 2 timeslots 1,3-8,10 speed 64

.
.
.
!
virtual-router vrA
aaa authentication ppp default radius
aaa accounting ppp default radius
!
ip address-pool local
interface null 0
ip bgp-community new-format
no ip source-route
!
snmp-server
!
! End of generated configuration script.
```

Example using **interface** keyword:

```
host1#show configuration interface serial 4/0
interface atm 4/0
 atm vc-per-vp 1024
 atm uni-version 3.0
!
interface atm 4/0.1 point-to-point
 profile pppoe myProfile
 qos-profile myQosProfile
!
interface atm 4/0.2 point-to-point
 qos-profile myQosProfile
 ip description TestIP
!
interface atm 4/0.3 point-to-point
```

Example using **category** keyword:

```
host1#show configuration category system file-system
boot config running-configuration
boot system m.rel
no boot backup
no boot subsystem
no boot backup subsystem
```

show running-configuration

- Use to display the configuration currently running on the router, a specified virtual router, a specified interface, or a specified category of router settings.
- Example

  host1#**show running-configuration**

- Example 2

  host1#**show running-configuration interface serial 4/0**

- Example 3

  host1#**show running-configuration category system file-system**

tag-group

- Use to configure an interface tag group.
- Any number of interfaces can be in a tag group.
- Interface types tunnel, lag, mlppp, and mlframe-relay cannot be added to tag groups.
- An interface can be in only one tag group.
- Example

  host1(config-if)#**tag-group red**

- Use the **no** version to remove the tag group.

Configuring the System Automatically

You can create an autoconfiguration script that runs whenever you reset the router. The following guidelines apply:

- You must name the script autocfg.scr.
- Add the commands desired to configure the system.
- For some configuration tasks, you might need to pause the CLI for about 10 seconds by adding a **sleep** *seconds* command. The exact period must be determined empirically because it depends on your configuration and the software release version.

NOTE: The autocfg.scr script is bypassed if you arm the system to load from a script (not autocfg.scr) through the **boot config** command or **boot backup** command.

Saving the Current Configuration

By default, the system automatically saves any change to the system configuration to nonvolatile storage (NVS). This feature is known as Automatic Commit mode, but has no effect on the CLI prompt. For more information about displaying the current configuration of the system while in Automatic Commit mode, see **show configuration** on page 232.

You can disable this feature by issuing the **service manual-commit** command. In Manual Commit mode (again with no effect on the CLI prompt), any configuration change affects only the current system configuration (the running configuration). For more information about displaying the running configuration of the system while in Manual Commit mode, see **show running-configuration** on page 234.

If you are in Manual Commit mode and want to save the configuration changes to NVS, you must issue either the **write memory** command or the **copy running-configuration startup-configuration** command.

If you change the configuration while in Manual Commit mode and issue the **reload** command without saving the changes to the startup configuration, the system provides a warning, allowing you to save the changes before reloading.

You can use the **include-text-config** keyword with the **copy running-configuration** command to add the text configuration to the system configuration file. If you change from commit mode to manual-commit mode, the configuration that is available at that point in time is written into the .cnf file. A Perl script is provided in the Tools folder on the *E-series System Software* CD shipped with your router that enables you to view the text configuration in a configuration file that contains both binary and text configuration. The Perl script supports multiple platforms. The UsageExtractScrFromCnf.txt file provides an explanation of how to extract the system configuration file, using the extractScrFromCnf.pl script.

NOTE: To avoid any discrepancies between the text-generated file and the system configuration file, do not change the configuration when the **copy running-configuration** command is running.

copy running-configuration

- Use to save the current configuration to a system configuration (*.cnf) file.
- Use the **include-text-config** keyword to add the text configuration to the system configuration file.
- This command is available only if the system is in Automatic Commit mode.
- The destination filename must have a .cnf extension.
- The destination file can be either a local or a network file.
- If you want to restore a previously saved configuration, use the **boot config** *cnfFileName* command.

- Example

  host1#**copy running-configuration system2.cnf**

- There is no **no** version.

copy running-configuration startup-configuration

- Use to save all outstanding (unsaved) configuration changes to NVS.
- This command is an exact alias of the **write memory** command.
- This command is available if the system is in either Automatic Commit mode or Manual Commit mode. If issued while in Automatic Commit mode, the CLI notifies you that the command is not necessary, but allows you to proceed.
- If automatic synchronization between the primary and standby SRP modules is enabled (the default system behavior) and the system is in Manual Commit mode (the nondefault system behavior), issuing this command triggers file system synchronization immediately after the system writes, or commits, all outstanding configuration changes to NVS.
- This command is prevented during the high availability initialization state. If issued during this state, the CLI notifies you of the state and requests that you try again later.
- Example

  host1#**copy running-configuration startup-configuration**

- There is no **no** version.

copy startup-configuration

- Use to copy the previously saved startup configuration to a system configuration (*.cnf) file. If you have made but not saved any configuration changes, those changes are not in the startup configuration.
- This command is available only if the system is in Manual Commit mode.
- Example

  host1#**copy startup-configuration system1.cnf**

- There is no **no** version.

service manual-commit

- Use to stop the system from automatically saving configuration changes to NVS.
- Issuing this command places the system into Manual Commit mode. This mode has no effect on the CLI prompt.
- Issuing this command causes an immediate save of configuration data not yet committed to NVS.
- If issued when high availability is initializing, the CLI notifies you of the state and requests that you try again later.

- Example

  host1(config)#**service manual-commit**

- The **no** version returns the system to Automatic Commit mode; the **no** version has no effect if the system is already in Automatic Commit mode.

write memory

- Use to save all outstanding (unsaved) configuration changes to NVS.
- This command is an exact alias of the **copy running-configuration startup-configuration** command.
- This command is available if the router is in either Automatic Commit mode or Manual Commit mode. If issued while in Automatic Commit mode, the CLI notifies you that the command is not necessary, but allows you to proceed.
- If automatic synchronization between the primary and standby SRP modules is enabled (the default system behavior) and the system is in Manual Commit mode (the nondefault system behavior), issuing this command triggers file system synchronization immediately after the system writes, or commits, all outstanding configuration changes to NVS.
- Example

  host1#**write memory**

- There is no **no** version.

Customizing the User Interface

You can access the CLI through a console connected directly to the system or through a Telnet session. This section describes how you can customize the user interface. Some commands apply to the console, and some commands apply to vty lines that support Telnet sessions.

Setting the Console Speed

You can specify the console speed for only the current console session or for the current console session and all subsequent console sessions.

speed

- Use to set the speed for the current and all subsequent console sessions immediately.
- Example

  host1(config)#**line console 0**
  host1(config-line)#**speed 14400**

- Use the **no** version to revert to the default, 9600 bps.

terminal speed

- Use to set the speed for the current console session.
- Example

  host1#**terminal speed 14400**

- There is no **no** version.

Configuring the Display Terminal

You can specify the number of lines that appear on a terminal screen and the number of characters that appear on a line.

terminal length

- Use to set the number of lines on a screen.
- If a command generates more lines than the number configured, the output pauses after each screen.
- Set the number of lines on a screen in the range 0–512.
- Use 0 for no pausing.
- Example

  host1#**terminal length 25**

- There is no **no** version.

terminal width

- Use to set the width of the display terminal.
- Set the number of characters on a screen line in the range 30–512.
- Example

  host1#**terminal width 80**

- There is no **no** version.

Specifying the Character Set

You can specify the number of data bits per character for the current vty session and for all subsequent sessions on the specified vty lines. This feature allows you to display international characters on the terminal's screen.

data-character-bits

- Use to set the number of bits per character on the terminal's screen for all future sessions on the specified lines.
- Use the default setting, 8, to view the full set of 8-bit international characters. Be sure that the software on other devices in the network also supports international characters.
- Set the number of bits to 7 to view only characters in the standard ASCII set.

- Example

  host1(config)#**line vty 1 3**
  host1(config-line)#**data-character-bits 7**

- There is no **no** version.

terminal data-character-bits

- Use to set the number of bits per character on the terminal's screen for the current session.
- Use the default setting, 8, to view the full set of 8-bit international characters. Be sure that software on other devices in the network also supports international characters.
- Set the number of bits to 7 to view only characters in the standard ASCII set.
- Example

  host1#**terminal data-character-bits 7**

- There is no **no** version.

Configuring Login Conditions

You can issue the **dsr-detect** command to configure the system so that a data set ready (DSR) signal is required to log in to the console. If a session is in progress and the DSR signal is lost, the user is logged out automatically.

host1(config)#**line console 0**
host1(config-line)#**dsr-detect**

DSR is carried on pin 6 of the SRP module's RS-232 (DB-9) connector. The DSR input must be connected to the DSR output of a modem or the DTR output of another data terminal device, such as a terminal server, that supports this signal.

dsr-detect

- Use to require that a DSR signal be detected on the line for a user to log in to the console.
- By default, DSR is not required and DSR detection is disabled.
- Example

  host1(config-line)#**dsr-detect**

- Use the **no** version to remove the DSR requirement for login.

Setting Time Limits for User Login

You can specify a time interval that the CLI waits for a user to provide a password when logging in to the console or a vty line. To do so:

1. Access the line configuration mode using either the **console** or **vty** keyword.
2. Specify the time during which the user must enter the password. For example:

```
host1(config)#line console 0
host1(config-line)#login
host1(config-line)#timeout login response 15
```

timeout login response

- Use to set the time interval that the console or vty lines wait for the user to log in.
- If the interval passes and the user has not responded, the system closes the session or lines.
- Specify an interval in the range 0–300 seconds. A value of 0 means that there is no time limit during which the user must respond.
- The default value is 30 seconds.
- Example

  ```
  host1(config-line)#timeout login response 15
  ```

- Use the **no** version to restore the default interval, 30 seconds.

Setting Time Limits for User Input

You can specify a time interval that the CLI waits for user input on the console or vty lines. To do so:

1. Access the line configuration mode using either the **console** or **vty** keyword.
2. Specify the time during which the user must enter information. For example:

```
host1(config)#line vty 0
host1(config-line)#exec-timeout 4192 13
```

exec-timeout

- Use to set the time interval that the console or vty lines wait for expected user input.
- If the interval passes and the user has not responded, the system closes the session or lines.
- Specify a time limit in the range 0–35791 minutes, and optionally specify the number of seconds.

- By default, there is no time limit.
- Example

  host1(config-line)#**exec-timeout 4192 13**

- Use the **no** version to remove the time limit.

Configuring CLI Messages

You can configure text banners for the CLI to display to users at different times in the connection process.

banner

- Use to configure message-of-the-day (MOTD), login, or exec banner to be displayed by the CLI:
  - motd—Displays the banner when a console or vty connection is initiated.
  - login—Displays the banner before any user authentication (line or RADIUS authentication). The banner is also displayed if user authentication is not configured.
  - exec—Displays the banner after user authentication (if any) and before the first prompt of a CLI session.
- If you do not specify an option, the default behavior is to display the banner as an MOTD.
- The first character in the banner string must be repeated at the end of the string; these characters delimit the banner. The CLI prompts you if you fail to repeat the opening delimiter. All text following the second occurrence of the delimiter is ignored without warning. The delimiter is case sensitive.
- Banner text can span multiple lines. It is truncated after 1,024 characters.
- Insert **\n** where you want the banner text to split and start a new line. Alternatively, you can press Enter on the CLI when you want the text to break. In the second case, you will be prompted for the remainder of the text after you press Enter. To display a backslash as part of the message, it must be immediately preceded by another backslash, like this: \\. Do not use a backslash as a delimiter or end a line with a backslash.
- To insert a **?** character inside the text of a banner, you must enter Ctrl + v before entering the **?** character. Failure to do so may produce undesired results.
- Examples

  host1(config)#**banner motd x This is an MOTD banner x**
  host1(config)#**banner Y This is also an MOTD banner Y**
  host1(config)#**banner "Quotes make good delimiters"**
  host1(config)#**banner Xno space is required between the delimiter and the real banner textX**
  host1(config)#**banner b bad choice for a delimiter; everything after that second b was ignored b**
  host1(config)#**banner "This is one way\nto specify a multiple line banner"**
  host1(config)#**banner "This is another way to specify a**
  Enter remainder of text message. End with the character '"'.
  multiple line banner"

- Use the **default** version to restore the default setting, in which the banner is displayed on all lines.
- You can configure MOTD or exec banners, but not login banners, for the CLI to display on a per-line basis.
- Use the **no** version to remove the banner.

exec-banner

- Use to display an exec banner on a particular line after user authentication (if any) and before the first prompt of a CLI session.
- Banners on the lines are enabled by default; the **no** version does *not* reenable banners on the lines.
- See the **banner** command description for more information about configuring an exec banner.
- Example

  host1(config-line)#**exec-banner**

- Use the **default** version to restore the default setting, in which the banner is displayed on all lines.
- Use the **no** version to disable the exec banner on the line. If both the exec and MOTD banners are enabled on a line, issuing the **no exec-banner** command disables both the exec banner and the MOTD banner. The **no motd-banner** command behaves differently from the **no exec-banner** command.

motd-banner

- Use to display an MOTD banner on a particular line when a connection is initiated.
- Banners on the lines are enabled by default; the **no** version does *not* reenable banners on the lines.
- See the **banner** command description for more information about configuring an MOTD banner.
- Example

  host1(config-line)#**motd-banner**

- Use the **default** version to restore the default setting, in which the banner is displayed on all lines.
- Use the **no** version to disable the MOTD banner on the line. If both MOTD and exec banners are enabled on a line, issuing the **no motd-banner** command disables the MOTD banner and leaves the exec banner enabled. The **no motd-banner** command behaves differently from the **no exec-banner** command.

Monitoring the Console Settings

You can use the following commands to monitor console settings.

show line console 0

- Use to view the parameters configured for all future console sessions and the current console session.
- Example

```
host1#show line console 0
dsr-detect disabled
configured speed 9600, current speed 9600
exec-timeout never
```

show terminal

- Use to view parameters of the current console session.
- Field descriptions
  - Length—Number of lines on the screen
  - Width—Number of characters on each line of the screen
  - data-character-bits—Number of bits per character
    - 7—Setting for the standard ASCII set
    - 8—Setting for the international character set
  - Speed—Speed of the console session
  - dsr-detect—Status of DSR signal detection
    - enabled—DSR signal must be detected for a user to log in to the console.
    - disabled—DSR signal need not be detected for a user to log in to the console.
  - exec-timeout—Time interval that the terminal waits for expected user input
    - Never—Indicates that there is no time limit
  - exec-banner—Status for the exec banner: enabled or disabled. This banner is displayed by the CLI after user authentication (if any) and before the first prompt of a CLI session.
  - motd-banner—Status for the MOTD banner: enabled or disabled. This banner is displayed by the CLI when a connection is initiated.
  - login-timeout—Time interval during which the user must log in.
    - Never—Indicates that there is no time limit
- Example

```
host1#show terminal
Length: 25 lines, Width: 80 columns
data-character-bits: 8 bits per character
Speed: 9600 bits per second
dsr-detect disabled
exec-timeout never
exec-banner enabled
motd-banner enabled
login-timeout 30 seconds
```

Sending Messages

You can send a message to one or more terminals with the **send** command. You can specify a line number, a console number, or a vty number. You can also send the message to all terminals.

The following command sends the message “hello console” to line 0:

```
host1#send 0 “hello console”
```

The following command sends the message “hello everyone” to all terminals:

```
host1#send * “hello everyone”
```

If you begin the message on the same line as the **send** command, the first character of the message is considered to be a delimiter. You must use the same character to terminate the message. In both examples above, the delimiter was a double quotation mark (**“**).

If you press Enter without typing the second delimiter, the CLI prompts you for more message text and reminds you to complete the message with the delimiter, as shown in the following example:

```
host1#send vty4 XYou can start a message on the same line
 Enter remainder of text message.  End with the character 'X'.
and continue it on subsequent lines; the CLI prompts you for
 Enter remainder of text message.  End with the character 'X'.
more message text until you enter the second delimiterX
 Proceed with send? [confirm]
```

If you do not begin the message on the same line as the **send** command, the CLI prompts you for the message text after you press Enter. The CLI does not recognize delimiters for these messages; you must enter Ctrl + z, as shown in the following example:

```
host1#send 0
 Enter remainder of text message.  End with ^Z.
Good morning, Major Tom^Z
 Proceed with send? [confirm]
```

The receiving terminals display the message without regard to other output currently displayed on the terminal. Pagination is not affected.

The sending terminal is not affected by the state of the intended receiving terminal. For example, if the receiving terminal is flow-controlled off or at a --More-- prompt, the message is still sent, and the sending terminal is available for further commands. The receiving terminal in this case displays the message when subsequently flow-controlled on or when the user responds to the --More-- prompt.

The receiving terminal displays the message, the line number of the sender, the username of the sender if the user was authenticated through RADIUS, and the time the message was sent.

send

- Use to send a message to one or more terminals. You can specify a line number, a console number, or a vty number. You can use the * keyword to send the message to all terminals.
- If you begin the message on the same line as the **send** command, the first character of the message is considered to be a delimiter. You must use the same character to terminate the message.
- The CLI prompts you for message text if you do not begin or complete the message on the same line as the **send** command. The CLI reminds you to signal the end of the message either with the delimiter or Ctrl + z.
- Example

  host1#**send 0 "hello console"**

- There is no **no** version.

Managing Memory

The system performs most memory management tasks automatically. The system allocates some memory permanently and some memory temporarily. When applications are deleted, memory that the system assigned temporarily becomes available again.

The system releases available memory on an SRP module or line module automatically if that module requires extra memory for an application. However, you can force the system to release available memory on the primary SRP module if you issue either the **show processes memory** command or the **show utilization** command.

For information about the **show processes memory** command, see *Managing Files* on page 245. For information about the **show utilization** command, see *Chapter 6, Managing Modules*.

NOTE: When you issue the **show utilization** command, the system releases available memory on the SRP module immediately; however, the display appears a few seconds later.

Managing Files

You are responsible for file management. Table 31 shows the types of system files and their corresponding extensions.

Table 31: Types of System Files and Corresponding Extensions

Type of File	Extension	Description
Configuration	*.cnf	Snapshot of the system's configuration
Core dump	*.dmp	File you can create for troubleshooting if a module fails
History	*.hty (reboot.hty)	Details of when and why modules rebooted

Table 31: Types of System Files and Corresponding Extensions (continued)

Type of File	Extension	Description
Log	*.log	A series of messages that describe events that occurred on the system
Macro	*.mac	A macro program
Release	*.rel	Software releases you can install in the system
Script	*.scr	A sequence of CLI commands. When you run a script file, the system executes the commands as though they were entered at the terminal
Secure Shell (SSH) Server public key	*.pub	Host key for the SSH server
Statistics	*.sts	Bulk statistics created when you run the **bulkstats** commands
Text	*.txt	Text file

System files may reside in four locations:

- The system space
- The user space
- A network host
- The standby SRP module

The system space contains files for system operation. For example, the current software configuration is stored in the system space.

The user space is reserved for FTP server operations and has the typical directory structure of a secure FTP server. The root or top level directory is a read-only directory that contains two subdirectories:

- /incoming—Read-write directory to and from which an FTP client can send and retrieve files.
- /outgoing—Read-only directory from which an FTP client can retrieve files.

Users can transfer files through FTP to the user space from a network host and vice versa. However, users cannot access the system space through FTP. To install a file from the user space to the system space, use the **copy** command. For detailed information about transferring files between locations, see *Transferring Files* on page 254.

To conserve NVS and minimize the installation time, files are not stored in both the system space and the user space. When you issue the **copy** command to install a file from user space to system space, the E-series router establishes a link to the file, but does not make a physical copy.

Managing the User Space from a Network Host

If you enable the system's FTP server (see *Configuring the FTP Server* on page 262), you can manage files on the user space from an FTP client on a network host. Table 32 lists the FTP protocol commands that the E-series router supports. Whether you can perform these functions on the user space depends on the features that the FTP client offers.

Table 32: FTP Commands That the System Supports

FTP Command	Function
HELP	List supported commands.
USER	Verify username.
PASS	Verify password for the user.
QUIT	Quit the session.
LIST	List contents of a directory.
NLST	List directory contents using a concise format.
RETR	Retrieve a file.
STOR	Store a file.
CWD	Change working directory.
CDUP	Change working directory to parent.
TYPE	Change the data representation type.
PORT	Change the port number.
PWD, XPWD	Get the name of current working directory.
STRU	Change file structure settings (only stream mode supported).
MODE	Change file transfer mode (only stream mode supported).
PASV	Make the server listen on a port for data connection.
NOOP	Do nothing.
DELE	Delete a file.
MKD, XMKD	Make directory.
RMD, XRMD	Remove directory.
RNFR	Rename from.
RNTO	Rename to.

File Commands and FTP Servers

Commands—**copy**, **configure file**, and **macro**—that invoke a remote FTP server take place in the context of the current virtual router rather than the default virtual router. You must configure the remote FTP server so that any traffic destined for the virtual router can reach the virtual router; typically, you configure the FTP server to reach the default address of the system, which will always be able to reach the virtual router.

Renaming Files

To rename files, use the **rename** command. Table 33 shows the types of files you can rename in different locations.

rename

- Use to rename a local file.
- You can change the base name but not the extension of a file.
- Example

  host1#**rename boston1.cnf boston2.cnf**

- There is no **no** version.

Table 33: File Types You Can Rename

	Destination			
Source	System Space	User Space (Linked Files and Unlinked Files)	Network Host Within a Firewall	Standby SRP Module
System	*.cnf *.dmp *.hty *.log *.mac *.rel *.scr *.txt Nonsystem files	*.cnf *.dmp *.hty *.log *.mac *.scr *.txt	*.sts	None
User Space	*.cnf *.hty (excluding reboot.hty) *.log (excluding system.log) *.mac *.scr *.txt	*.cnf *.dmp *.hty *.log *.mac *.pub *.rel *.scr *.sts *.txt Nonsystem files	None	None
Network Host Within a Firewall	None	None	None	None
Standby SRP Module	None	None	None	None

Deleting Files

Use the **delete** command to delete files in NVS. Table 34 on page 250 shows the types of files you can delete in different locations.

delete

- Use to delete files in NVS.
- To delete a file in user space, specify the incoming or outgoing directory on the FTP server. You can specify the name of a subdirectory in the incoming or outgoing directory.
- You can include an asterisk (*) as a wildcard at any position in a specified filename. The asterisk substitutes for zero or more characters in the name. You cannot use an asterisk in a directory or subdirectory name.
- You cannot delete reboot.hty or system.log files when you use a wildcard.
- When you do not use a wildcard, the CLI deletes the file immediately without prompting you for confirmation. When you use a wildcard, the CLI prompts you for confirmation unless you also specify the **force** keyword; in that case the deletion takes place without confirmation.
- The **force** keyword causes the immediate deletion of the directory or file even when it is not empty. However, if a file in the specified directory, or a specified file, is marked by the file system as in use because it is required for the current operation or configuration, the **force** keyword cannot force the deletion.
- The **force** keyword is ignored when you attempt to delete any .dmp or .tsa file (unless the deletion is issued from a .mac or .scr file); this means that the CLI always prompts for confirmation for these file types.
- Examples

```
host1#delete test-2.txt
host1#

host1#del test*.txt
Delete disk0:test-1.txt? [confirm]          -> press n
disk0:test-1.txt: not deleted (per user request)
Delete disk0:test-2.txt? [confirm]          -> press y
disk0:test-2.dmp: Deleted
Deleted 1 file, matched 2 files

host1#del test*.txt force
disk0:test-1.txt: deleted
disk0:test-2.txt: deleted
Deleted 2 files, matched 2 files
```

```
host1#del *.dmp force
WARNING: The force option is ignored for this file type.
Delete disk0:sample-1.dmp? [confirm]          -> press n
disk0:sample-1.dmp: not deleted (per user request)
Delete disk0:sample-2.dmp? [confirm]          -> press y
disk0:sample-2.dmp: Deleted
Deleted 1 file, matched 2 files

host1#delete /outgoing/test.scr
```

- There is no **no** version.

Table 34: File Types You Can Delete

Location			
System Space	User Space (Linked Files and Unlinked Files)	Network Host Within a Firewall	Standby SRP Module
*.cnf	*.cnf	None	*.dmp
*.dmp	*.dmp		
*.hty	*.hty		
*.log	*.log		
*.mac	*.mac		
*.rel	*.pub		
*.scr	*.rel (deletes *.rel file only and not associated files)		
*.sts	*.scr		
*.txt	*.sts		
	*.txt		
	Nonsystem files		

Monitoring Files

Use the **dir** command to view files in NVS.

NOTE: When high availability is enabled on the router, it is possible that files or file attributes may appear unsynchronized when they are not. When enabled, high availability mirrors configuration changes instantly from the active SRP to the standby SRP. However, although these changes are reflected immediately in memory, the standby SRP NVS is updated at 5 minute intervals.

dir

- Use to show a list of files in NVS.
- Specify a directory path, a local filename, a local device name, or some combination of these to view any local files or directories. You canot use the **dir** command on a network device.
- You can include an asterisk (*) at any position in a specified filename as a wildcard. The asterisk substitutes for zero or more characters in the name. You cannot use a wildcard in a path.
- Bulk statistics .sts files are stored in volatile storage on a RAM disk, and are displayed only when bulkstats is configured.

NOTE: When you issue the **dir** command from Boot mode, a reduced set of file types is displayed.

- Field descriptions
  - file—Name of file or directory (DIR indicates a directory)
  - size—Physical size of file
  - unshared size—Size of file in user space
    - Value of zero indicates that this file has been installed onto the system space and that there is a link to this file.
    - Value other than zero indicates that the file has not been installed onto the system space and equals the physical size of the file.
  - date—Date that file was created
  - in use—An exclamation point (!) indicates that the system is using this file
- Example 1

```
host1#dir
Please wait.....

Active/standby file systems are synchronized.

                                                    unshared
                    file                    size      size
-------------------------------------------------  ---------  ---------
disk0:/incoming <DIR>                             0
disk0:/outgoing <DIR>                             0
disk0:810beta13.cnf                          280944     280944
disk0:800beta12.cnf                          327011     327011
disk0:bng___1.txt                             11092      11092
disk0:bng___2.txt                             11092      11092
```

```
disk0:bng___3.txt                                      11092       11092
disk0:erx701rel.cnf                                   255400      255400
disk0:730beta19.cnf                                   283141      283141
disk0:730beta18.cnf                                   284503      284503
disk0:erx_8-0-0b0-24.cnf                              327404      327404
disk0:7.3run.cnf                                      301635      301635
disk0:80beta_bce_backup.cnf                           333228      333228
disk0:800beta5.cnf                                    300575      300575
disk0:820beta5.cnf                                    311616      311616
disk0:810beta16.cnf                                   297764      297764
disk0:SRP-10Ge_3_SC_08_22_2006_07_39.dmp           153268924   153268924
disk0:SRP-10Ge_3_SC_04_12_2007_09_47.dmp           182385184   182385184
disk0:reboot.hty                                      402368      402368
disk0:system.log                                         702         702
disk0:erx_9-0-0a1-7.rel                            176128192   160912356
disk0:erx_8-1-0b1-2.rel                            164065212   148633854
disk0:erx_8-2-0b1-5.rel                            166117319   150685961
disk0:testing_cat.txt                                  21848       21848
standby-disk0:SRP-10Ge_1_SC_08_21_2006_13_48.dmp   153547479   153547479
standby-disk0:SRP-10Ge_1_SC_04_12_2007_10_04.dmp   194849368   194849368
standby-disk0:reboot.hty                              123136      123136
standby-disk0:system.log                                 855         855

                                                                        in
                    file                                 date (UTC)     use
-------------------------------------------------   -------------------  ---
disk0:/incoming <DIR>                               02/08/2008 15:06:42
disk0:/outgoing <DIR>                               02/08/2008 15:06:42
disk0:810beta13.cnf                                 02/06/2007 15:13:44
disk0:800beta12.cnf                                 09/29/2006 16:31:54
disk0:bng___1.txt                                   02/12/2008 07:05:20
disk0:bng___2.txt                                   02/12/2008 07:05:28
disk0:bng___3.txt                                   02/12/2008 06:59:46
disk0:erx701rel.cnf                                 10/07/2005 13:01:02
disk0:730beta19.cnf                                 07/12/2006 07:21:22
disk0:730beta18.cnf                                 06/19/2006 15:23:46
disk0:erx_8-0-0b0-24.cnf                            11/02/2006 12:23:38
disk0:7.3run.cnf                                    08/21/2006 11:19:52
disk0:80beta_bce_backup.cnf                         10/04/2007 09:01:36
disk0:800beta5.cnf                                  01/02/2007 16:01:36
disk0:820beta5.cnf                                  05/09/2007 14:29:58
disk0:810beta16.cnf                                 03/15/2007 06:58:14
disk0:SRP-10Ge_3_SC_08_22_2006_07_39.dmp            08/22/2006 07:43:14
disk0:SRP-10Ge_3_SC_04_12_2007_09_47.dmp            04/12/2007 09:51:08
disk0:reboot.hty                                    01/09/2008 13:57:02
disk0:system.log                                    11/12/2007 09:56:14
disk0:erx_9-0-0a1-7.rel                             10/04/2007 08:40:06    !
disk0:erx_8-1-0b1-2.rel                             03/15/2007 06:50:32
disk0:erx_8-2-0b1-5.rel                             05/09/2007 14:22:22
disk0:testing_cat.txt                               03/13/2006 17:42:12
standby-disk0:SRP-10Ge_1_SC_08_21_2006_13_48.dmp    08/21/2006 13:51:42
standby-disk0:SRP-10Ge_1_SC_04_12_2007_10_04.dmp    04/12/2007 10:08:38
standby-disk0:reboot.hty                          01/09/2008 13:53:10
standby-disk0:system.log                            04/12/2007 09:47:24

                 Disk capacity
                 -------------
                 Capacity      Free      Reserved
    Device       (bytes)      (bytes)    (bytes)
--------------   ----------   ---------   --------
disk0:           1054900224   167372414   68157440
standby-disk0:   1054900224   153330775   68157440
```

- Example 2

```
host1#dir *.txt
Please wait.....

Active/standby file systems are synchronized.

                                                                  unshared
                     file                              size          size
-------------------------------------------------   ---------   ---------
disk0:bng___1.txt                                       11092       11092
disk0:bng___2.txt                                       11092       11092
disk0:bng___3.txt                                       11092       11092
                                                                          in
                     file                               date (UTC)        use
-------------------------------------------------   -------------------   ---
disk0:bng___1.txt                                   02/12/2008 07:05:20
disk0:bng___2.txt                                   02/12/2008 07:05:28
disk0:bng___3.txt                                   02/12/2008 06:59:46

                 Disk capacity
                 -------------
                 Capacity      Free      Reserved
    Device       (bytes)      (bytes)    (bytes)
--------------   ----------   ---------   --------
disk0:           1054900224   167372414   68157440
standby-disk0:   1054900224   153330775   68157440
```

- Example 3

```
host1#dir /incoming
                           unshared                          in
    file          size       size         date (UTC)        use
-------------   --------   --------   -------------------   ---
disk0:3-0-0a3-7.rel        256         0    12/19/2000 07:14:01
disk0:srp.exe          30012312        0    12/19/2000 07:14:12
disk0:srpIc.exe         1801208        0    12/19/2000 07:20:32
disk0:srpDiag.exe       6984222        0    12/19/2000 07:22:08

             Disk capacity
             -------------
          Capacity      Free      Reserved
Device    (bytes)      (bytes)    (bytes)
------   ----------   ---------   --------
disk0:    220200960   120616448   36700160
```

- Example 4

```
host1#dir /outgoing
                           unshared                          in
    file          size       size         date (UTC)        use
-------------   --------   --------   -------------------   ---
disk0:test.scr            1204          0   12/18/2000 03:01:04
disk0:foo.scr             1278       1278   12/20/2000 04:02:12

             Disk capacity
             -------------
          Capacity      Free      Reserved
Device    (bytes)      (bytes)    (bytes)
------   ----------   ---------   --------
disk0:    220200960   120616448   36700160
```

- There is no **no** version.

Viewing Files

Use the **more** command to display the contents of a macro, script, or text file. The file can reside in NVS on the primary SRP module, in NVS on the redundant (standby) SRP module, or on a remote server that you access using FTP.

more

- Use to display the contents of a macro, script, or text file that resides in NVS on the primary SRP module, in NVS on the redundant SRP module, or on a remote server that you access using FTP.
- Specify the file you want to display using one of the following formats, depending on the location of the file:
  - *fileName*—Name of the file that resides in NVS on the primary SRP module
  - standby:*fileName*—Name of the file that resides in NVS on the redundant (standby) SRP module
  - *serverName*:*filePathName*—Name of the remote server on which the file resides and the complete pathname of the file
- Example 1—Displays the contents of a text file named erxconfig.txt that resides in NVS on the primary SRP module

  host1#**more erxconfig.txt**

- Example 2—Displays the contents of a macro file named mysetup.mac that resides in NVS on the redundant (standby) SRP module

  host1#**more standby:mysetup.mac**

- Example 3—Displays the contents of a script file named myconfig.scr that resides on a remote server named fileserver1

  host1#**more fileserver1:/startup/scripts/myconfig.scr**

- There is no **no** version.

Transferring Files

You may need to transfer files between the following locations:

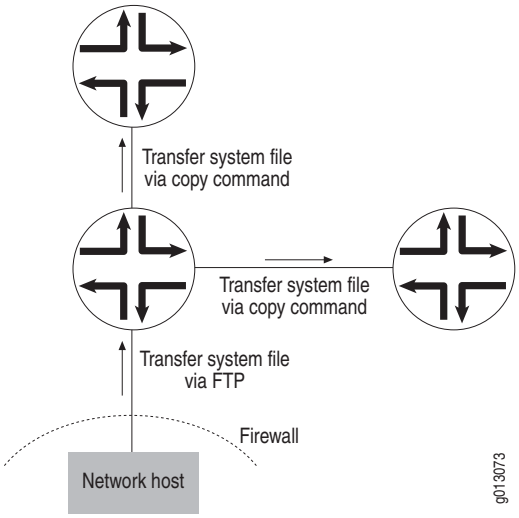
- System space
- User space
- Network host
- Standby SRP module

You can transfer files in any of three ways: the **copy** command, the system's FTP server, or a remote host that is configured as an FTP or a TFTP server. Table 35 on page 257 lists the types of files that you can transfer between the locations using the **copy** command, which activates a hidden FTP or TFTP client on the E-series router.

You can use the system's FTP server to transfer files between a network host and the user space. When a firewall separates the E-series router from the network host, you must use the FTP server to transfer files to the user space. You can then install the files from the user space to the system space by using the **copy** command. However, if there is no firewall between the E-series router and the network host, you can use the **copy** command, the remote FTP server, or the remote TFTP server to transfer files.

For example, you can transfer a file from a network host to an E-series router through FTP, and then transfer the file through the **copy** command from the E-series router to other E-series routers. See Figure 22 on page 255.

Figure 22: Transferring System Files to the E-series Router



References

For more information about file transfer protocols, consult the following resources:

- RFC 959—File Transfer Protocol (FTP) (October 1985)
- RFC 1350—Trivial File Transfer Protocol (TFTP) (Revision 2) (July 1992)

Copying and Redirecting Files

You have two options for copying or redirecting files to or from a remote FTP or TFTP server:

- Include all remote file data in the **copy** command. You can specify remote files using the URL format and the file redirect option for the related **show** commands.
- Use the **host** command to define the host and the appropriate file transfer protocol. FTP is the default if you do not specify a file transfer protocol or when Domain Name System (DNS) service is used to map IP addresses to the hostname.

If you include the remote file data, the **copy** command contains a source and destination filename, either of which (but not both) can be remote files. The following URL format is supported for both source and destination files:

protocol://[username [:password]@]location[/directory]/filename

The location can be a hostname or an IP address.

The two versions of the URL format are as follows:

ftp://[username[:password]@]location[/directory]/filename
tftp://location[/directory]/filename

NOTE: The TFTP protocol does not support username and password. Entering a username and password in the TFTP version results in a command error.

The protocol specified in the command always overrides the protocol associated with the host entry, if any, in the host table. Some protocols, such as FTP, require a username and password with each request. For the URL version of the **copy** command, the following sequence is followed:

- If the command contains a username, the username and password specified in the command are used. The password null is used if the command does not contain a password.
- If the location in the URL is a hostname with a corresponding host entry (created by the **host** command), the username and password of the host entry are used. A host entry that is created without an explicit user name is created with the default username of anonymous and password of null.

The location is the IP address or hostname of the remote file server. The directory/filename is the full path of the file relative to the user login root path.

The characters in the URL format can be encoded. Any of the delimiter characters can be used in the host, username, password, and directory and file fields when added as encoded characters. The encoded characters must be three characters, starting with a percent and followed by the two hexadecimal digits that are the ASCII equivalent. The system converts all printable characters before passing them to the protocol support. Unprintable characters (0-012F and 0x7f-0x7F) are not converted and are passed directly to the protocol. Printable characters (0x20–0x7E) are decoded and all others (0x80–0xFF) are rejected.

In the following example, the username contains the @ delimiter character encoded as %40, and the directory passed to the FTP protocol layer is /dirA/dirB/dirC. The delimiter between the hostname and directory is a forward slash (/) character. To add a slash to the start of the directory specification, add the encoded slash after the host and directory delimiter.

ftp://user%40%40name:pwd@mary/%2fdirA/dirB/dirc/fileA

In the following example, the directory passed to the FTP protocol layer is dirA/dirB/dirC.

ftp://username:pwd@mary/dirA/dirB/dirc/fileA

Using the copy Command

Table 35 shows the types of files that you can transfer between the locations by using the **copy** command.

Table 35: File Types You Can Transfer Using the copy Command

	Destination			
Source	System	User Space (Linked Files and Unlinked Files)	Network Host **Within** a Firewall	Standby SRP Module
System	*.cnf *.hty (excluding reboot.hty) *.log (excluding system.log) *.mac *.scr *.txt	*.cnf *.hty *.log *.mac *.pub *.scr *.txt	*.cnf *.dmp *.hty *.log *.mac *.pub *.scr *.sts *.txt	None
User Space	*.cnf *.mac *.rel *.scr *.txt	*.cnf *.hty *.log *.mac *.pub *.rel (*.rel file only, not files associated with the *.rel file) *.scr *.txt Nonsystem files	None	None
Network Host Within a Firewall	*.cnf *.mac *.rel *.scr *.txt	None	None	None
Standby SRP Module	system.log reboot.hty	system.log reboot.hty *.dmp	system.log reboot.hty *.dmp	None

To transfer files using the **copy** command between the system space and a network host:

1. Determine whether there is a route to the network host, and create one if necessary. See *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*.

2. Configure the network host as an FTP server, or use a remote host that is configured as a TFTP server.

NOTE: This command takes place in the context of the current virtual router (VR) rather than the default VR. You must configure the FTP server so that any traffic destined for the VR can reach the VR; typically, you configure the FTP server to reach the default address of the E-series router, which will always be able to reach the VR.

3. Add the FTP server to the static host table, and specify the file transport protocol (FTP or TFTP), so that the E-series router can access the network host.
4. (Optional) Specify a source interface to use in FTP packets leaving the router.
5. Copy the files.

copy

- Use to copy a file from one location to another.

NOTE: You cannot copy script (.scr) or macro (.mac) files while in Boot mode. You can copy only .cnf, .hty, and .rel files. If you issue the **dir** command from Boot mode, existing .scr and .mac files are not displayed.

- See Table 35 on page 257 for the types of files that you can copy.
- Specify a network path to copy to or from another device on the network.
- Specify the incoming or outgoing directory to copy to or from the user space.
- Specify a subdirectory name to create a subdirectory within the incoming or outgoing directory in the user space.
- You cannot use wildcards.
- You cannot create or copy over files generated by the system; however, you can copy such files to an unreserved filename.
- Examples

  host1#**copy host1:westford.cnf boston.cnf**
  host1#**copy /incoming/releases/2-8-0a3-7.rel 2-8-0a3-7.rel**
  host1#**copy /shconfig.txt ftp://joe:passwd@173.28.32.156/ftpDir /results/shConfigJoe.txt**

- There is no **no** version.

host

- Use to add or modify an entry to the host table. You can enter the optional username and password in plain text (unencrypted). Or, if you know the correct encrypted forms of the username and password, you can enter the encrypted forms (see below).
- This command supports both IPv4 and IPv6 address formats.
- This command allows network files to be accessible from a host.
- This command supports both FTP and TFTP for copying and redirecting files.

- You cannot invent an encrypted string to be used with the algorithm **8** option. You must use plain text (unencrypted) strings for the initial configuration. The only way to obtain a valid encrypted string is to enable password encryption (by issuing the **service password-encryption** command) and then examine the output of the **show configuration** command. Username and password encryption is made available primarily so that scripts generated from the **show configuration** output can be saved, used, and transferred without fear of password exposure.
- Example

  host1(config)#**host westford 10.10.8.7 ftp user25 easy53**

- To determine the encrypted values for usernames and passwords entered in cleartext, you must do the following:

  1. Issue the **service password-encryption** command. This causes subsequently issued **show configuration** commands to generate encrypted forms of the username and password for this command, as well as for all other commands that support encryption. See *Chapter 9, Passwords and Security*, for more information about the **service password-encryption** command.

  2. Issue the **show configuration** command and search for the **host** command. The encrypted forms are preceded by the number 8.

  3. You can copy and paste the command showing the encrypted forms into a macro or script to use as desired. Specify the number 8 before the username and before the password to enter an encrypted value.

- Example for encrypted values

```
host1(config)#service password-encryption
host1(config)#host test 10.2.3.4 ftp nick nick
host1(config)#end
host1#show config | inc host
hostname "host1"
host test 10.2.3.4 ftp 8 CU&I,XM(S 8 X=emZn>'S
```

- Use the **no** version to remove a specified host.

ip ftp source-address

- Use to specify an operational interface by IP address as the source interface for FTP packets sent by the system's FTP client.
- This command overrides a setting you configured previously with the **ip ftp source-interface** command.
- If you issue this command, the output of the **show configuration** command includes an entry of the following format:

  ip ftp source-address *ipAddress*

  This entry also appears in the output if you delete an interface or change its IP address after issuing the **ip ftp source-interface** command, in which case the IP address is the one that was configured on the interface before you issued the **ip ftp source-interface** command.

- Example

  host1(config)#**ip ftp source-address 10.10.5.21**

- Use the **no** version to restore the default, in which the source address in the FTP packets is that of the interface where the FTP connection is made.

ip ftp source-interface

- Use to specify an operational interface by interface type and location as the source interface for FTP packets sent by the system's FTP client.
- The interface you specify must have an IP address.
- This command overrides a setting you configured previously with the **ip ftp source-address** command.
- If you issue this command and the interface is valid, the output of the **show configuration** command includes an entry of the following format:

  ip ftp source-interface *interfaceType interfaceSpecifier*

  - *interfaceType*—Type of interface
  - *interfaceSpecifier*—Location of the interface

  For information about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.

- If you delete the interface or change its IP address, the output of the **show configuration** command appears as if you had entered the **ip ftp source-address** command:

  ip ftp source-address *ipAddress*

  - *ipAddress*—IP address of the interface when you issued the **ip ftp source-interface** command

- Example

  host1(config)#**ip ftp source-interface loopback1**

- Use the **no** version to restore the default, in which the source address in the FTP packets is that of the interface where the FTP connection is made.

copy Command Examples

The examples in this section assume that the following host entries have been defined in the host table:

- host mary 172.28.32.156 ftp mike mikePwd
- host joe 172.28.32.99 ftp joe jPasswd

Example 1 Copy a remote file to a local file by using the CLI file **copy** command format. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username mike and password mikePwd from the host entry mary are used to access the remote file.

copy mary:ftpDir/scripts/autocfg.scr autocfg.scr

Example 2 Copy a local file to a remote fileby using file **copy** command format. The following command creates or replaces the remote file shConfigForJoe.txt in the directory ftpDir/results on the host joe by copying the local file shConfig.txt. The username joe and password jPasswd from the host entry joe are used to access the remote file.

```
copy shConfig.txt joe:ftpDir/results/shConfigForJoe.txt
```

Example 3 Copy a remote file to a local file by using the URL format, use the hostname to specify the location, and specify the user name and password in the command. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username fred and the password passwd in the command are used; the username and password in the host entry are ignored.

```
copy ftp://fred:passwd@mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 4 Copy a remote file to a local file by using the URL format, use the hostname to specify the location, specify the user name in the command, and use the default value of the password. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username fred from the command and the default password null are used; the username and password in the host entry are ignored.

```
copy ftp://fred@mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 5 Copy a remote file to a local file by using the URL format, and use the hostname to specify the location. The protocol TFTP, which does not support usernames or passwords, is the protocol in the URL. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The protocol specified in the command is used; the protocol for the host entry mary is ignored.

```
copy tftp://mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 6 Copy a remote file to a local file by using the URL format, use the hostname to specify the location, and use the username and password from the host entry. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host mary. The username mike and password mikePwd from the host entry are used.

```
copy ftp://mary/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 7 Copy a remote file to a local file by using the URL format. Use the host's IP address to specify the location. The following command creates or replaces the local file autocfg.scr by copying the remote file autocfg.scr located in the directory ftpDir/scripts on the host 172.28.32.156. Use the username fred to access the remote file.

```
copy ftp://fred@172.28.32.156/ftpDir/scripts/autocfg.scr autocfg.scr
```

Example 8 Copy a local file to a remote file by using the URL format, and use the host's IP address to specify the location. The following command creates or replaces the remote file shConfigJoe.txt in the directory ftpDir/results on the host 172.28.32.156 by copying the local file shConfig.txt. The username joe and the password passwd from the command are used to access the remote file.

```
copy shConifg.txt ftp://joe:passwd@172.28.32.156/ftpDir/results/shConfigJoe.txt
```

Example 9 Redirect the output of a command to a remote file by using the URL format, and use the host's IP address to specify the location. Execute **show config**, and redirect the output to the remote file shConfigJoe.txt in directory ftpDir/results on host 172.28.32.156 using username joe and password passwd.

```
show config > ftp://joe:passwd@172.28.32.156/ftpDir/results/shConfigJoe.txt
```

Using TFTP to Transfer Files

You can use TFTP to copy files and redirect output from the E-series router to a remote server if the remote host supports TFTP. Before transferring files by the remote TFTP server, you must use the **host** command to define the host and to specify TFTP as the file transfer protocol.

The maximum file size is 32 MB for file transfer. The release package for JUNOSe Release 6.1.0 and higher-numbered releases includes a split version of all release images that exceed 32 MB. Each chunk is less than 32 MB. You can therefore use TFTP with JUNOSe Release 6.1.0 and higher-numbered releases to transfer large software images. The JUNOSe software copies the split images and reassembles them to full size on the router. The file system on the router does not contain any additional images as a result of this operation.

Configuring the FTP Server

To transfer files by the system's FTP server, you must configure the FTP server and ensure that FTP client software is installed on the network host.

Although you can transfer any type of file by FTP to the E-series router, the principal aim of this feature is to allow the transfer of system files to NVS. You can transfer files by FTP to the user space. You can then install files from the user space onto the system using the **copy** command. It is not possible to access the system files directly through FTP operations.

FTP sessions on the E-series router use the vty lines. The E-series router divides its vty resources between Telnet, SSH, and FTP services. Each FTP session requires one vty line. The FTP service uses the authentication method configured for the vty lines.

Features

The system supports the following FTP features:

- Compliance with RFC 959—File Transfer Protocol (FTP) (October 1985)
- FTP passive mode

- Efficient NVS organization
- User authentication by RADIUS or password checking

FTP Passive Mode

Normally, when a client connects to an FTP server, the client establishes the control channel with the server, and the server responds by opening a data channel to the client. However, when the FTP client and server are on opposite sides of a firewall that prohibits inbound FTP connections, the server cannot open a data channel to the client.

FTP passive mode overcomes this connection limitation. In passive mode, the client opens a control channel to the server, tells the server it wants to operate in passive mode, and opens the data channel to the server. This method of establishing the FTP connection allows both the control channel and the data channel to pass through the firewall in the allowed direction.

Configuring Authentication

Before you enable the FTP server, configure the authentication procedure for the vty lines, as follows:

1. Configure host access lists.
2. Configure user authentication methods.
3. Configure the vty lines to use the host access lists and user authentication methods.

You can specify authentication by a RADIUS server or by password checking. If you choose no authentication service, any client can access the FTP server. For information about authentication on vty lines, see *Chapter 9, Passwords and Security*.

Configuration Tasks

FTP is disabled by default. You must enable the FTP server with the **ftp-server enable** command before the system allows FTP clients to connect.

ftp-server enable

- Use to enable the FTP server and to monitor the FTP port for attempts to connect to the FTP server.
- You can enable the FTP server on the default virtual router only.
- Example

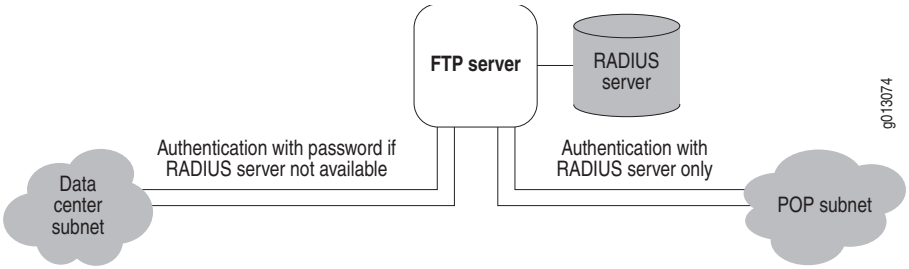
  host1(config)#**ftp-server enable**

- Use the **no** version to terminate current FTP sessions and to disable the FTP server.

Configuration Example

Figure 23 shows the scenario for this configuration example.

Figure 23: FTP Configuration Example



In this example, two FTP lines are required for administrators on the data center subnet, and two more lines are required for users on the POP subnet. The system verifies passwords of administrators on the data center subnet through either a RADIUS server or through simple line authentication if the RADIUS server is unreachable. However, the system verifies passwords of users on the POP subnet only through the RADIUS server.

The following example shows all steps for configuring this scenario, from specifying a RADIUS server to enabling the FTP line:

1. Configure the RADIUS server.

   host1(config)#**radius authentication server 10.6.131.51**
   host1(config-radius)#**key abc123**
   host1(config-radius)#**udp-port 1645**

2. Configure two access lists—one named “DataCenter,” permitting only the data center subnet, and one named “Pops,” permitting only the POP subnet.

   host1(config)#**access-list DataCenter permit 10.6.128.0 255.255.128.0**
   host1(config)#**access-list DataCenter deny any**
   host1(config)#**access-list Pops permit 199.125.128.0 255.255.128.0**
   host1(config)#**access-list Pops deny any**

3. Configure two authentication method lists, named “RadiusAndLine” and “RadiusOnly.”

   host1(config)#**aaa new-model**
   host1(config)#**aaa authentication login RadiusAndLine radius line**
   host1(config)#**aaa authentication login RadiusOnly radius**

4. Configure two FTP lines to be used by data center administrators.

   host1(config)#**line vty 0 1**
   host1(config-line)#**password foobar**
   host1(config-line)#**access-class DataCenter in**
   host1(config-line)#**login authentication RadiusAndLine**

5. Configure the remaining FTP lines to be used by POP administrators.

```
host1(config)#line vty 2 4
host1(config-line)#password foobar
host1(config-line)#access-class Pops in
host1(config-line)#login authentication RadiusOnly
```

6. Enable the FTP server.

```
host1(config)#ftp-server enable
```

Monitoring the FTP Server

Use the **dir** command to monitor files on the FTP server. Use the **show ftp-server** and **show users** commands to monitor settings of the FTP server.

show ftp-server

- Use to display information about the FTP server.
- Field descriptions
  - FTP Server state—Status of the FTP server: enabled or disabled
  - Open connections—Number of open connections to the FTP server
  - Statistics since server was last started—Data about the connection attempts since you enabled the FTP server
  - Statistics since last system reload—Data about the connection attempts since you last booted the system
    - attempts—Number of attempts to connect
    - failed hosts—Number of connection attempts that failed because of disallowed host addresses
    - failed users—Number of connection attempts that failed because users were not authenticated
- Example

```
host1#show ftp-server
FTP Server state: enabled, 0 open connections
Statistics since server was last started:
        attempts: 32
        failed hosts: 5
        failed users: 7
Statistics since last system reload:
        attempts: 35
        failed hosts: 5
        failed users: 8
```

show users

- Use to display information about users of the vty lines.
- Specify the **all** keyword to view information for all configured lines (both connected and not connected).
- Specify the **detail** keyword to view detailed information.

- Field descriptions
  - line number—Number of the line to which the user is connected
  - line name—Name of the line, the service the line offers, and the relative line number
  - user—Name of the user
  - connected from—Location or IP address of the user
  - connected since—Date and time that the user connected to the line
  - idle time—Amount of time it has been since an entry was made from this line (detail only)
  - virtual router—Virtual router used by this line user (detail only)
  - privilege level—Privilege level of this line user (detail only)
  - current command—Command currently being executed by the user over this line (detail only)
- Example 1

```
host1#show users
 line                              connected
number     line name      user       from      connected since
------   --------------   -----   ----------   ----------------
0*       console 0                 console      02/12/2001 19:57
4        vty 3 (ftp)      fred    10.10.0.64   02/12/2001 20:04
5        vty 4 (telnet)            10.10.0.64   02/12/2001 20:04

Note: '*' indicates current user.
```

- Example 2

```
host1#show users detail
 line                              connected                          idle
number     line name      user       from       connected since      time
------   --------------   ----   ------------   ----------------   --------
0        console 0                 console        08/14/2003 08:01   00:23:50
1*       vty 0 (telnet)            10.10.120.90   08/15/2003 10:37
 line    virtual   privilege
number   router      level      current command
------   -------   ---------   -----------------
0        default   10
1*       default   10          show users detail
Note: '*' indicates current user.
```

Copying Partial Releases

You can shorten the time it takes to copy a release from a server and reduce the amount of storage needed for a release. At the default setting, all subsystems are included when you copy a release from a server. Use the **exclude-subsystem** command to specify subsystems that you do not want to copy from the server. Use the **show subsystems** command to verify which files are included and excluded when you copy a release from a server.

Follow this example:

1. Determine which subsystems are included in the release on the server.

   host1#**show subsystems file m:/x/images/x-y-z.rel**

2. Exclude any subsystems in the release that you do not need for the configuration.

   host1#(config)#**exclude-subsystem coc12**
   host1#(config)#**exclude-subsystem oc12s**

3. (Optional) Remove a subsystem from the exclude list.

   host1#(config)#**no exclude-subsystem oc12s**

4. (Optional) Verify the subsystems that will be included and excluded in future release copies.

   host1#**show configuration**
   ...
   exclude-subsystem coc12

5. (Optional) After copying a release, view which subsystems were excluded.

   host1#**show subsystems file x8.rel**

6. (Optional) Determine whether the currently running software is a result of a copy with excluded subsystems. The word "Partial" indicates that subsystems were excluded.

   host1#**show version**
   Juniper Networks, Inc. Operating System Software
   Copyright (c) 200X Juniper Networks, Inc. All rights reserved.
   System Release: x-y-z.rel Partial

exclude-subsystem

- Use to exclude any subsystems that are in a release that you do not need for the system configuration.
- Example

  host1(config)#**exclude-subsystem coc12**

- The subsystems that you indicate are added to the "exclude list." All subsequent release copies will exclude the images for these subsystems from the release copy.

- Example

  host1(config)#**no exclude-subsystem coc12**

- Use the **no** version of this command *with the subsystem name* to remove a subsystem from the exclude list. Use the **no** version of this command *without a subsystem name* to remove *all* subsystems from the exclude list.

show subsystems

- Use to determine which subsystems are included in the current software release on the system or in a specified software release file.
- Specify either a local filename or a remote path and filename to view the subsystems that are included in a software release file other than the current software release on the system.
- Field descriptions
  - Required—Number of bytes of data for the required portion of the release.
  - Included Subsystems—Number of bytes of data for the included subsystems listed. All included subsystems in the release are listed.
  - Excluded Subsystems—Number of bytes of data for the excluded subsystems listed. All excluded subsystems in the release are listed.
- Use the command before you copy a release to verify which subsystems are present in the release.
- Example

```
host1#show subsystems file m:/x/images/x-y-z.rel
oc3
oc12p
oc12a
ge
fe8
coc12
oc12s
```

- Use the command after copying a release to verify which subsystems are included and excluded.
- Example

```
host1#show subsystems file x8.rel
Required: 1423005  bytes
Included Subsystems:  27882192  bytes
oc12p
oc12a
ge
fe8
coc12
oc12s

Excluded Subsystems:  6840211   bytes
oc3
```

Configuring the NFS Client

You can configure a virtual router on the E-series router as a Network File System (NFS) client to provide remote file access for E-series applications that need NFS-based transport.

The system provides NFS client support only for E-series applications designed to use NFS-based transport. Unlike the typical implementation on UNIX workstations, the E-series NFS client does not provide services such as mounting or unmounting of files through the CLI.

This section describes how to configure the NFS client if you are using an E-series application that requires NFS-based transport.

References

The NFS client complies with the following standards:

- RFC 1094—Network File System Protocol Specification (March 1989)
- RFC 1057—Remote Procedure Call Protocol Specification (June 1988)

Prerequisites

The E-series NFS client requires a remote host to act as an NFS server. The remote host must support NFS server protocol version 2 or higher.

Configuration Tasks

To configure a virtual router as an NFS client:

1. Access the virtual router context.
2. Add the remote host to the host table.
3. Configure the remote host as an NFS server for this virtual router.
4. Specify the E-series interface that this virtual router will use to exchange NFS communications with this server.

host

- Use to add or modify an entry to the host table.
- Example

  host1:boston(config)#**host host50 10.2.3.4**

- Use the **no** version to remove a specified host.

ip nfs

- Use to specify the E-series interface that the current virtual router will use to exchange messages with the NFS server.
- Specify either the **source-address** keyword with the IP address of the interface or the **source-interface** keyword with the interface type and specifier. For information about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Issuing this command provides connectivity between the E-series router and the remote host if the network configuration restricts communications between devices.
- Example

  host1:boston(config)#**ip nfs source-address 10.1.1.1**
  host1:boston(config)#**ip nfs source-interface atm 3/2.6**

- Use the **no** version to delete the name server.

ip nfs host

- Use to configure a remote host as an NFS server for the current virtual router.
- Optionally, specify a user identity and a group identity that a user must specify to connect to the remote host. The default user identity is 2001, and the default group identity is 100.
- Example

  host1:boston(config)#**ip nfs host host50 user 1500 group 150**

- Use the **no** version to disassociate this NFS server from the current virtual router.

Monitoring the NFS Client

Use the **show hosts** command (see *Monitoring the System* on page 288) to monitor information about connected NFS servers. Use the **show ip nfs** command to display information about the interface that the current virtual router uses to exchange messages with the NFS server.

show ip nfs

- Use to display information about the interface that the current virtual router uses to exchange messages with the NFS server.
- Field descriptions
  - Source address—IP address of the interface that the current virtual router uses to exchange messages with the NFS server.
  - Source interface—Type and specifier of the interface that the current virtual router uses to exchange messages with the NFS server. For information about interface types and specifiers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.
- Example

```
host1#show ip nfs
Source address is 1.1.1.1
```

Using a Loopback Interface

The loopback interface provides a stable address for protocols (for example, BGP, Telnet, or LDP) to use so that they can avoid any impact if a physical interface goes down.

The loopback interface sends packets back to the router or access server for local processing. Any packets routed from the loopback interface, but not destined to the loopback interface, are dropped.

NOTE: Do not confuse loopback with the null 0 interface. Traffic routed to null 0 is discarded on the line module.

The **no** version deletes the loopback interface.

interface loopback

- Use to access and configure the loopback interface.
- Provides a stable address to minimize impact of a physical interface going down.
- Example

  host1(config)#**interface loopback 20**
  host1(config-if)#**ip address 10.10.20.5 255.255.255.254**

- Use the **no** version to delete the loopback interface.

Using the Telnet Client

The system has an embedded Telnet client that enables you to connect to remote systems. You can configure a Telnet daemon to listen in virtual routers other than the default virtual router. You must be in the context of the desired virtual router to issue the command.

telnet

- Use to open a Telnet connection to a remote system.
- Specify the IP address or name of the remote host.
- You can specify a VRF context in which the request takes place.
- Depending on how the remote system accepts Telnet requests, you can specify a port number or port name through which the system will connect to the remote host. In the Transmission Control Protocol (TCP), ports define the ends of logical connections that carry communications. In most cases, you can accept the default, port number 23, the Telnet port. For more information about port numbers and associated processes, see www.iana.org.
- You can force Telnet to use the IP address of an interface that you specify as its source address.

- Example

  host1#**telnet 192.168.35.13 fastEthernet 0**

- There is no **no** version.

telnet listen

- Use to create a Telnet daemon to listen in a virtual router.
- Example

  host1(config)#**virtual-router 3**
  host1:3(config)#**telnet listen port 3223**

- Use the **no** version of the command to delete the daemon.

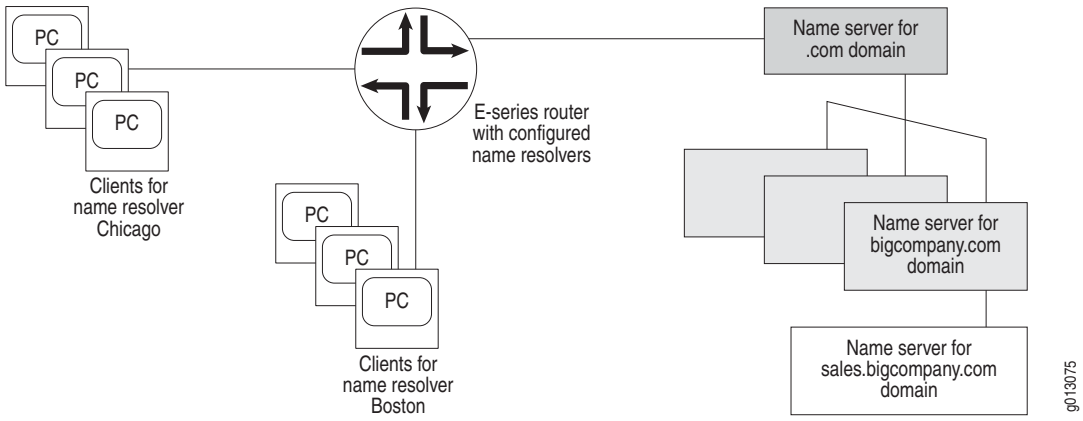
Configuring DNS

You can configure virtual routers to act as *name resolvers* for Domain Name Service (DNS). DNS is a client/server mechanism that maps IP addresses to hostnames.

The name resolver is the client side of DNS and receives address-to-hostname requests from its own clients when they want to contact hosts on other networks. By polling *name servers,* the name resolver learns name-to-address translations for the hosts its clients want to contact.

A name server may provide the translation from its cache or may poll servers lower in the DNS hierarchy to obtain a translation. Typically, name servers at the top of the hierarchy recognize top level domain names and know which servers to contact for information about more detailed domain names. See Figure 24.

Figure 24: DNS Hierarchy Example



DNS messages from a name resolver to a name server must include the domain name for the resolver's clients. Consequently, you must specify a default domain name for the clients. The default domain name is appended to unqualified hostnames (those without domain names).

The name resolver must be able to access at least one name server. Accordingly, you must configure a static route to a gateway that provides access to the name server and assign the name server to the name resolver. For more information, see *Assigning Name Servers* on page 273.

Each virtual router can have its own name resolver and domain name. However, if two virtual routers use the same name servers and belong to the same local domain, you do not need to configure name resolvers on both virtual routers. For more information, see *Using One Name Resolver for Multiple Virtual Routers* on page 274.

References

For more information about the DNS, consult the following resources:

- RFC 1035—Domain Names – Implementation and Specification (November 1987)
- RFC 2308—Negative Caching of DNS Queries (DNS NCACHE) (March 1998)

Assigning Name Servers

To assign name servers to the system:

1. Access the virtual router context.
2. Define static routes to the gateways that provide access to the name servers.
3. Enable the virtual router to query name servers.
4. Specify a default domain name for the hosts.
5. Specify the name servers.

Example

host1(config)#**virtual-router boston**
host1:boston(config)#**ip route 0.0.0.0 0.0.0.0 *gatewayIpAddress***
host1:boston(config)#**ip domain-lookup**
host1:boston(config)#**ip domain-name urlofinterest.com**
host1:boston(config)#**ip name-server 10.2.0.3**
host1:boston(config)#**ip name-server 10.2.5.5**

ip domain-lookup

- Use to enable the system to query the configured DNS name servers when it needs an IP-hostname-to-IP-address translation.
- Domain lookup is disabled by default.
- Example

  host1(config)#**ip domain-lookup**

- Use the **no** version to disable domain lookup.

ip domain-name

- Use to define a default domain name for the clients that a name resolver serves.
- You must define a default domain name for each name resolver. Multiple name resolvers can use the same default domain name.
- If you map an unqualified hostname (one without a domain name) to an IP address with the **host ftp** command, the domain name is appended to the hostname before the name is stored in the host table.
- Example

  host1(config)#**ip domain-name bigcompany.com**

- Use the **no** version to delete the domain name; that is, the domain name will no longer be appended to hostnames in the static host table.

ip name-server

- Use to specify a DNS name server that the system can query for hostname-to-IP-address resolution.
- This command supports both IPv4 and IPv6 addressing formats.
- Example

  host1(config)#**ip name-server 192.168.25.100 1:2:3:4:5:6:7:8:9:0:a:b:c:d:e:f**

- Use the **no** version to delete the name server.

Using One Name Resolver for Multiple Virtual Routers

You can use one name resolver for multiple virtual routers if those virtual routers use the same name servers and belong to the same local domain. To do so, complete the following steps:

1. Configure a name resolver for the first virtual router.
2. Access the context for the second virtual router.
3. Specify that the second virtual router should use the name resolver you configured for the first virtual router.
4. Repeat Steps 2 and 3 for other virtual routers that you want to point to this name resolver.

Example To configure the virtual router *boston* to use the same name servers as the default router, enter the following commands.

```
host1(config)#virtual router boston
host1:boston(config)#ip domain-lookup transit-virtual-router default
```

ip domain-lookup transit-virtual-router

- Use to configure a virtual router to use the name servers you configured for another virtual router.
- Example

  host1:boston(config)#**ip domain-lookup transit-virtual-router default**

- Use the **no** version to stop a virtual router from using the same name servers you configured for another virtual router.

Monitoring DNS

After you configure DNS, you can use the **show ip domain-lookup** command to view information about the name servers.

show ip domain-lookup

- Use to display the name servers that you have specified on the system with the **ip name-server** command.
- Field descriptions
  - Bind to client—Name of the virtual router context in parentheses, followed by the name of the virtual router providing the name resolver
  - Using following Domain Name Servers—Name servers you assigned
  - Using following Local Domain Names—Default domain names you specified
- Example—The virtual router *boston* uses the name resolver on the default virtual router.

```
host1#show ip domain-lookup
Bind to client: (boston)default
Using following Domain Name Servers:
10.2.0.3
11.1.1.1
10.1.1.1
1:2:3:4:5:6:7:8:9:0:a:b:c:d:e:f
Using following Local Domain Names :
urlofinterest.com
concord
```

Troubleshooting the System

You can use **log** commands to discover and isolate problems with the system. For information about using the log commands, see the *JUNOSe System Event Logging Reference Guide, Chapter 1,* . Juniper Networks Customer Service can use core dump files to troubleshoot line module and SRP module failures.

Creating Core Dump Files

You can enable the system to create a core dump file if a module fails. You can choose to send the core dump file to an FTP server or save the file to NVS. Juniper Networks Customer Service can then access the core dump file and analyze it to determine what went wrong. Local core dumps—stored in NVS—are enabled by default. You can enable the core dump from Boot mode or Global Configuration mode.

CAUTION: Create a core dump file only under the direction of Juniper Networks Customer Service. Network function can be disrupted if you create a core dump file while the system is running in a network.

On the E120 router and the E320 router, the failure of some components on a line module generates multiple core dumps to provide more complete information about system state at the time of the failure. Other E-series routers generate only a single core dump for line module failures. When you contact Juniper Networks Customer Service for assistance, send all of the generated core dump files.

Boot Mode

To enable the core dump from Boot mode:

1. Access Boot mode by reloading the SRP module; then press the mb key sequence (case insensitive) during the countdown.
2. Specify where the system should transfer the core dump file.
3. Set the IP address and mask of the system interface over which you want to send the core dump file.
4. Specify the gateway through which the system sends the core dump file to the FTP server.
5. (Optional) Set a username and password for FTP access to the server where you transferred the core dump file.
6. Reload the operating system.

Example

```
:boot##exception dump 192.168.56.7 CORE_DUMPS
:boot##exception protocol ftp user_name user_password
:boot##exception gateway 192.168.12.3
:boot##exception source 10.10.33.8 255.255.255.0
:boot##reload
```

Global Configuration Mode

To enable the core dump from Global Configuration mode:

1. Access Global Configuration mode.
2. Specify where the system should transfer the core dump file.
3. Set the IP address and mask of the system interface over which you want to send the core dump file.

4. Specify the gateway through which the system sends the core dump file to the FTP server.
5. (Optional) Set a username and password for FTP access to the server where you want to transfer the core dump file.
6. (Optional) View parameters associated with creating a core dump file.

Example

```
host1(config)#exception dump 192.168.56.7 CORE_DUMPS
host1(config)#exception protocol ftp username userpassword
host1(config)#exception gateway 192.168.12.3
host1(config)#exception source 10.10.33.8 255.255.255.0
host1(config)#reload
```

exception dump

- Use to specify where the system should transfer the core dump file.
  - To send the file to an FTP server, enter the IP address of the FTP server and the name of the directory on the server to which the system will transfer the file.
  - To send the core dump file to NVS memory, use the **local** keyword.
- Local core dumps—stored in NVS—are enabled by default.
- Example

  host1(config)#**exception dump 192.168.56.7 CORE_DUMPS**
- Use the **no** version to disable the core dump.

exception gateway

- Use to specify the gateway through which the system sends the core dump file to the FTP server.
- Example

  host1(config)#**exception gateway 10.10.1.15**
- Use the **no** version to return the value to its default (null).

exception protocol ftp

- Use to set a username and password for FTP access to the server where you transferred a core dump file. The default settings are the username anonymous and no password.
- Specify the number 8 before the username and before the password to encrypt these values. By default, the username and password are not encrypted.
- Example

  host1(config)#**exception protocol ftp 8 user_core 8 user_password**
- Use the **no** version to restore the default settings.

exception source

- Use to set the IP address and mask of the system interface over which you want to send the core dump file to the FTP server.
- You can optionally include an IP address mask.
- Example

  host1(config)#**exception source 192.168.1.33 255.255.255.0**

- Use the **no** version to return the value to its default, null.

reload

- Use to reload the software on the router immediately.
- Reloads the system software (.rel) file and the configuration (.cnf) file.
- Reloading the standby SRP causes high availability to be temporarily disabled until the standby SRP reloads and resynchronizes with the active SRP.
- Example

  host1#**reload**

- There is no **no** version.

show exception dump

- Use to display the parameters associated with the core dump operation.
- Field descriptions
  - Dump host IP address—Address of the host where the system is configured to transfer the dump file
  - Dump directory—Name of directory on the host where the system is configured to transfer the dump file
  - Dump protocol—Protocol used to send the core dump file; currently only FTP is supported
  - User name—Name configured for access to the core dump file on the FTP server
  - Password—Password configured for access to the core dump file on the FTP server
  - Interface IP address—Address of the system interface configured to send the core dump file
  - Interface netmask—Mask of the system interface configured to send the core dump file
  - Gateway IP address—Address of gateway configured between the system and the FTP server

- Example

```
host1#show exception dump
Dump host IP address: 192.168.56.7
Dump directory:CORE_DUMPS/
Dump protocol: FTP
User name: user_name
Password: user_password
Interface IP address:
Interface netmask:
Gateway IP address:
```

Managing Core Dump Files

When a core dump occurs on a redundant SRP and you have the router configured to store network core dumps, the SRP that experiences the trouble retains the management Ethernet port to perform the core dump. This prevents the standby SRP from taking over operations until the core dump is complete.

When a router uses local NVS to store a core dump, the SRP does not need the management Ethernet port. However, because of the immense size of local core dump files, using NVS to store core dumps is not practical.

The SRP-120 available on the E120 router and the SRP-320 available on the E120 and E320 routers has a second NVS card which is dedicated to storing core dump files.

The core dump monitor eliminates the impact that core dumps may have on redundant routers by allowing you to manage core dump files in NVS. The core dump monitor allows you to automatically transfer core dump files from NVS to an FTP server location for storage. The core dump monitor can also automatically delete transferred core dump files.

The core dump monitor attempts to delete transferred files when all of the following conditions have been met:

- The router attempts to write a core dump file to NVS.
- NVS contains insufficient space to hold the new core dump file.
- The core dump files have already been transferred from NVS to an FTP server location using the automatic core dump monitor transfer process.

Only those core dump files that have already been transferred from NVS are considered for deletion. Of those, the oldest files are deleted first, and the router generates a log message for each core dump file it deletes.

NOTE: If the router NVS does not contain sufficient space to hold a new core dump file even after deleting all possible core dump files, the core dump fails and the router generates a log message for this condition.

Enabling and Disabling the Core Dump Monitor

The core dump monitor is disabled by default. To enable the core dump monitor, use the **exception monitor** command. Use the **no** version of this command to disable the core dump monitor.

exception monitor

- Use to enable the router core dump monitor and specify the location to which you want the router to transfer core dump files.
- To send the file to an FTP server, enter the IP address of the FTP server and the name of the directory on the server to which the system will transfer the file.
- Enabling the core dump monitor specifies that future core dump files be saved to NVS. See the **exception dump** command for details.
- Example

  host1(config)#**exception monitor 192.168.56.7 CORE_DUMPS**

- Use the **no** version to disable the core dump monitor.

NOTE: You can use the **exception protocol ftp** command to assign a username and password to the targeted FTP server. If you choose not to define a username or password, the router uses the values of "anonymous" and "null," respectively.

Specifying the Core Dump Monitor Interval

To specify the length of time that the router waits between checking for core dump files, use the **exception monitor interval** command. Use the **no** version of this command to revert the core dump monitor interval to its default value of 60 minutes (1 hour).

exception monitor interval

- Use to specify the interval (in minutes) at which you want the router to check NVS for core dump files.
- Example

  host1(config)#**exception monitor interval 1000**

- Use the **no** version to revert the core dump monitor interval to its default value, 60 minutes.

Viewing Core Dump Monitor Status

To view information about core dump monitor status and configuration, use the **show exception monitor** command.

show exception monitor

- Use to display information about the core dump monitor status and configuration.
- Field descriptions
  - Core dump monitor—Status (enabled or disabled) of the core dump monitor
  - Next dump monitor check time—Time at which the core dump monitor will next check for any new core dump files
  - Host—IP address of the FTP host on which the core dump monitor saves core dump files

- Directory—Directory or directory path on the host to where the core dump files are located
- Core dump monitor interval—Time interval (in minutes) at which the core dump monitor checks for any new core dump files
- Files on flash which have been transferred—A list of core dump files in the router NVS that have already been transferred to the FTP host
- Files on flash which have not been transferred—A list of core dump files in the router NVS that have not yet been transferred to the FTP host

- Example

```
host1#show exception monitor
Core dump monitor is enabled
Next dump monitor check time: WED AUG 16 2003 15:50:38 UTC
Host: 10.10.120.99
Directory: monitor
Core dump monitor interval(minutes): 10

Files on flash which have been transferred
------------------------------------------
standby:OC12Atm(P2)_5_IC_ERX-10-16-5b_09_15_2002_11_59.dmp
SRP-5GPlus_1_SC_tImBo-lAb-3_09_18_2002_19_39.dmp

Files on flash which have not been transferred
----------------------------------------------
standby:SRP-10Ge_1_SC_ERX-10-24-36_09_24_2002_11_04.dmp
OC12-SERVER_5_FC1_E_ERX-10-24-36_03_28_2003_12_44.dmp
E3_1_IC_ERX-10-0f-ab_10_08_2002_16_10.dmp
```

Accessing the Core Dump File

If a module fails and saves a core dump file to NVS memory (which can take several minutes), and you have not configured the Core Dump Monitor for automatic transfer, you must transfer the file to a network host before it can be examined. You can transfer the core dump file when the module is back online or has assumed a redundant status. For information about the status of modules, see *ERX Hardware Guide, Chapter 9, Troubleshooting*. To transfer the core dump file to a network host, use the **copy** command.

In a system with two SRP modules, the following behavior applies if you have configured the SRP modules to save core dump files to an FTP server:

- If the primary SRP module fails, it saves the core dump file to the FTP server before the standby SRP module assumes control.

- If the standby SRP module fails, it must save the core dump file to NVS because it has no access to any configured network host.

The **show version** command output indicates the failed SRP module state as not responding during the save process. Consequently, when the failed SRP module recovers and assumes the role of redundant module, the **show version** command output indicates the SRP module state as standby and displays output for the standby SRP. The standby SRP can notify the primary SRP during a core dump. Output from the **show version** command displays core dumping for the Standby SRP.

If the standby SRP boot image encounters a problem loading the diagnostics or operational image, the state of the standby SRP appears as disabled (image error). When standby SRP diagnostics encounter a test failure, the primary SRP is notified and the state is set to hardware error.

You can now transfer the core dump file to a network host for examination. For example, to transfer the file *SRP_1_SC_05_24_2000_02_20.dmp* from NVS of the failed SRP module to the host server1, enter the following command:

```
host1#copy SRP_1_SC_05_24_2000_02_20.dmp
host:/public/server1/SRP-5G_1_SC_05_24_2000_02_20.dmp
```

copy

- Use to copy a core dump file.
- You cannot use wildcards.
- You can copy core dump files only to network locations.
- You cannot create or copy over files generated by the system; however, you can copy such files to an unreserved filename.
- Example

  ```
  host1#copy fault.dmp host:/public/server1/fault.dmp
  ```

- There is no **no** version.

Capturing and Writing Core Dumps

You can capture and write a core dump to a file for an active or a standby SRP module or the line modules. You can store the file on the file system or on a network host. The SRP core dump files are stored on the respective SRP flash memory. The line module core dump files are stored on the active SRP flash memory at the instance of the core dump event. The core dump files are not synchronized between the active and the standby SRP module. You can use the resulting information to help diagnose a problem or to verify whether the core settings are correct (primarily for the network settings).

write core

- Use to reboot the active SRP module, the standby SRP module, or the module in a specified slot, and write the core dump to a file.
- If you specify the **force** keyword, you are prompted for confirmation to reboot when the router is in a state that can lead to loss of configuration data or NVS corruption.

NOTE: The **force** keyword enables you to specify a slot only if that slot is an SRP module slot.

- If you do not specify a reason, Write Core is the default reason recorded in the reboot history.
- Example 1—Prompts for confirmation to reboot

  ```
  host1#write core force
  ```

- Example 2—Reboots the module in slot 7 and writes a core memory file

  host1#**write core slot 7**

- There is no **no** version.

Understanding the Core Dump File

The dump file indicates which module has failed by referencing that module's hardware slot number. The hardware slot number is the slot number designation on the systems's backplane. This slot number is different from the chassis slot number that appears on the front of the chassis and in screen displays (for example, in the display resulting if you issue the **show version** command).

Table 36 shows how the chassis slot numbers relate to the hardware slot numbers.

Table 36: Chassis Slot Numbers Versus Hardware Slot Numbers

Slot Number on Chassis	ERX-7xx Model Hardware Slot Number	ERX-14xx Model Hardware Slot Number	E320 Model Hardware Slot Number
0	1	0	16
1	2	1	17
2	3	2	18
3	4	3	19
4	5	4	20
5	6	5	21
6	7	7	8
7	8	9	10
8	–	10	9
9	–	11	12
10	–	12	13
11	–	13	25
12	–	14	26
13	–	15	27
14	–	–	28
15	–	–	29
16	–	–	30

Tracking IP Prefix Reachability

You can use the **track** command to define an IPv4 prefix object and track its reachability. The **show track** command displays the tracked information for any specified objects.

show track

- Use to display tracking details for the object you specify.
- Field descriptions
  - Track—Name of the object being tracked
  - IP Route—IP prefix being tracked
  - Virtual router—Virtual router on which the object resides
  - First-hop interface—Outgoing interface to reach the prefix
  - changes—Number of times the object has changed state
  - Tracked by—Application that is doing the tracking
- Example

```
host1(config)#show track ERX_Bangalore

Track ERX_Bangalore
 IP Route 1.1.1.0 255.255.255.0 reachability
 in virtual router 1
 Reachability is Up
 First-hop interface is FastEthernet3/0
 2 change(s)
Tracked by:
 Vrrp in virtual router 1
```

show track brief

- Use to display a one-line summary of all objects being tracked.
- Field descriptions
  - Object—Name of the object being tracked
  - Type—Type of object being tracked
  - Parameter—Parameter type being tracked
  - Value—State of the object being tracked
- Example

```
host1(config)#show track brief

Object  Type            Parameter       Value
ERX-WF  IP-route        reachability    Up
ERX-BNG IP-route        reachability    Up
```

track

- Use to create an IPv4 object and to track its reachability.
- The name of the object must be unique for the chassis.
- Use the **vrf** keyword to specify the VRF on which the IP prefix resides.

- Example

  host1(config)#**track ERX_Bangalore vrf VR1 ip-route 10.10.24.6 255.255.0.0 reachability**

- Use the **no** version to delete the object and stop tracking for that object.

Gathering Information for Customer Support

When you report a problem with your router, customer support personnel from the Juniper Networks Technical Assistance Center (JTAC) may request that you issue the **show tech-support** command. This command was created to help streamline the information-gathering process by providing a large amount of router information from one command and avoiding the need to access certain diagnostic commands.

The **show tech-support** command functions like any other show command, and you can issue this command the same way you issue any other show commands on the router. This means that you can redirect the output from the command to a file. For information about redirecting show command output, see *Redirection of show Command Output* on page 40.

Another command that customer support personnel might ask you to use is the **tech-support encoded-string** command. Customer support will provide you with an encoded string of commands that this command then executes.

tech-support encoded-string

- Use to execute an encoded command string provided by Juniper Networks customer support personnel.
- This command requires privilege level 15 access.
- Optionally, specify a slot number on the router.
- Optionally, specify a reliable or fast connection type; fast does not work under some conditions. The default connection type is reliable.
- Example 1

  host1(config)#**tech-support encoded-string debug 1**

- Example 2

  host1(config)#**tech-support slot 0 connection fast encoded-string debug1**

- There is no **no** version.

show tech-support

- Use to display technical support information used by Juniper Networks customer support personnel to assist in troubleshooting the router.
- Example

```
host1#show tech-support
Show Technical Support
------------------------------------------------------------------------------

System Name     : host1
Time            : THU JUL 15 2004 17:12:48 UTC
System up since : WED JUN 30 2004 16:07:51 UTC
```

```
Software release: 1088523900
Boot Flags      : 0x100663296
Slot Number     : 0
Serial Number   : 7100170293
Assembly Number : 3400003701
Assembly Rev    : A07
Description     :

Command List:
CLI:show version
CLI:show boot
CLI:show hardware
CLI:show redundancy
CLI:show environment
CLI:show users detail
CLI:show utilization
CLI:show process cpu
CLI:show process memory
....
```

Managing and Monitoring Resources

The resource threshold monitor (RTM) allows you to set the rising and falling thresholds and trap hold-down times for certain interfaces. You can also view the resource threshold information.

Enabling and Disabling the Resource Threshold Monitor

You may want to set thresholds for certain interface resources on the router. The RTM allows you to specify rising and falling thresholds as well as hold-down times for certain interfaces by using the **resource if-type** and **resource threshold** commands.

resource if-type

- Use to specify rising and falling thresholds and hold-down times for certain interfaces on a slot or systemwide basis.
- Example

  host1(config)#**resource if-type ip slot 4 falling 500**

- Use the **no** version to set the threshold parameter to its default value (for rising, 90 percent of the maximum value of the resource; for falling, 1 percent of the maximum value of the resource; for hold-down time, 300 seconds).

resource threshold

- Use to disable the issuance of trap messages when the router reaches preset threshold limits.
- Example

  host1(config)#**resource threshold disable traps**

- Use the **no** version to reenable traps for resource threshold conditions.

Viewing Resource Threshold Information

The RTM allows you to view information about resource use on the router. The show resource command displays statistical information about resources and their current threshold configurations.

show resource

- Use to display statistical information about resources and their current threshold configurations.
- Field descriptions
  - Resource Threshold Trap—Status (enabled or disabled) of the resource threshold trap
  - type—Interface type
  - location—Location of the interface (system or slot location)
  - max capacity—Maximum capacity of the interface at either the system or slot level
  - current value—Current capacity of the interface at either the system or slot level
  - rising threshold—Rising threshold setting for the interface at either the system or slot level
  - falling threshold—Falling threshold setting for the interface at either the system or slot level
  - hold-down time—Hold-down time setting for the interface at either the system or slot level
- Example 1

```
host1#show resource
Resource Threshold Trap: enabled
                                          max      current    rising
           type               location   capacity    value    threshold
---------------------------   --------   --------   -------   ---------
ip interface                  system        32000         1       28800
ip interface                  slot 3         8192         0        7373
ip interface                  slot 4         4095         0        3686
atm-sub-if interface          system        65536         0       58982
atm-vc interface              system        65536         0       58982
ppp-link interface            system        32768         0       29491
ppp-link interface            slot 3         2048         0        1843
ppp-link interface            slot 4            6         0           5
atm-active-sub-if interface   system        65536         0       58982
                                         falling    hold-down
           type               location   threshold     time
---------------------------   --------   ---------   ---------
ip interface                  system           320         300
ip interface                  slot 3            82         300
ip interface                  slot 4            41         300
atm-sub-if interface          system           655         300
atm-vc interface              system           655         300
ppp-link interface            system           328         300
ppp-link interface            slot 3            20         300
ppp-link interface            slot 4             0         300
atm-active-sub-if interface   system           655         300
```

- Example 2

```
host1#show resource threshold trap
Resource Threshold Trap: enabled
```

Monitoring the System

This section provides basic system commands that allow you to display information about the router's state. The **show configuration** command, for example, allows you to display the router's entire configuration.

baseline show-delta-counts

- Use to configure the system to always display statistics relative to the most recent appropriate baseline.
- The system collects many statistics during its operation. Various **show** commands are available to display these statistics. Baselining allows the user to identify a point in time relative to which such statistics can be reported.
- Typically, the optional **delta** keyword is used with **show** commands to specify that baselined statistics are to be shown. This command applies the "delta" function implicitly.
- Example

  host1#**baseline show-delta-counts**

- Use the **no** version to have access to the total statistics.

show configuration

- Use to display the current (running) configuration of the router, a specified virtual router, a specified interface, or a specified category of router settings.
- See full description and examples in **show configuration** on page 232.

show environment

- Use to display information about the router's physical environment, such as voltage or temperature.
- Optionally, specify the **all** keyword to view both the system environment information and the detailed temperature status table, or specify the **table** keyword to view only the temperature status table.
- The system displays a message if the voltage or temperature exceeds normal operating limits.
- The system enters thermal protection mode if the temperature exceeds maximum operating limits or if the fan system on the E120 router or the E320 router reports a critical error. For information about thermal protection mode on ERX-7xx models, ERX-14xx models, and the ERX-310 router, see *ERX Hardware Guide, Chapter 9, Troubleshooting*. For information about thermal protection mode on the E120 and E320 routers, see *E120 and E320 Hardware Guide, Chapter 9, Troubleshooting*.

- Field descriptions
  - chassis—Number of slots, midplane identifier, and hardware revision number
    - 14Slot—5 Gbps, 14 slot midplane
    - midplaneId7Slot—5 Gbps, 7 slot midplane
    - midplaneIdRx1400—10 Gbps ASIC compatible, 12 line module slots, 2 SRP module slots for ERX-14xx models
    - midplaneIdRx700—10 Gbps ASIC compatible, 5 line module slots, 2 SRP module slots for ERX-7xx models
    - 17 slot—100 or 320 Gbps, 17-slot midplane for the E120 router
    - 11 slot—320 Gbps, 11-slot midplane for the E120 router
  - fabric—Capacity and hardware revision of the fabric
  - fans—Status of fans
  - nvs—Status and capacity of NVS and amount of space used
  - power—States of power feeds
  - AC power—For ERX-310 routers only; states of power feeds
  - srp redundancy—Availability of a redundant SRP module
  - slots: cards missing or offline—Status of each slot
    - online
    - standby
    - offline
    - empty
  - line redundancy—Number of redundancy groups installed
    - width—Number of slots the redundant midplane covers
    - spare—Slot that contains a spare line module
    - primary—Slot that contains the primary line module
  - fabric redundancy—Status of redundancy on the switch fabric on the E120 and E320 routers
    - ok
    - none
  - temperature—Status of the system temperature
  - timing—Source of the timing signal
    - primary—Type and status of the primary timing signal
    - secondary—Type and status of the secondary timing signal
    - tertiary—Type and status of the tertiary timing signal
    - auto-upgrade—Status of the auto-upgrade parameter, which enables the system to revert to a higher-priority timing source after switching to a lower-priority timing source.

- system operational—Status of the system
- slot—Number of the slot in which the module resides
- type—Type of module in the slot on the E120 and E320 routers
- temperature—Temperature of the line module, SRP module, or SFM on the E120 and E320 routers
- processor temperature—Temperature of the line module or SRP module
- processor temperature status—Temperature condition of the line module
  - normal—Temperature is in normal range
  - too hot—Module is too hot; system will go into thermal protection mode if the temperature of any module exceeds 80° C
  - too cold—Module is too cold; system will go into thermal protection mode if the temperature of any module drops below –5° C
- IOA temperature—Temperature of the corresponding I/O module or IOA
- IOA temperature status—Temperature condition of the corresponding I/O module or IOA
  - normal—Temperature is in normal range
  - too hot—Module is too hot; system will go into thermal protection mode if the temperature of any module exceeds 80° C
  - too cold—Module is too cold; system will go into thermal protection mode if the temperature of any module drops below –5° C
- processor temperature ranges—Displays the temperature ranges for the line modules and SRP modules

- IOA temperature ranges—Displays the temperature ranges for the I/O modules on ERX-7xx models, ERX-14xx models, and the ERX-310 router or IOAs on the E120 and E320 routers
- fabric temperature ranges—Displays the temperature ranges for the SRP modules and SFMs on the E120 and E320 routers
- Example 1—Displays the environment of an ERX-7xx model

```
host1#show environment all
    chassis: 14 slot (id 0x3, rev. 0x0)
    fabric: 5 Gbps (rev. 1)
    fans: ok
    nvs: ok (81MB flash disk, 54% full)
    power: A ok, B not present
    AC power: A not present, B not present
    srp redundancy: none
*** slots: cards missing or offline
        online: 6 9
        standby: 8
        offline: 2
        empty: 0 1 3 4 5 7 10 11 12 13
    line redundancy: 1 redundancy group(s)
        width 6, spare 8, primary 9
    temperature: ok
    timing: primary
        primary: internal SC oscillator (ok)
        secondary: internal SC oscillator (ok)
```

```
        tertiary: internal SC oscillator (ok)
        auto-upgrade enabled
*** system operational: no

        processor     processor        IOA           IOA
       temperature   temperature   temperature   temperature
slot   (10C - 70C)     status      (10C - 70C)     status
----   -----------   -----------   -----------   -----------
0          31        normal            30        normal
3          31        normal            30        normal
5          31        normal            30        normal
7          31        normal            30        normal
processor temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
IOA temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
```

- Example 2—Displays the environment of an E320 router

```
host1#show environment all

    chassis: 17 slot (id 0x3, rev. 0x0)
    fabric: 100 Gbps (rev. 1)
    fans: fanSubsystemOk
    nvs: ok (977MB flash disk, 29% full), matches running config
    power: A ok, B not present
    srp redundancy: mode is file-system-synchronization       auto-sync
enabled, switch-on-error enabled
status unknown
*** slots: cards missing or offline
online: 0 6 13
offline: 7
empty: 1 2 3 4 5 11 12 14 15 16
fabric slots: ok
online: 6 7 8 9 10
line redundancy: none
temperature: ok
timing: primary
primary: internal SC oscillator (ok)
secondary: internal SC oscillator (ok)
tertiary: internal SC oscillator (ok)
auto-upgrade enabled
fabric redundancy: ok

*** system operational: no

                              temperature   temperature
slot          type            (10C - 70C)     status
----   ------------------     -----------   -----------
0      LM-4                       42        normal
0/1    GE-4 IOA                   23        normal
6      SRP-100                    32        normal
6      SFM-100                    32        normal
6/0    SRP IOA                    25        normal
7      SFM-100                    30        normal
8      SFM-100                    23        normal
9      SFM-100                    25        normal
```

```
10     SFM-100                  24        normal
13     LM-4                     24        normal
13/0   GE-4 IOA                 23        normal

fabric temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
processor temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
IOA temperature ranges
        below -5C is too cold
        above 80C is too hot
        low temperature warning below 10C
        high temperature warning above 70C
```

- Example 3—Displays the environment on an E120 router

```
host1#show environment all
    chassis: 11 slot (id 0x8, rev. 0x0)
    fabric: 120 Gbps (rev. 1)
    fans: fanSubsystemOk
    nvs: ok (998MB flash disk, 14% full), matches running config
    power: A ok, B not present
    srp redundancy: mode is file-system-synchronization        auto-sync
enabled, switch-on-error enabled
in sync
slots: ok
online: 1 2 6
standby: 7
empty: 0 3 4 5
fabric slots: ok
online: 6 7 8 9 10
line redundancy: none
temperature: ok
timing: primary
primary: internal SC oscillator (ok)
secondary: internal SC oscillator (ok)
tertiary: internal SC oscillator (ok)
auto-upgrade enabled
fabric redundancy: ok

system operational: yes

                 temperature   temperature
slot     type    (10C - 56C)     status
----   --------  -----------   -----------
1      LM-10          37        normal
1/1    GE-8 IOA       35        normal
2      LM-10          37        normal
2/1    GE-8 IOA       39        normal
6      SRP-120        40        normal
6      SFM-120        40        normal
6/0    SRP IOA        30        normal
7      SRP-120        41        normal
7      SFM-120        41        normal
8      SFM-120        31        normal
9      SFM-120        32        normal
10     SFM-120        32        normal
```

```
fabric temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
processor temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 51C
IOA temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
```

- Example 4—Displays the temperature status table on an E120 router

```
host1#show environment table

                  temperature   temperature
slot     type     (10C - 56C)     status
----   --------   -----------   -----------
1      LM-10          37        normal
1/1    GE-8 IOA       35        normal
2      LM-10          37        normal
2/1    GE-8 IOA       39        normal
6      SRP-120        40        normal
6      SFM-120        40        normal
6/0    SRP IOA        30        normal
7      SRP-120        41        normal
7      SFM-120        41        normal
8      SFM-120        31        normal
9      SFM-120        32        normal
10     SFM-120        32        normal

fabric temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
processor temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 51C
IOA temperature ranges
        below -5C is too cold
        above 79C is too hot
        low temperature warning below 10C
        high temperature warning above 56C
```

show fabric weights

- Use to display multicast-to-unicast ratio for the router switch fabric.
- Field descriptions
  - multicast—Ratio value of multicast bandwidth
  - unicast—Ratio value of unicast bandwidth
- Example

```
host1#show fabric weights

Fabric scheduler weights: multicast = 1 , unicast = 8
```

show hosts

- Use to display a list of configured network servers.
- Field descriptions
  - Static Host Table—Information about the connected static hosts
    - name—Name of the host
    - ip address—IPv4 or IPv6 address of the host
    - type of host—Type of host; for example, ftp means an FTP server
  - NFS Host Table—Information about connected NFS servers
    - name—Name of the NFS server
    - userid—Identity for the user
    - groupid—Identity for the group
- Example

```
host1#show hosts
     Static Host Table
     -----------------
name       ip address    type
----       ----------    ----
host1      10.2.0.124    ftp
hFtp       10.5.6.7      ftp
hTftp      10.5.6.7      tftp
    Static Host Table
    -----------------
name        ip address                              type
-----   ---------------------------------------     ----
george   1111:2222:3333:4444:5555:6666:7777:8888   ftp
dsw      10.10.121.42                               ftp
deab     10.6.128.12                                ftp
mFtp     10.10.121.11                               ftp
mTftp    10.10.121.11                               tftp
mary     10.10.121.11                               ftp
sd       10.10.121.80                               ftp

    NFS Host Table
    --------------
name   userid   groupid
----   ------   -------
deab    2001     100
```

show processes cpu

- Use to display the CPU use.
- Field descriptions
  - task name—Name of the process
  - times invoked—Number of times the process has been invoked
  - invocations per second—Frequency of the process invocation
  - total running time (msec)—Time the process has been running
  - percent running time—Percentage of the total running time attributable to this process
  - average time per invocation (usec)—Average number of microseconds per invocation of this process
  - 5 second utilization (%)—CPU use by the process for the last 5 seconds
  - 1 minute utilization (%)—CPU use by the process for the last minute
  - 5 minute utilization (%)—CPU use by the process for the last 5 minutes
- Example

```
host1#show processes cpu
                        Process Statistics
                        ------------------

                                                 total
                                 invocations     running     percent
                        times        per          time       running
      task name        invoked     second        (msec)      time
---------------------  -------  -----------   --------   -------
aaaAtm1483Config             1            0          0        0%
aaaServer                   52            0        260        0%
agent1                     399            0       3600        0%
ar1EthHelp              362856            4        590        0%
.
.
.
templateMgr                 48            0        540        0%
timerd                2346566           32          0        0%
~GONE~                 405202            5     184700        0%
~IDLE~                      0            0        360        0%
~INTERRUPT~           8840490          121      51050        0%

                        average
                          time          5            1            5
                          per         second       minute       minute
                        invocation   utilization  utilization  utilization
      task name           (usec)        (%)          (%)          (%)
---------------------   ----------   ----------   ----------   ----------
aaaAtm1483Config                0            0            0            0
aaaServer                    5000            0            0            0
agent1                       9022            0            0            0
ar1EthHelp                      1            0            0            0
ar1InternalNetwork             19            0            0            0
.
.
.
~IDLE~                        ---            0            0            0
~INTERRUPT~                     5            0            0            0
```

show processes memory

- Use to display the amount of memory-related resources used by system processes. Because the router allocates memory to system processes in chunks, issuing this command performs a cleanup process to gather unused, available memory for reallocation.
- You can display different output variations by using the **application**, **slot**, and **virtual-router** keywords. In addition, you can combine these keywords in specific ways to display information combinations of application, slot, and virtual router.
- The appearance of parentheses in the output is significant. The parentheses indicate "partial accountability" of the current memory size. In other words, the values are accurate for the row in which they appear, but the memory value used for calculating the sum total for the column may be smaller than the value displayed. This can result in the sum total for the "current size" column not matching the sum of the values that appear within the column. This disparity can occur under shared memory conditions where a portion of the memory size for one or more of the virtual routers may be accounted for elsewhere, resulting in a lower column total.
- Field descriptions
  - Memory usage summary—Statistical information about the memory usage information being displayed
  - application—Name of the application being viewed (if applicable); asterisk (*) if no application is specified
  - router—Name of the virtual router being viewed (if applicable); asterisk (*) if no virtual router is specified
  - app—Application to which the statistics information applies
  - rtr—Virtual router to which the statistics information applies
  - vrf—Virtual routing and forwarding instance to which the statistics information applies
  - _unassoc_—Special virtual router output category that summarizes all memory that is not currently associated with any particular virtual router
  - current size—Amount of memory reserved by the listed application or virtual router
  - utilization—Percentage of reserved memory currently used for the listed application or router
  - headroom—Amount of memory overage available to each listed application or virtual router (if needed); 100% indicates an unlimited headroom (that is, no memory limits are set for the application or virtual router)
- Example 1

```
host1#show processes memory application

*** Memory usage summary (by application, 37 total) ***
    application: *
         router: *

              current
   app         size   utilization headroom
```

```
---------- ------- ----------- --------
aaa             98K           3%      100%
bgp             90K          28%      100%
bridge           1M           4%      100%
cli              3K           8%      100%
dcm             64K           7%      100%
dhcp           644K           0%      100%
dns              4K           6%      100%
dvmrp           36K           0%      100%
ethernet         3K          75%      100%
forwarding      20K          50%      100%
gplaan          52K           0%      100%
igmp             1K           0%      100%
.
.
```

- Example 2

```
host1#show processes memory virtual-router

*** Memory usage summary (by router, 4 total) ***
    application: *
         router: *

          current
   rtr     size   utilization headroom
--------- ------- ----------- --------
_unassoc_   (40M)           7%       99%
default    (339K)          23%      100%
test       (366K)          23%      100%
vr5        (327K)          18%      100%
--------- ------- ----------- --------
Total:        41M           7%       99%
```

- Example 3

```
host1#show processes memory virtual-router vr5 application ip

*** Memory usage summary (by VRF) ***
    application: ip
         router: vr5

    current
vrf  size   utilization headroom
--- ------- ----------- --------
vr5   (19K)          48%      100%
```

show reboot-history

- Use to display the history of system and module resets.
- You can display the current reboot.hty file or a saved reboot history file.
- If you have a redundant router, it can be convenient to copy the redundant module's reboot.hty file to another filename for viewing with this command.
- Field descriptions
  - Entry—Number of entry in the reboot history; numbers range from lowest (most recent reset) to highest (oldest reset)
  - time of reset—Timestamp for reset
  - run state—State of system at reset
  - image type—Type of image running when the record is written

- boot—Module is running the boot file
- diagnostics—Module is running the diagnostics file
- application—Module is running the software file

- location—Slot that reset; location is offset by two slots at slot 7 and above (the SRP module in slot 6 shows location as slot 7, the SRP module in slot 7 shows location as slot 9, and slots 8-13 show location as 10-15, respectively).
- build date—Build date of software version
- reset type—Cause of reset

- Example

```
host1#show reboot-history
*** Entry  1 ***
time of reset: TUE APR 10 2001 20:25:59 UTC
run state: unknown
image type: diagnostics
location: slot (7)
build date: 0x3abf4337 MON MAR 26 2001 13:25:11 UTC
reset type: user reboot, task "scheduler", reason "not specified"
*** Entry  2 ***
time of reset: TUE APR 10 2001 20:25:44 UTC
run state: unknown
image type: diagnostics
location: slot (8)
build date: 0x3abf5d5f MON MAR 26 2001 15:16:47 UTC
reset type: user reboot, task "scheduler", reason "not specified"
*** Entry  3 ***
time of reset: TUE APR 10 2001 20:25:03 UTC
run state: unknown
image type: diagnostics
location: slot (4)
build date: 0x3abf3ee0 MON MAR 26 2001 13:06:40 UTC
reset type: user reboot, task "scheduler", reason "not specified"
```

show running-configuration

- Use to display the configuration currently running on the router, a specified virtual router, a specified interface, or a specified category of router settings.
- See full description and examples in **show running-configuration** on page 234.

show version

- Use to display the armed and running releases for every slot in the router and the operational status of the SRP module and line modules for all E-series routers.
- Use the **all** keyword with the E120 router and the E320 router to display the operational status of the IOAs.
- Field descriptions
  - Model identification
  - Copyright—Copyright details for the system software
  - System Release—Filename, version, and date of the system software currently running on the router

- System running for—How long the router has been running (time elapsed since the last boot of the router), date and time of last boot; does not reflect the uptime of a particular SRP module
- slot—Physical slot that contains the line module
- state—Status of the line module
  - booting—Line module is booting
  - disabled (assessing)—Router is evaluating the status of this line module
  - disabled (admin)—Line module disabled by **slot disable** command
  - disabled (cfg error)—Use of the line module in this slot violates the permitted configuration for the router. For example, the fabric cannot supply sufficient bandwidth to the line module in this position.
  - disabled (image error)—Software for this line module is missing or corrupted
  - disabled (mismatch)—Line module in this slot is a different type from that specified in the software. Correct the condition by inserting the original module, or use the **slot accept** command to find information about the new module.
  - hardware error—Line module has a hardware fault
  - inactive—On ERX routers, either the I/O module is not present or the primary line module is fully booted and ready to resume operation. In the latter case, the standby is currently providing services. On E120 and E320 routers, one of the following conditions exists: the primary line module has no IOAs; or the primary line module has IOAs, but they have failed diagnostics; or the standby line module has taken over for the primary line module, and has control of the IOAs.
  - initializing—Transitional state before the line module proceeds to the online, standby, or inactive state; diagnostics are complete, module is initializing software
  - online—Line module is operating
  - not present—Line module configured for this slot is missing
  - not responding—Line module has a hardware or ROM problem
  - standby—Spare line module or SRP module is fully booted and ready to operate if the primary line module or active SRP module fails
  - unknown—Transitional state while the SRP is initializing
- type—Kind of module; an “e” at the end of an SRP module type (for example, SRP-5Ge) indicates that the module includes error checking code (ECC)
- admin—Status of the slot in the software
  - enabled—Slot is enabled
  - disabled—Slot is disabled
- spare—Line module is a spare for line module redundancy
- running release—Software that is running on the line module

- slot uptime—Length of time for which the module has been operational; a value of --- indicates that the module is not available.
- The following symbols and notices may be displayed at the end of the report:
  - # This release is a result of a subsystem override
  - * This release is a result of a "boot slot" override
  - # The running or armed release on the slot is the same as the armed release for a subsystem. A subsystem is all the line modules of one type, such as OC3.
  - * This release reflects whichever release the router is armed with at startup.

- Example 1—Displays the version of an ERX-7xx model

```
host1#show version

Juniper Edge Routing Switch ERX-700
Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
System Release: erx_7-1-0.rel Partial
       Version: 7.1.0 [BuildId 4518]   (December 21, 2005  11:23)
System running for: 25 days, 3 hours, 31 minutes, 5 seconds
       (since THU DEC 22 2005 11:36:41 UTC)

slot  state     type     admin  spare  running release    slot uptime
---- ------- ---------- ------- ----- ------------------ --------------
0    standby SRP-10Ge   enabled  ---  erx_7-1-0.rel           ---
1    online  SRP-10Ge   enabled  ---  erx_7-1-0.rel      25d03h:28m:49s
2      ---      ---       ---    ---         ---             ---
3      ---      ---       ---    ---         ---             ---
4    online  CT3-12     enabled  ---  erx_7-1-0.rel      25d03h:24m:46s
5    online  OC3-4A-APS enabled  ---  erx_7-1-0.rel      25d03h:24m:22s
6    online  GE         enabled  ---  erx_7-1-0.rel      25d03h:24m:44s
```

- Example 2—Displays the version of an E320 router

```
host1#show version
Juniper Edge Routing Switch E320
Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
System Release: 7b12.rel
       Version: 7.0.0 [BuildId 3468]   (April 29, 2005  10:46)
System running for: 2 days, 19 hours, 16 minutes, 17 seconds
       (since FRI MAY 13 2005 15:10:54 UTC)

                                    running

slot  state   type    admin  spare  release   slot uptime

---- ------- ------- ------- ----- --------- -------------
0    online  LM-4    enabled  ---  7b12.rel  2d19h:13m:24s
1      ---     ---     ---    ---     ---         ---
2    online  LM-4    enabled  ---  7b12.rel  2d19h:13m:19s
3      ---     ---     ---    ---     ---         ---
4      ---     ---     ---    ---     ---         ---
5      ---     ---     ---    ---     ---         ---
6    online  SRP-100 enabled  ---  7b12.rel  2d19h:14m:48s
6    online  SFM-100 enabled  ---     ---    2d19h:14m:47s
7    standby SRP-100 enabled  ---  7b12.rel       ---
7    online  SFM-100 enabled  ---     ---    2d19h:14m:42s
8    online  SFM-100 enabled  ---     ---    2d19h:14m:44s
```

```
9    online  SFM-10O enabled  ---     ---    2d19h:14m:39s
10   online  SFM-10O enabled  ---     ---    2d19h:14m:40s
11     ---     ---     ---    ---     ---         ---
12   online  LM-4    enabled  ---  7b12.rel  2d19h:13m:13s
13     ---     ---     ---    ---     ---         ---
14   online  LM-4    enabled  ---  7b12.rel  2d19h:13m:08s
15     ---     ---     ---    ---     ---         ---
16     ---     ---     ---    ---     ---         ---
```

■ Example 3—Displays the version of an E320 router using the **all** keyword

```
host1#show version all
Juniper Edge Routing Switch E320
Copyright (c) 1999-2006 Juniper Networks, Inc.  All rights reserved.
System Release: 7-3-0.rel
        Version: 7.3.0 [BuildId 5759]   (July 27, 2006  10:40)
System running for: 3 days, 1 hour, 37 minutes, 4 seconds
        (since FRI JUL 28 2006 09:08:14 UTC)

                                                    running
slot  state         type          admin  spare    release     slot uptime
---- ------- ------------------- ------- ----- ------------- -------------
0    online  LM-4                enabled  ---    7-3-0.rel   3d01h:29m:01s
0/0  present 10GE IOA            enabled  ---                      ---
0/1    ---          ---           ---    ---       ---           ---
1    online  LM-4                enabled  ---    7-3-0b.rel  3d01h:26m:36s
1/0  present OC12/STM4-2 POS IOA enabled  ---                      ---
1/1    ---          ---           ---    ---       ---           ---
2    online  LM-10 Uplink        enabled  ---    7-3-0.rel   2d18h:27m:46s
2/0  present 10GE PR IOA         enabled  ---                      ---
2/1    ---          ---           ---    ---       ---           ---
3    online  LM-4                enabled  ---    7-3-0.rel   2d19h:03m:53s
3/0  present 10GE IOA            enabled  ---                      ---
3/1    ---          ---           ---    ---       ---           ---
4    online  LM-10 Uplink        enabled  ---    7-3-0.rel   3d01h:24m:39s
4/0  present 10GE PR IOA         enabled  ---                      ---
                                                    running
slot  state         type          admin  spare    release     slot uptime
---- ------- ------------------- ------- ----- ------------- -------------
4/1    ---          ---           ---    ---       ---           ---
5      ---          ---           ---    ---       ---           ---
5/0    ---          ---           ---    ---       ---           ---
5/1    ---          ---           ---    ---       ---           ---
6    standby SRP-320             enabled  ---    7-3-0.rel        ---
6    online  SFM-320             enabled  ---       ---      3d01h:33m:48s
7    online  SRP-320             enabled  ---    7-3-0.rel   3d01h:34m:04s
7    online  SFM-320             enabled  ---       ---      3d01h:33m:59s
7/0  present SRP IOA             enabled  ---                      ---
8    online  SFM-320             enabled  ---       ---      3d01h:34m:03s
9    online  SFM-320             enabled  ---       ---      3d01h:33m:50s
10   online  SFM-320             enabled  ---       ---      3d01h:33m:53s
11   online  LM-4                enabled  ---    7-3-0.rel   3d01h:26m:43s
11/0 present OC12/STM4-2 ATM IOA enabled  ---                      ---
11/1   ---          ---           ---    ---       ---           ---
12   online  LM-4                enabled  ---    7-3-0.rel   2d18h:26m:59s
12/0 present GE-8 IOA            enabled  ---                      ---
12/1 present GE-8 IOA            enabled  ---                      ---
13   online  LM-4                enabled  ---    7-3-0.rel   2d18h:17m:34s
13/0 present GE-4 IOA            enabled  ---                      ---
13/1   ---          ---           ---    ---       ---           ---
14   online  LM-4                enabled  ---    7-3-0.rel   3d01h:27m:06s
14/0   ---          ---           ---    ---       ---           ---
14/1 present OC12/STM4-2 POS IOA enabled  ---                      ---
```

```
15   online  LM-4                 enabled  ---    7-3-0.rel   3d01h:26m:28s
15/0   ---           ---            ---    ---       ---           ---
15/1 present OC12/STM4-2 ATM IOA enabled  ---                     ---
16   online  LM-4                 enabled  ---    7-3-0.rel   3d01h:25m:17s
16/0 present OC3/STM1-8 ATM IOA  enabled  ---                     ---
16/1 present OC3/STM1-8 ATM IOA  enabled  ---                     ---
```

- Example 4—Displays the version of an E120 router

```
host1#show version
Juniper Edge Routing Switch E120
Copyright (c) 1999-2007 Juniper Networks, Inc.  All rights reserved.
System Release: 8-2-0b0-9.rel
        Version: 8.2.0 beta-0.9 [BuildId 7030]   (April 2, 2007  13:04)
System running for: 1 day, 8 hours, 38 minutes, 0 seconds
        (since MON APR 09 2007 05:57:30 UTC)

                                        running
slot  state   type    admin  spare    release     slot uptime
---- ------- ------- ------- ----- ------------- -------------
0      ---     ---     ---    ---       ---           ---
1    online  LM-10   enabled  ---  8-2-0b0-9.rel 1d08h:32m:29s
2    online  LM-10   enabled  ---  8-2-0b0-9.rel 1d08h:32m:24s
3      ---     ---     ---    ---       ---           ---
4      ---     ---     ---    ---       ---           ---
5      ---     ---     ---    ---       ---           ---
6    online  SRP-120 enabled  ---  8-2-0b0-9.rel 1d08h:34m:46s
6    online  SFM-120 enabled  ---       ---      1d08h:34m:45s
7    standby SRP-120 enabled  ---  8-2-0b0-9.rel      ---
7    online  SFM-120 enabled  ---       ---      1d08h:34m:35s
8    online  SFM-120 enabled  ---       ---      1d07h:31m:04s
9    online  SFM-120 enabled  ---       ---      1d08h:34m:26s
10   online  SFM-120 enabled  ---       ---      1d08h:34m:30s
```

- Example 5—Displays the version of an E120 router using the **all** keyword

```
host1#show version all
Juniper Edge Routing Switch E120
Copyright (c) 1999-2007 Juniper Networks, Inc.  All rights reserved.
System Release: 8-2-0b0-9.rel
        Version: 8.2.0 beta-0.9 [BuildId 7030]   (April 2, 2007  13:04)
System running for: 1 day, 8 hours, 38 minutes, 6 seconds
        (since MON APR 09 2007 05:57:30 UTC)

                                          running
slot  state    type    admin  spare    release     slot uptime
---- ------- -------- ------- ----- ------------- -------------
0      ---     ---      ---    ---       ---           ---
0/0    ---     ---      ---    ---       ---           ---
0/1    ---     ---      ---    ---       ---           ---
1    online  LM-10    enabled  ---  8-2-0b0-9.rel 1d08h:32m:35s
1/0    ---     ---      ---    ---       ---           ---
1/1  present GE-8 IOA enabled  ---                     ---
2    online  LM-10    enabled  ---  8-2-0b0-9.rel 1d08h:32m:29s
2/0    ---     ---      ---    ---       ---           ---
2/1  present GE-8 IOA enabled  ---                     ---
3      ---     ---      ---    ---       ---           ---
3/0    ---     ---      ---    ---       ---           ---
3/1    ---     ---      ---    ---       ---           ---
4      ---     ---      ---    ---       ---           ---
4/0    ---     ---      ---    ---       ---           ---
4/1    ---     ---      ---    ---       ---           ---
5      ---     ---      ---    ---       ---           ---
```

```
5/0    ---     ---      ---    ---       ---           ---
5/1    ---     ---      ---    ---       ---           ---
6    online  SRP-120  enabled  ---  8-2-0b0-9.rel 1d08h:34m:51s
6    online  SFM-120  enabled  ---       ---      1d08h:34m:51s
6/0  present SRP IOA  enabled  ---                      ---
7    standby SRP-120  enabled  ---  8-2-0b0-9.rel      ---
7    online  SFM-120  enabled  ---       ---      1d08h:34m:41s
8    online  SFM-120  enabled  ---       ---      1d07h:31m:09s
9    online  SFM-120  enabled  ---       ---      1d08h:34m:32s
10   online  SFM-120  enabled  ---       ---      1d08h:34m:36s
```

Chapter 6

Managing Modules

This chapter describes how to manage line modules, switch route processor (SRP) modules, switch fabric modules (SFMs), I/O modules, and I/O adapters (IOAs) in E-series routers.

This chapter contains the following sections:

- Overview on page 306
- Platform Considerations on page 306
- Disabling and Reenabling Line Modules, SRP Modules, and SFMs on page 310
- Disabling and Reenabling IOAs on page 311
- Removing an SRP Module on page 313
- Replacing Line Modules on ERX Routers, the E120 Router, and the E320 Router on page 314
- Replacing IOAs on the E120 Router and the E320 Router on page 317
- Software Compatibility on page 321
- Configuring Performance Rate of Line Modules on ERX-7xx Models and the ERX-1410 Router on page 322
- Line Module Redundancy on page 327
- SRP Module Redundancy on page 330
- Monitoring Line Module and SRP Module Redundancy on page 338
- Managing Flash Cards on SRP Modules on page 341
- Updating the Router with JUNOSe Hotfix Files on page 355
- Managing the Ethernet Port on the SRP Module on page 366
- Enabling Warm Restart Diagnostics on Modules on page 368
- Monitoring Modules on page 370

Overview

When managing modules, you need to consider both software and hardware procedures. For example, before you remove an SRP module, you must enter the **halt** command to prevent damage to nonvolatile storage (NVS).

This chapter describes the software issues associated with managing modules. Each section in the chapter covers a different topic; where appropriate, a section contains an overview of the topic, configuration tasks, and information about monitoring the associated settings.

Platform Considerations

Procedures for managing modules vary depending on the type of E-series router that you have. The following sections describe the types of modules that you can manage for each type of E-series router and the general software procedures associated with them.

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

You can manage line modules, I/O modules, and SRP modules on ERX-7xx models, ERX-14xx models, and the ERX-310 router. For more information about these modules, see the *ERX Module Guide*.

For information about upgrading software on SRP modules, see *Chapter 3, Installing JUNOSe Software*. For information about related procedures and installing modules, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

Line Modules and I/O Modules

Most line modules available with these E-series models pair with a corresponding I/O module; however, some line modules do not require a corresponding I/O module. For example, the Service Module (SM) does not have a corresponding I/O module.

By configuring the performance line rate for a line module in the ERX-705, ERX-710, and ERX-1410 routers, you can enable the line modules either to operate at full line rate performance or to allow line modules to operate at a rate dependent on the resources available. For more information, see *Configuring Performance Rate of Line Modules on ERX-7xx Models and the ERX-1410 Router* on page 322.

The ERX-1440 router has two turbo slots (numbered 2 and 4). You can install certain line modules in the turbo slots to achieve greater line rate performance than when the modules are installed in other slots. For more information, see *JUNOSe Physical Layer Configuration Guide, Chapter 3, Configuring Unchannelized OCx/STMx Interfaces* and *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

Redundancy is supported for some line modules on these models. For more information, see *Line Module Redundancy* on page 327.

For more information about interface types and specifiers for ERX-7xx models, ERX-14xx models, and the ERX-310 router, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

SRP Modules

If you want to configure the performance line rate for a line module on supported routers, you must consider the bandwidth requirements of the SRP module that is installed on the router. For more information, see *Configuring Performance Rate of Line Modules on ERX-7xx Models and the ERX-1410 Router* on page 322.

Redundancy is supported for SRP modules on certain E-series routers; for more information, see *SRP Module Redundancy* on page 330.

SRP modules have a corresponding SRP I/O module that contains a Fast Ethernet management port. You can configure this port to access the router from a Telnet session or SNMP. For more information, see *Managing the Ethernet Port on the SRP Module* on page 366.

For information about using high availability mode for stateful SRP switchover, see *Chapter 7, Managing High Availability*.

E120 Router and E320 Router

You can manage line modules, SRP modules, SFMs, and IOAs on the E120 router and E320 router. For more information about these modules, see the *E120 and E320 Module Guide*.

For information about related procedures and installing modules, see *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*. For information about upgrading software on SRP modules, see the *E120 and E320 Hardware Guide*.

Line Modules and IOAs

Line modules on the E120 and E320 routers act as frame-forwarding engines for the physical interfaces, which are the IOAs.

You cannot configure the performance line rate of line modules for E120 and E320 routers. Redundancy is supported for line modules on this router. For more information, see *Line Module Redundancy* on page 327.

On the E120 router, line modules can be installed in slots 0–5. On the E320 router, line modules can be installed in slots 0–5 and 11–16. Both the E120 and E320 routers have two turbo slots, numbered 2 and 4. When a 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).

The 100 Gbps switch fabric that is available with the SRP 100 on 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. With a 100 Gbps fabric configuration, you must install the ES2 10G Uplink LM in the turbo slots. For more information, see *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

The 120 Gbps switch fabric on the E120 router allocates 10 Gbps of overall bandwidth to each line module slot. Similarly, the 320 Gbps switch fabric on the E320 router allocates 10 Gbps of overall bandwidth to each line module slot. For both configurations, you can install any line module in any of the slots.

A line module on the E120 and E320 routers can accommodate one full-height IOA or up to two half-height IOAs per slot. 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).

You can configure the slot by using the command-line interface (CLI), as well as the individual IOAs. For example, if you want to disable the line module installed in slot 3, issue the **slot disable 3** command. If you want to disable the IOA in the upper bay or left bay of slot 3, issue the **adapter disable 3/0** command. Table 37 lists the IOA bay values that you use to manage half-height and full-height IOAs.

For some IOAs, issuing the **adapter disable 3/0** command reboots the line module. Modules that support hot-swapping enable you to remove and add an IOA in a slot without rebooting the line module. If the slot is populated with another active IOA, it continues to operate.

Depending on the IOA type, you can manage IOAs from certain slots or bays. Table 37 lists the IOA management information, including valid IOA combinations and hot-swapping support.

Table 37: IOA Management Information

IOA	Right Bay (E120) Upper Bay (E320) (Adapter 0)	Left Bay (E120) Lower Bay (E320) (Adapter 1)	Both Bays Concurrently	Combined with Other IOAs in Same Slot	Hot-Swapping Support
ES2-S1 GE-4	Yes	Yes	No	No	Yes
ES2-S1 GE-8	Yes	Yes	Yes	Yes (GE-8 when paired with ES2 4G LM or ES2 10G LM; GE-8, OC3/STM1, and OC12/STM4 IOAs when paired with ES2 4G LM)	Yes
ES2-S3 GE-20	Yes (Full-height IOA)	Not applicable	Not applicable	Not applicable	No
ES2-S1 10GE	Yes (Full-height IOA)	Not applicable	Not applicable	Not applicable	No
ES2-S2 10GE PR	Yes (Full-height IOA)	Not applicable	Not applicable	Not applicable	No
ES2-S1 OC3-8 STM1 ATM	Yes	Yes	Yes	Yes (GE-8, OC3/STM1, and OC12/STM4 IOAs only)	Yes

Table 37: IOA Management Information

IOA	Right Bay (E120) Upper Bay (E320) (Adapter 0)	Left Bay (E120) Lower Bay (E320) (Adapter 1)	Both Bays Concurrently	Combined with Other IOAs in Same Slot	Hot-Swapping Support
ES2-S1 OC12-2 STM4 ATM	Yes	Yes	Yes	Yes (GE-8, OC3/STM1, and OC12/STM4 IOAs only)	Yes
ES2-S1 OC12-2 STM4 POS	Yes	Yes	Yes	Yes (GE-8, OC3/STM1, and OC12/STM4 IOAs only)	Yes
ES2-S1 OC48 STM16 POS	Yes	Yes	No	No	Yes
ES2-S1 Service	Yes (Full-height IOA)	Not applicable	Not applicable	Not applicable	No
ES2-S1 Redund	Yes (Full-height IOA; slots 0 and 11 only)	Not applicable	Not applicable	Not applicable	No

For more information about interface types and specifiers for the E120 and E320 routers, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

SRP Modules and SFMs

The router accommodates up to two SRP modules and three SFMs that act as an integrated system controller (SC) and switch fabric system. The SC is located on the SRP modules; the router's switch fabric is distributed between the SRP modules and SFMs. The switch fabric is divided into fabric slices; each SRP module and SFM has a resident fabric slice. At least four of the five possible fabric slices must be installed for the E120 and the E320 routers to operate.

You can configure the E120 router with a 320 Gbps fabric by installing SRP 120 modules and SFM 120 modules, or SRP 320 modules and SFM 320 modules.

You can configure the E320 router with a 100 Gbps fabric by installing SRP 100 modules and SFM 100 modules. To achieve increased switch fabric capacity and speed, you can configure the E320 router with a 320 Gbps fabric by installing SRP 320 modules and SFM 320 modules.

You can configure the SC and the fabric slices on the SRP modules separately. For example, if you disable the fabric slice on the standby SRP module by using the **slot disable 7 fabric** command, the SC on that SRP module is still enabled.

Redundancy is supported for SRP modules on the E120 and E320 routers. For more information, see *SRP Module Redundancy* on page 330.

SRP modules on the E120 and E320 routers have two slots for flash cards; other E-series routers have only a single slot. Cards installed in the second slot can be used only for core dump (.dmp) files. For more information, see *Managing Flash Cards on SRP Modules* on page 341.

SRP modules on the E120 and E320 routers have a corresponding SRP IOA that contains a Fast Ethernet management port. You can configure this port to access the router from the CLI or SNMP. For more information, see *Managing the Ethernet Port on the SRP Module* on page 366.

For information about using high availability mode for stateful SRP switchover, see *Chapter 7, Managing High Availability*.

Disabling and Reenabling Line Modules, SRP Modules, and SFMs

Disabling a line module, an SRP module, or an SFM has the same effect as removing that module from a slot. A disabled module cannot operate, although its configuration remains in NVS. For the module to operate, you must reenable it.

slot disable

- Use to disable the module in the specified slot.
- You can use this command to disable a module so that you can run diagnostic tests on the module.
- You cannot use this command on a standby SRP module.
- If you specify a slot on the E120 router or the E320 router that contains an SRP module, you disable the SC subsystem on that slot by default. You do not, however, disable the fabric slice that resides on the slot.
  - Use the **srp** keyword to disable only the portion of the SC subsystem that resides on a specified SRP module.
  - Use the **fabric** keyword to disable only the fabric slice that resides on the specified SRP module.
- If you specify a slot that contains a line module, you disable only the line module; you do not disable the line module and the I/O modules and IOAs associated with it. To disable a specific IOA on the E120 router or the E320 router, issue the **adapter disable** command.
- Example 1—Disables the module in slot 3

  host1(config)#**slot disable 3**

- Example 2—Disables the SRP module and the SC subsystem in slot 7 (applies only to the E120 and E320 routers)

  host1(config)#**slot disable 7**

- Example 3—Disables only the fabric slice on the SRP module in slot 7 (applies only to E120 and E320 routers)

  host1(config)#**slot disable 7 fabric**

- There is no **no** version.

slot enable

- Use to enable the module in the specified slot.
- Allows you to restart the module that was installed in the slot.
- You cannot use this command on a standby SRP module.
- If you specify a slot on the E120 router or the E320 router that contains an SRP module, you enable the SC subsystem on that slot by default. You do not, however, enable the fabric slice that resides on the slot.
  - Use the **srp** keyword to enable only the portion of the SC subsystem that resides on a specified SRP module.
  - Use the **fabric** keyword to enable only the fabric slice that resides on the specified SRP module.
- If you specify a slot that contains a line module, you enable only the line module; you do not enable the line module and the I/O modules and IOAs associated with it. To enable a specific IOA on the E120 router or the E320 router, use the **adapter enable** command.
- The default is enable.
- Example 1—Enables the module in slot 3

  host1(config)#**slot enable 3**

- Example 2—Enables the SRP module and the SC subsystem in slot 7 (applies only to E120 and E320 routers)

  host1(config)#**slot enable 7**

- Example 3—Enables only the fabric slice on the SRP module in slot 7 (applies only to E120 and E320 routers)

  host1(config)#**slot enable 7 fabric**

- There is no **no** version.

Disabling and Reenabling IOAs

Disabling an IOA on the E120 router or the E320 router has the same effect as removing that IOA from a slot. A disabled IOA cannot operate, although its configuration remains in NVS. To allow the IOA to operate, you must reenable it.

adapter disable

- Use to disable the IOA in the specified IOA bay.
- You can use this command to disable an IOA so that you can run diagnostic tests on it.
- On IOAs that support hot-swapping, issuing this command does not reboot the line module. On unsupported IOAs, issuing this command does reboot the line module associated with the IOA, but does not disable the line module. Issue the **slot disable** command to disable the line module. For a list of IOAs that support hot-swapping, see Table 37 on page 308.

- When you issue the **adapter disable** command in a redundancy configuration, the line module (primary or spare) currently associated with that IOA is rebooted. If the IOA is protected by a line module redundancy group, an automatic line module redundancy switchover or revert can be triggered by the line module reboot. To prevent undesired line module redundancy actions, issue the **redundancy lockout** command for the primary line module slot before issuing the **adapter disable** command. For more information, see *Line Module Redundancy* on page 327.
- 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).
- Example—Disables the IOA residing in the upper bay of slot 5 in an E320 router

  host1(config)#**adapter disable 5/0**

- There is no **no** version.

adapter enable

- Use to enable the IOA in the specified IOA bay.
- Enables you to restart the IOA that was installed in the slot.
- The default is enable.
- On IOAs that support hot-swapping, issuing this command does not reboot the line module. On unsupported IOAs, issuing this command reboots the line module associated with the IOA, but does not enable the line module. Issue the **slot enable** command to enable the line module. For a list of IOAs that support hot-swapping, see Table 37 on page 308.
- When you issue the **adapter enable** command in a redundancy configuration, the line module (primary or spare) currently associated with that IOA is rebooted. If the IOA is protected by a line module redundancy group, an automatic line module redundancy switchover or revert can be triggered by the line module reboot. To prevent undesired line module redundancy actions, issue the **redundancy lockout** command for the primary line module slot before issuing the **adapter enable** command. For more information, see *Line Module Redundancy* on page 327.
- 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).
- Example—Enables the IOA residing in the upper bay of slot 5 in an E320 router

  host1(config)#**adapter enable 5/0**

- There is no **no** version.

Removing an SRP Module

Before you remove an SRP module, you must issue the **halt** command, which stops operation on that module. If the router contains both primary and redundant SRP modules, you can specify which modules the command should affect.You can also configure the router to prompt you when the modules are in a state that might lead to loss of configuration data or NVS corruption.

CAUTION: If you do not use the **halt** command before removing or powering down an SRP module, the router's NVS may become corrupted.

For information about physically removing an SRP module, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

halt

- Use to stop the router's operation before you remove or power down an SRP module
- The following guidelines apply when you issue the **halt** command in Privileged Exec mode:
  - Specify neither the **primary-srp** nor the **standby-srp** keyword to stop operation on both SRP modules.
  - Specify the keyword **primary-srp** to stop operation on the primary SRP module only. This action causes the redundant SRP module to assume the primary role.
  - Specify the keyword **standby-srp** to stop operation on the redundant SRP module only.
  - If you do not specify the **force** keyword, the procedure fails if:
    - The SRP modules are in certain states, such as during a synchronization. In these cases, the router will display a message that indicates that the procedure cannot currently be performed and the reason why. However, if the SRP modules are in other states that could lead to a loss of configuration data or NVS corruption, the router displays a message that explains the state of the SRP modules and asks you to confirm (enter yes or no) whether you want to proceed.
    - The SRP modules are in any state that could lead to loss of configuration data or NVS corruption, and the router will display a message that explains why the command failed.
- In Boot mode, you cannot issue any keywords with this command.
- When the high availability state is active or pending, this command ensures that the router configuration, up to when you issued the **halt** command, is mirrored to the standby SRP.
- When you issue this command, the router prompts you for a confirmation before the procedure starts.
- Remove or power down the SRP module within 2 minutes of executing the **halt** command. Otherwise, the SRP module will automatically reboot.

- Examples

  host1#**halt**
  host1#**halt primary-srp**
  host1#**halt standby-srp force**

- There is no **no** version.

Replacing Line Modules on ERX Routers, the E120 Router, and the E320 Router

You can install line modules in slots previously occupied by different types of line modules. For example, on the ERX-1440 router, you can replace a GE-2 line module and a GE-2 SFP I/O module in a slot that previously contained an OCx/STMx/DS3-ATM line module and an OC3-4 I/O module.

When you configure a line module and an I/O module or IOAs, the router stores the configuration in NVS. In some cases, you must erase the interface configuration on the slot and reconfigure it after you have installed the new line module. However, some line modules enable you to replace the line module without reconfiguring the interfaces on the slot.

Tasks to replace a line module are:

- Replacing a Line Module by Erasing the Slot Configuration on page 314
- Replacing a Line Module Without Erasing the Slot Configuration on page 315

Replacing a Line Module by Erasing the Slot Configuration

Use this procedure when you are replacing the following line modules:

- All line modules on ERX routers
- All line modules on the E120 and E320 routers except for:
  - ES2 4G LM and ES2-S1 GE-8 IOA combination
  - ES2 10G LM and ES2-S1 GE-8 IOA combination
  - ES2 4G LM and ES2-S1 Redund IOA combination
  - ES2 10G LM and ES2-S1 Redund IOA combination

To replace a line module:

1. Copy your slot configuration so you can reconfigure the interfaces after replacing the line module.
2. (Optional) If line module redundancy is configured for the slot, disable redundancy for the slot.

   host1(config)#**redundancy lockout 7**

3. Disable the slot.

   host1(config)#**slot disable 7**

4. Remove the current line module and insert the new line module.

5. Issue the **slot accept** command for the affected slot.

   host1(config)#**slot accept 7**

   The **slot accept** command erases the configuration and enables you to reconfigure the new line module.

6. When the replacement line module has come online, reconfigure the interfaces.

7. If you disabled redundancy in Step 2, enable redundancy for the slot when the replacement line module has come online.

   host1(config)#**no redundancy lockout 7**

Replacing a Line Module Without Erasing the Slot Configuration

Use this procedure when you are replacing an ES2 4G LM with an ES2 10G LM, or vice-versa. Both line modules must already be paired with an ES2-S1 GE-8 IOA or the ES2-S1 Redund IOA.

You can replace a single line module or all of the line modules in a redundancy group using this procedure.

NOTE: In some cases, the ES2 4G LM and ES2 10G LM support different system maximums and protocols. Before you replace an ES2 4G LM with an ES2 10G LM, make sure that:

- The ES2 10G LM supports the features already configured on the slot for the ES2 4G LM.
- The ES2 10G LM can support the existing system maximums configured on the ES2 4G LM.

If you have a configuration on the ES2 4G LM that is not supported on the ES2 10G LM, you must erase the configuration before replacing the line module. For more information, see *Replacing a Line Module by Erasing the Slot Configuration* on page 314.

To replace a line module without erasing the slot configuration:

1. (Optional) If line module redundancy is configured for the slot, disable redundancy.

   host1(config)#**redundancy lockout 1**

2. Disable the slot.

   host1(config)#**slot disable 1**

3. After the line module has booted, issue the **show version** command to ensure that the status of the line module is `disabled (admin)`.

```
host1#show version
Juniper Edge Routing Switch E120

.......

                                                    running
slot  state   type    admin             spare     release     slot uptime
---- ------- ------- -------           ----- ------------- -------------
0      ---     ---     ---    ---        ---       ---
1    online  LM-10   disabled (admin)    ---  9-1-0b0-9.rel 1d08h:32m:29s
2    online  LM-10   enabled             ---  9-1-0b0-9.rel 1d08h:32m:24s
3      ---     ---     ---               ---       ---           ---

.......
```

4. Remove the current line module and insert the new line module without removing the IOA.

   For example, remove the ES2 4G LM and insert the new ES2 10G LM. Do not remove the ES2-S1 GE-8 IOA or the ES2-S1 Redund IOA.

5. After the new line module has booted, issue the **show version** command to ensure that the status of the line module is `disabled (mismatch)`.

```
host1#show version
Juniper Edge Routing Switch E120

.......

                                                    running
slot  state   type    admin             spare     release     slot uptime
---- ------- ------- -------           ----- ------------- -------------
0      ---     ---     ---    ---        ---       ---
1    online  LM-4    disabled (mismatch) ---  9-1-0b0-9.rel 1d08h:32m:29s
2    online  LM-10   enabled             ---  9-1-0b0-9.rel 1d08h:32m:24s
3      ---     ---     ---               ---       ---           ---

.......
```

6. Issue the **slot replace** command on the slot.

```
host1(config)#slot replace 1
```

TIP: If the line module is in a redundancy group and you did not disable redundancy in Step 1, the system switches to the spare line module. The system reloads both the replaced line module and the spare line module when you issue the **slot replace** command.

---

7. If you disabled redundancy for the slot in Step 1, enable redundancy when the replacement line module has come online.

```
host1(config)#no redundancy lockout 1
```

8. (Optional) If the following settings were configured before replacing the module, reconfigure the settings:

   a. Configure the Ethernet physical interface configuration using an SNMP set request for entPhysicalAssetID and entPhysicalAlias.

   b. Specify the threshold values for specific interface types for the slot.

      host1(config)#**resource if-type ip slot 1 threshold**

Related Topics

- **redundancy lockout** command
- **resource if-type** command
- **slot accept** command
- **slot replace** command
- **snmp-server** command

Replacing IOAs on the E120 Router and the E320 Router

When you configure an IOA in an IOA bay on the E120 and E320 routers, the router stores the configuration in NVS.

When you replace an IOA that supports hot-swapping with the same type of IOA, the line module goes online immediately. When you replace an IOA that *does not* support hot-swapping with the same type of IOA, the line module reboots.

Before you install an IOA that was previously occupied by another IOA in the E120 router or the E320 router—for example, an ES2-S1 GE-4 IOA in an IOA bay that previously contained an ES2-S1 OC3-8 STM1 ATM IOA—consider whether the IOA that you are replacing supports hot-swapping. For example:

- When you replace an IOA that does not support hot-swapping, the line module reboots. Before installing the different type of IOA, issue the **adapter erase** or **slot erase** command for the slot that contains the IOA bay.
- When you replace an IOA that supports hot-swapping, the line module becomes inactive with a “mismatch” state. After installing the different type of IOA, issue the **adapter accept** command or the **slot erase** command for the slot that contains the IOA bay.

Replacing SRP Modules and SFMs

If you remove a standby SRP module or an SFM, you must issue the **slot erase** command to delete the configuration. If you fail to issue the **slot erase** command, then the E-series router cannot guarantee that the SRP modules were synchronized. In this situation, the E-series router does not properly execute a simple **reload** command.

To reload the router you must do either of the following:

- Issue the **reload force** command.
- Issue the **slot erase** command followed by the **reload** command.

If you perform one of the following actions, you must reset the configuration of the router to factory default:

- Replace a 5-Gbps SRP module with a 10-Gbps SRP module or vice versa.
- Transfer an SRP module from an ERX-7xx router to an ERX-1410 router or vice versa.

You cannot use the **slot accept** command to force the router to accept the new SRP module.

When you have installed the SRP module in the new location, reset the configuration of the router to factory defaults as follows:

1. Reload the operating router, then press mb key sequence (case-insensitive) during the countdown.

   host1#**reload**

2. Reboot the router with the factory defaults.

   :boot##**boot config factory-defaults**

3. Reload the operating router.

   :boot##**reload**

For more information about the **reload** and **boot config** commands, see *Chapter 11, Booting the System*.

adapter accept

- Use to delete the configuration of the IOA in the specified IOA bay after you install a different type of IOA.
- This command enables you to create a fresh configuration for the module installed in the IOA bay.
- You can also use this command to accept an empty IOA bay that was previously occupied.
- Issuing this command reboots the line module associated with the IOA, but it does not erase the line module's configuration. To erase the configuration of the line module and its associated IOAs, issue the **slot accept** command.
- Issuing this command erases the interfaces associated with the specified IOA. To erase the interfaces for both IOAs installed in a slot, issue the **slot accept** command.
- Depending on the previous configuration of the slot, the system might take a few moments to execute this command.

- Example—Accepting the IOA in the upper bay of slot 5 in an E320 router

  host1(config)#**adapter accept 5/0**

- There is no **no** version.

adapter erase

- Use to delete the configuration of the specified IOA in the specified IOA bay before you install a different type of IOA.
- This command enables you to create a fresh configuration for the IOA to be installed in the IOA bay.
- Issuing this command reboots the line module associated with the IOA, but it does not erase the line module's configuration. To erase the configuration of the line module and its associated IOAs, issue the **slot erase** command.
- Issuing this command erases the interfaces associated with the specified IOA. To erase the interfaces for both IOAs installed in a slot, issue the **slot erase** command.
- Example—Erasing the IOA in the upper bay of slot 5 in an E320 router

  host1(config)#**adapter erase 5/0**

- There is no **no** version.

slot accept

- Use to delete the configuration of the module in the selected slot after you install a different type of module.
- This command enables you to create a fresh configuration for the module installed in the slot.
- You can also use this command to accept an empty slot that was previously occupied.
- You cannot use this command on a primary SRP module; however, you can use it on a standby SRP module.
- You can use this command only when the state of the module in the slot is not present or disabled (mismatch).
- If you specify a slot on an E120 router or an E320 router that contains an SRP module, you accept the configuration of the SC subsystem on that slot by default. You do not, however, accept the configuration of the fabric slice that resides on the slot.
  - Use the **srp** keyword to accept only the configuration of the portion of the SC subsystem that resides on a specified SRP module.
  - Use the **fabric** keyword to accept only the configuration of the fabric slice that resides on the specified SRP module.
- If you specify a slot that contains a line module, you erase the configuration of the line module and the I/O modules or IOAs associated with it. To erase the configuration of a specific IOA on the E120 router or the E320 router, use the **adapter accept** command.
- Depending on the slot's previous configuration, the router might take a few moments to execute this command.

- The following is a sample log message resulting from putting an OC3 line module in a slot that was previously configured for a line module:

```
ERROR 02/07/2003 15:16:20 system (slot 3): boardId mismatch: read 0x6 (OC3
dual port without classifier), configured 0x2e (OC12 ATM)
ERX-00-17-04(config)# slot accept  3
Please wait....
ERX-00-17-04(config)#ERROR 02/07/2003 15:16:31 system (slot 3): unrecognized
board type (0x6)
```

  To resolve the problem, issue the **slot accept** command for slot 3.

- Example 1—Accepts the configuration of the module in slot 3

  host1(config)#**slot accept 3**

- Example 2—Accepts the configuration of the specified SRP module and the SC subsystem in slot 7 (applies only to E120 and E320 routers)

  host1(config)#**slot accept 7**

- Example 3—Accepts the configuration of the SC on the SRP module in slot 7 (applies only to E120 and E320 routers)

  host1(config)#**slot accept 7 srp**

- There is no **no** version.

slot erase

- Use to delete the configuration of the module in the selected slot before you install a different type of module.
- This command enables you to create a fresh configuration for the module installed in the slot.
- You cannot use this command on a primary SRP module; however, you can use it on a standby SRP module.
- If you specify a slot on the E120 router or the E320 router that contains an SRP module, you erase the configuration of the SC subsystem on that slot by default. You do not, however, erase the configuration of the fabric slice that resides on the slot.
  - Use the **srp** keyword to erase only the configuration of the portion of the SC subsystem that resides on a specified SRP module.
  - Use the **fabric** keyword to erase only the configuration of the fabric slice that resides on the specified SRP module.
- If you specify a slot that contains a line module, you erase the configuration of the line module and the I/O modules or IOAs associated with it. To erase the configuration of a specific IOA on the E120 router or the E320 router, use the **adapter erase** command.
- Example 1—Erases the configuration of the module in slot 3

  host1(config)#**slot erase 3**

- Example 2—Erases the configuration of the specified SRP module and the SC subsystem in slot 7 (applies only to E120 and E320 routers)

  host1(config)#**slot erase 7**

- Example 3—Erases the configuration of the SC on the SRP module in slot 7 (applies only to E120 and E320 routers)

  host1(config)#**slot erase 7 srp**

- There is no **no** version.

Software Compatibility

An E-series software release supports a specific set of line modules and associated I/O modules or IOAs. Before you install a new line module, I/O module, or IOA, you should install a software release that supports the new module.

Line Modules

If the router uses a software version that does not support a line module that you install, you see the message unrecognized board type, and the router disables the module. When you issue a **show version** command, the state of the line module is disabled (admin).

If you subsequently boot the router with software that supports the line module, the line module becomes available and its state is enabled.

I/O Modules and IOAs

If the router uses a software version that does not support an I/O module or IOA that you install, the I/O module or IOA will be unavailable, and you will not be able to upgrade the software on the router. To upgrade the software:

1. Remove the I/O module or IOA.
2. Reboot the line module that corresponds to this I/O module or IOA. See *Chapter 11, Booting the System*.
3. When the line module has rebooted, install the I/O module or IOA.
4. Upgrade the software on the router. See *Chapter 3, Installing JUNOSe Software*.

Configuring Performance Rate of Line Modules on ERX-7xx Models and the ERX-1410 Router

NOTE: The information in this section does not apply to the ERX-1440 router, ERX-310 router, E120 router, or the E320 router. It also does not apply to the OC48 line module, which is supported only by the ERX-1440 router.

Line modules in an ERX-1440 router or an ERX-310 router always operate at line rate performance. However, you can configure ERX-7xx models and the ERX-1410 router to enable the line modules either to operate at full line rate performance or to allow line modules to operate at a rate dependent on the resources available.

Operating at full line rate performance restricts the combination of line modules in the router. Operating at a rate dependent on the resources available allows a much more extensive combination of line modules in the router and is known as *bandwidth oversubscription*.

To configure performance:

1. Choose a combination of line modules appropriate for the performance. See *Choosing a Combination of Line Modules* on page 322.

2. Disable slots that contain unwanted line modules, or modify the combination of line modules in the router. See *Disabling and Reenabling Line Modules, SRP Modules, and SFMs* on page 310, and *ERX Hardware Guide, Chapter 4, Installing Modules*.

3. Specify the type of performance. See *Specifying the Type of Performance* on page 325.

Choosing a Combination of Line Modules

For line rate performance, the total bandwidth required by the line modules in the slot group must not exceed the bandwidth available from the SRP module. In this case, the combination of line modules that can reside in a slot group depends on the following:

- The number of slots per group
- The bandwidth available from the SRP module
- The bandwidth required by each line module
- In the case of the SRP-5G+ and SRP-10G modules, the switches (upper and lower) that the line module can use.

Slot Groups

The number of slots in a group depends on the E-series model. For information about slot groups, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

SRP Modules Bandwidth

Different SRP modules offer different bandwidths:

- The SRP-10G module provides 2.5 Gbps bandwidth per slot group.
- The SRP-5G+ module (ERX-705 router only) provides:
  - 2.5 Gbps bandwidth per slot group
  - 5 Gbps bandwidth per router

Line Modules Bandwidth and Switch Usage

The SRP-5G+ and SRP-10G modules comprise two switches; each switch provides 50 percent of the bandwidth.

The line modules in a slot group cannot operate at line rate if:

- The sum of their bandwidths exceeds the bandwidth that the SRP module can supply per slot group.
- The sum of the bandwidths they require from one SRP switch exceeds the bandwidth that the SRP switch can supply per slot group.

Table 38 shows the bandwidth that each line module requires for line rate performance and the switches that the line module can use on the SRP-5G+ and SRP-10G modules.

Table 38: Bandwidth Statistics for Line Modules

Line Module	Total Bandwidth Required (Gbps)	Switches Used on SRP-5G+ and SRP-10G Modules
cOCx/STMx	2.46	Both switches
COCX-F3	2.46	Both switches
CT3/T3-F0	2.46	Both switches
GE/FE	2.46	Both switches
IPSec Service	2.46	Both switches
OC3/STM1 GE/FE	2.46	Both switches
OCx/STMx ATM	1.22	Both switches
OCx/STMx POS	2.46	Both switches

Allowed Combinations for Line Rate Performance

The SRP-5G+ and SRP-10G modules support all the line modules listed in Table 38.

Only certain combinations of line modules allow line rate performance (see Table 39 through Table 41). However, if performance lower than line rate is acceptable, you can use any combination of line modules in a slot group.

For example, the SRP-10G module offers a total bandwidth of 2.5 Gbps for each slot group. The GE line module requires 2.46 Mbps bandwidth for operation at line rate, and can use both switches in the SRP-10G module. If you require line rate from a GE line module, install only one GE line module in the slot group. However, if lower performance is acceptable, you can install two or three GE line modules in a slot group and enable bandwidth oversubscription.

When bandwidth oversubscription is enabled, all line modules optimize use of the resources available. For example, if two GE line modules are installed in a slot group, each line module is allocated 50 percent of the available bandwidth. However, if one line module is using less bandwidth than it is allocated, the other line module can use more bandwidth than it is allocated and can operate at a greater rate.

Table 39, Table 40, and Table 41 indicate combinations of line modules that allow line rate performance.

Table 39: Combinations of Line Modules for Line Rate Performance—SRP-10G Module in an ERX-7xx Model

Possible Combinations of Line Modules	Examples of Allowed Combinations	Examples of Forbidden Combinations
■ One supported line module and one empty slot in slot group 1 **NOTE:** The SRP-10G module supports all line modules listed in Table 38. ■ Two OCx/STMx ATM line modules in slot group 1 ■ One supported line module in slot groups 2, 3 and 4	■ One OCx/STMx POS line module in slot group 1, a GE/FE line module in slot group 2, and one OCx/STMx ATM line module in slot group 4 ■ Two OCx/STMx ATM line modules in slot group 1, one GE/FE line module in slot group 2, and one SM in slot group 3	■ A GE/FE line module and any other line module in slot group 1 ■ Two OCx/STMx POS line modules in slot group 1

Table 40: Combinations of Line Modules for Line Rate Performance—SRP-10G Module in an ERX-1410 Router

Possible Combinations of Line Modules	Examples of Allowed Combinations	Examples of Forbidden Combinations
■ One supported line module and two empty slots in any slot group **NOTE:** The SRP-10G module supports all line modules listed in Table 38. ■ Two OCx/STMx ATM line modules and one GE/FE module and one empty slot in any slot group (bandwidth oversubscription enabled) ■ One OC3/STM1 GE/FE module in any slot (bandwidth oversubscription disabled)	■ One COCX-F3 line module in slot group 1, a GE/FE line module in slot group 2, and a OCx/STMx POS line module in slot group 3	■ Three OCx/STMx ATM line modules in any slot group ■ Two GE/FE line modules in any slot group

Table 41: Combinations of Line Modules for Line Rate Performance—SRP-5G+ Module in an ERX-705 Router

Possible Combinations of Line Modules In Slot Groups	Examples of Allowed Combinations	Examples of Forbidden Combinations
NOTE: The total bandwidth of all line modules must not exceed 5 Gbps. To make optimal use of the available bandwidth, put line modules that require maximum bandwidth in slot 2, 3, or 4.		
■ One supported line module and one empty slot in slot group 1 **NOTE:** The SRP-5G+ module supports all line modules listed in Table 38. ■ Two OCx/STMx ATM line modules in slot group 1 ■ One cOCx/STMx, COCX-F3, CT3/T3 FO, GE/FE, IPSec Service, or OCx/STMx line module in slot groups 2, 3, and 4	■ Two OCx/STMx ATM line modules (total 2.44 Gbps) in slot group 1, and a GE/FE line module (2.46 Gbps) in slot group 4 ■ Two OCx/STMx ATM line modules (total 2.44 Gbps) in slot group 1, and a COCX-F3 line module in slot group 2	■ Two OCx/STMx ATM line modules (total 2.44 Gbps) in slot group 1, a GE/FE line module (2.46 Gbps) in slot group 3, and an OCx/STMx POS line module (2.46 Gbps) in slot 4 (violates chassis limitation) ■ Two OCx/STMx POS line modules (total 4.92 Gbps) in slot group 1 (violates slot group limitation)

Specifying the Type of Performance

After you have installed a suitable combination of line modules, you can specify a different type of performance. To specify the type of performance:

1. Issue the **show bandwidth oversubscription** command.
2. If the setting is not the one you want, enable or disable bandwidth oversubscription.
3. Reboot the router.

bandwidth oversubscription

- Use to enable bandwidth oversubscription for an ERX-7xx model or ERX-1410 router. Reboot the router after you have issued this command to change the bandwidth oversubscription status.
- By default, bandwidth oversubscription is enabled.
- Example

  host1(config)#**bandwidth oversubscription**

- Use the **no** version to disable bandwidth oversubscription. Reboot the router after you have issued this command to change the bandwidth oversubscription status.

Monitoring Bandwidth Oversubscription

Use the **show bandwidth oversubscription** and **show utilization** (see *Monitoring Modules* on page 370) commands to monitor the status of bandwidth oversubscription.

show bandwidth oversubscription

- Use to display the bandwidth oversubscription status for an ERX-7xx model or ERX-1410 router.
- Example 1: This example shows the display when bandwidth oversubscription is enabled.

```
host1#show bandwidth oversubscription
Bandwidth oversubscription is currently in effect.
```

- Example 2: This example shows the display that appears after you issue the **no bandwidth oversubscription** command to disable bandwidth oversubscription.

```
host1#no bandwidth oversubscription
host1#show bandwidth oversubscription
Bandwidth oversubscription is currently in effect.
Bandwidth oversubscription will not be in effect the next time the system
reboots.
```

- Example 3: This example shows the display when bandwidth oversubscription is disabled.

```
host1#show bandwidth oversubscription
Bandwidth oversubscription is currently not in effect.
```

- Example 4: This example shows the display that appears after you issue the **bandwidth oversubscription** command to enable bandwidth oversubscription.

```
host1#bandwidth oversubscription
host1#show bandwidth oversubscription
Bandwidth oversubscription is currently not in effect.
Bandwidth oversubscription will be in effect the next time the system
reboots.
```

Troubleshooting Bandwidth Oversubscription

If you enter a forbidden combination of line modules or exceed the slot group bandwidth when you have not configured bandwidth oversubscription, you will see an error message.

For example, suppose you originally configure the router for bandwidth oversubscription and then want to change to full line rate performance. You forget to remove line modules or disable slots, and enter the **no bandwidth oversubscription** command. The following message appears:

```
host1(config)#no bandwidth oversubscription
% failed : bandwidth over subscribed at slot 0-2
```

To resolve the problem, remove the unwanted line modules, or disable the slots that contain those line modules.

Line Module Redundancy

You can install an extra line module in a group of identical line modules to provide redundancy if one of the modules fails.

The process by which the router switches to the spare line module is called *switchover*. During switchover, the line, circuit, and IP interfaces on the I/O module or one or more IOAs appear to go down temporarily. The duration of the downtime depends on the number of interfaces and the size of the routing table, because the router must reload the interface configuration and the routing table from the SRP module.

If the line module software is not compatible with the running SRP module software release, a warning message appears on the console.

Module Requirements

The requirements for line module redundancy depend on the type of router that you have.

NOTE: The information in this section does not apply to the ERX-310 router, which does not support line module redundancy.

ERX-7xx Models and ERX-14xx Models

To use this feature on ERX-7xx models and ERX-14xx models, you must also install a redundancy midplane and a redundancy I/O module. For a detailed explanation of how the router provides redundancy for line modules and procedures for installing the modules, see the *ERX Hardware Guide*.

E120 Router and E320 Router

To configure line module redundancy on the E120 router or the E320 router, you must also install an ES2-S1 Redund IOA in either slot 0 or slot 11. The ES2-S1 Redund IOA is a full-height IOA. For a detailed explanation of how the router provides redundancy for line modules and procedures for installing the modules, see the *E120 and E320 Hardware Guide*.

On E120 and E320 routers, each side of the chassis is treated as a redundancy group. The lowest numbered slot for each side acts as the spare line module, providing backup functionality when an ES2-S1 Redund IOA is located directly behind it. When the line module does not contain an ES2-S1 Redund IOA, it is considered a primary line module.

The spare line module only backs up a line module of the same type. For example, an ES2 4G LM spare line module backs up any ES2 4G LM, but does not back up an ES2 10G Uplink LM. The router accepts the following redundancy groups:

- ES2 4G LM and ES2 4G LM
- ES2 10G Uplink LM and ES2 10G Uplink LM
- ES2 10G LM and ES2 10G LM

Also, you cannot configure redundancy for the ES2-S1 Service IOA.

IOA Behavior When the Router Reboots

On E120 and E320 routers, switchover is based on the combined states of the line module and the IOAs that are installed in the affected slot.

When the router reboots and the formerly configured primary line module is not present, or is present and fails diagnostics, it switches to a spare line module and takes inventory of the IOAs. If the IOA is present and new, the router reverts back to the primary line module so that the spare line module can service other active primary line modules.

When the router reboots and there is a slot that contains a line module and one active and one inactive IOA, the inactive IOA remains in that state.

Line Module Behavior When Disabling or Enabling IOAs

On E120 and E320 routers, a line module reboots when you issue the **adapter disable** or **adapter enable** commands for an associated IOA.

When you issue the **adapter disable** or **adapter enable** commands, the line module (primary or spare) currently associated with that IOA reboots. If the IOA is protected by a line module redundancy group, an automatic line module redundancy switchover or revert can be triggered by the line module reboot. To prevent undesired line module redundancy actions, issue the **redundancy lockout** command for the primary line module slot before issuing the **adapter disable** or **adapter enable** commands.

Automatic Switchover

Provided you have not issued the **redundancy lockout** command for the primary line module, the router switches over to the spare line module automatically if it detects any of the following failures on the primary line module:

- Power-on self-test (POST) failure
- Software-detected unrecoverable error
- Software watchdog timer expiration
- Primary line module failure to respond to keepalive polling from the SRP module
- Removal, disabling, or reloading of the primary line module
- Missing or disabled primary line modules when the router reboots
- Resetting the primary line module using the concealed push button

Limitations of Automatic Switchover

If automatic switchover is enabled on a slot (the default configuration) and a spare line module is available, issuing some CLI commands for the primary line module causes a switchover (see Table 42).

You can also disable automatic switchover on individual slots. For more information, see *Configuring Line Module Redundancy* on page 329.

Table 42: Commands That Can Cause Automatic Switchover

Command	Reason for Automatic Switchover
slot disable *primary-line-module-slot*	The command disables the primary line module but not the primary I/O module or IOAs.
reload slot *primary-line-module-slot*	The command is equivalent to pushing the reset button on the primary line module.

Reversion after Switchover

You can install only one spare line module in the group of slots covered by the redundancy midplane or redundancy group. If the router is using the spare line module, no redundancy is available. It is desirable to revert to the primary module as soon as possible. By default, the router does not automatically revert to the primary module after switchover; however, you can configure it to do so. (See *Configuring Line Module Redundancy*.) Before reversion can take place, the primary line module must complete the POST diagnostics.

Configuring Line Module Redundancy

You can modify the default redundancy operations on the router as follows:

- Disable automatic switchover on a slot.
- Enable automatic reversion after switchover.

redundancy lockout

- Use to prevent the router from switching automatically to a spare line module if the primary module in the specified slot fails.
- The **redundancy force-switchover** command overrides the **redundancy lockout** command.
- Example

  host1(config)#**redundancy lockout 5**

- Use the **no** version to restart redundancy protection for the slot.

redundancy revertive

- Use to enable the router to revert from all spare line modules to the associated primary line modules automatically.
- Reversion takes place when the primary line module is once again available unless you specify a time of day. In that case, reversion takes place only when the primary module is available and after the specified time.

- Example

  host1(config)#**redundancy revertive 23:00:00**

- Use the **no** version to disable automatic reversion.

Managing Line Module Redundancy

When the router is running and a redundancy group is installed, you can manage the redundancy situation as follows:

- Force switchover manually.
- Force reversion manually.

redundancy force-switchover

- Use to force the router to switch from the primary line module in the specified slot or the primary SRP module to the spare line module or SRP module.
- The command causes a single switchover. When you reboot, the router reverts to the configured setting for this slot.
- The **redundancy force-switchover** command overrides the **redundancy lockout** command.
- Example

  host1#**redundancy force-switchover 5**

- There is no **no** version.

redundancy revert

- Use to force the router to revert to the primary line module in the specified slot.
- The router acts on this command immediately unless you specify a time or a time and date that the action is to take place.
- The command causes a single reversion. When you reboot, the router uses the configured setting for this slot.
- Example

  host1#**redundancy revert 4 23:00:00 5 September 200X**

- There is no **no** version.

SRP Module Redundancy

This section covers general issues of SRP module redundancy. It does not cover NVS cards or the behavior on systems running high availability features such as hitless SRP switchover. For information about managing NVS in a router that contains two SRP modules, see *Managing Flash Cards on SRP Modules* on page 341. For information about managing high availability in a router, see *Chapter 7, Managing High Availability*.

The information in this section does not apply to the ERX-310 router, which does not support SRP module redundancy. For this reason, any references to synchronization that may appear in command output or system messages do not apply to the ERX-310 router.

SRP Module Behavior

The SRP module uses a 1:1 redundancy scheme. When two SRP modules are installed in the router, one acts as a primary and the second as a redundant module. On ERX-7xx models, ERX-14xx models, and the ERX-310 router, both SRP modules share a single SRP I/O module located in the rear of the chassis. On the E120 router and the E320 router, both SRP modules share an SRP IOA located in the rear of the chassis.

After you install two SRP modules, the modules negotiate for the primary role. A number of factors determine which module becomes the primary; however, preference is given to the module in the lower slot. The SRP modules record their latest roles and retain them the next time you switch on the router.

With the default software settings, if the primary SRP module fails, the redundant SRP module assumes control without rebooting itself. For information about preventing the redundant SRP module from assuming control, see *Managing SRP Module Redundancy* on page 335.

On E120 and E320 routers, the switch fabric is distributed between the SFMs and the SRP modules. If the primary SRP module fails a diagnostic test on its resident slice of switch fabric, then it abdicates control to the redundant SRP module if both of the following are true:

- The standby SRP module does not indicate any error.
- The standby SRP module passes diagnostics on its attached fabric slice.

When the redundant SRP module assumes control, the following sequence of events occurs:

1. The original primary SRP module reboots and assumes the redundant role.
2. The redundant SRP module restarts and assumes the primary role without reloading new code. (When upgrading software, you must reload the software on the redundant SRP module. See *Chapter 3, Installing JUNOSe Software*.)
3. All line modules reboot.

The following actions activate the redundant SRP module:

- Failure of the primary SRP module (hardware or software)
- Pushing the recessed reset button on the primary SRP module (see Figure 25 on page 332 and Figure 26 on page 332)
- Issuing the **srp switch** command
- Issuing the **redundancy force-switchover** command

Figure 25: SRP Module on ERX-7xx Models and ERX-14xx Models

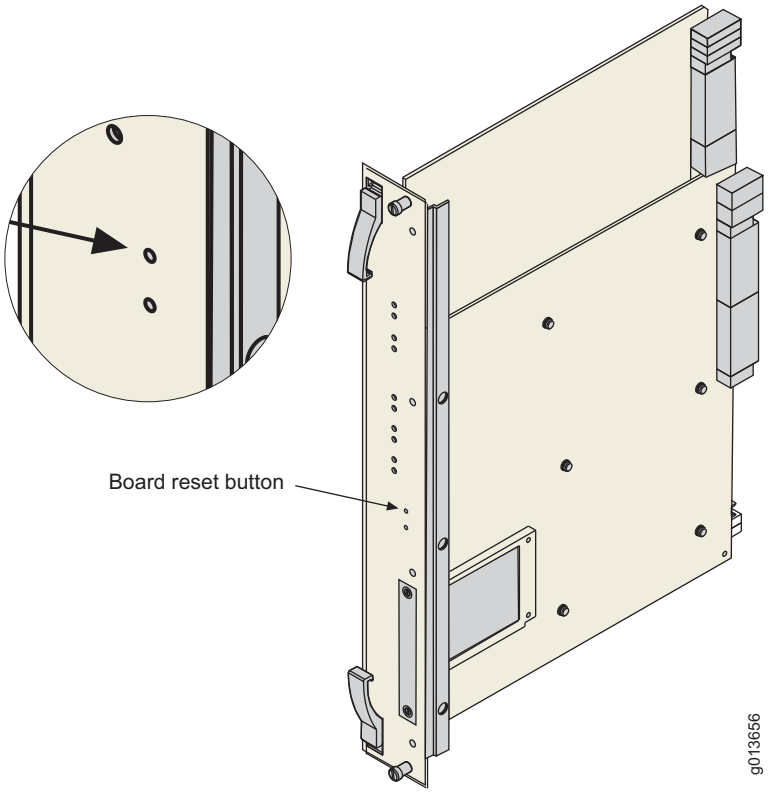
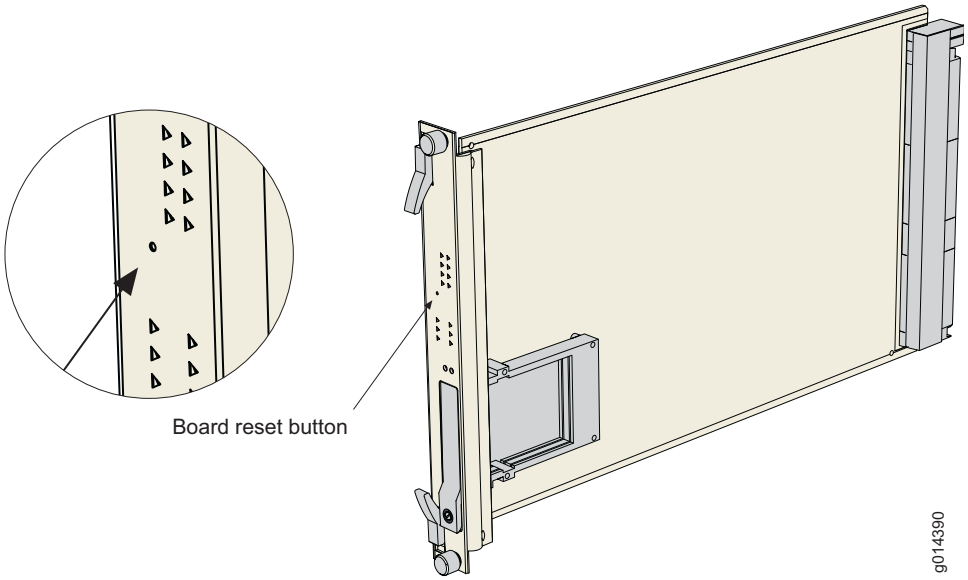


Figure 26: SRP Module on the E120 Router and the E320 Router



Specifying the Configuration for Redundant SRP Modules

On a router with redundant SRP modules, you can specify the configuration that both the primary and redundant modules load in the event of a reload or switchover. A switchover can result from an error on the primary SRP module or from an **srp switch** command. The following behavior takes place only in the event of a cold restart; it does not take place in the event of a warm restart.

When you arm a configuration (.cnf) file by issuing the **boot config** *cnfFilename* command, a subsequent SRP switchover causes the redundant SRP module to assume the role of primary SRP module with the configuration specified by the .cnf file. The new primary SRP module does not use the running configuration.

If you want the redundant SRP module to instead use the running configuration when it assumes the primary role, then you must first arm a configuration file with the **boot config** *cnfFilename* **once** command. To exhaust the **once** option, you must then cause the redundant SRP module to reload for some reason, such as by issuing a **reload** command or by arming a new JUNOSe release or a hotfix file.

When a switchover subsequently occurs, the redundant SRP module reloads with the running configuration and assumes the primary role. For more information about the **boot config** command, see *Chapter 11, Booting the System*.

Installing a Redundant SRP Module

You can install a redundant SRP module into a running router, provided that the redundant SRP module has a valid, armed software release on its NVS card. Access to a software release in NVS ensures that the redundant SRP module can boot; the release need not be the same as that on the primary SRP module. To install a redundant SRP module into a running router, follow these steps:

WARNING: Do not insert any metal object, such as a screwdriver, or place your hand into an open slot or the backplane when the router is on. Remove jewelry (including rings, necklaces, and watches) before working on equipment that is connected to power lines. These actions prevent electric shock and serious burns.

CAUTION: When handling modules, use an antistatic wrist strap connected to the router's ESD grounding jack, and hold modules by their edges. Do not touch the components, pins, leads, or solder connections. These actions help to protect modules from damage by electrostatic discharge.

1. Install the redundant SRP module into the open SRP slot (slot 6 or 7 for ERX-14xx models, the E120 router, and the E320 router; slot 0 or 1 for ERX-7xx models).

   For detailed information about installing the SRP module, see the *ERX Hardware Guide* or the *E120 and E320 Hardware Guide*.

2. Wait for the redundant SRP module to boot, initialize, and reach the standby state.

   When the module is in standby state, the REDUNDANT LED is on and the ONLINE LED is off. If you issue the **show version** command, the state field for the slot that contains the redundant SRP module is standby.

3. Synchronize the NVS file system of the redundant SRP module to that of the primary SRP module.

NOTE: The SRP module reboots after synchronization is complete.

reload slot

- Use to reboot a selected slot on the router.
- If you specify a slot on the E120 router or the E320 router that contains an SRP module, you reboot the SC subsystem on that slot by default. You do not, however, reboot the fabric slice that resides on the slot.
  - Use the **srp** keyword to reboot the portion of the SC subsystem that resides on a specified SRP module.
  - Use the **fabric** keyword to reboot the fabric slice that resides on the specified SRP module.
- Example 1—Reboots the module in slot 7

  host1#**reload slot 7**

- Example 2—Reboots the SC on the SRP module in slot 7 (applies only to E120 and E320 routers)

  host1#**reload slot 7 srp**

- There is no **no** version.

synchronize

- Use to force the file system of the redundant SRP module to synchronize with the NVS file system of the primary SRP module.
- If you synchronize the redundant SRP module with the primary SRP module and the redundant module is armed with a release different from the one it is currently running, the redundant SRP module is automatically rebooted to load the armed release.
- Optionally, you can use the **low-level-check** keyword to force the router to validate all files or only configuration files in NVS, and to synchronize all files that failed the checksum test during the **flash-disk-compare** command as well as any other files that are unsynchronized. See *Validating and Recovering Redundant SRP File Integrity* on page 347 for details.

- Examples

  host1#**synchronize**
  host1#**synchronize low-level-check all**
  host1#**synchronize low-level-check configuration**

- There is no **no** version.

Managing SRP Module Redundancy

You can prevent the redundant SRP module from taking over when:

- The primary SRP module experiences a software failure.
- You push the reset button on the primary SRP module.

NOTE: If you do not configure this option, when troubleshooting an SRP module, disconnect the other SRP module from the router. This action prevents the redundant SRP module from taking over if you push the reset button on the primary SRP module.

To configure this option:

1. Issue the **disable-switch-on-error** command.
2. Synchronize the NVS file system of the redundant SRP module to that of the primary SRP module.

Refer to the commands and guidelines in the previous section and below.

disable-switch-on-error

- Use to prevent the redundant SRP module from taking over if the primary SRP module experiences a software failure or if you push the reset button on the primary SRP module.
- Issue the **synchronize** command immediately before you issue this command.
- If you issue the **disable-switch-on-error** command, and later issue the **srp switch** command, the redundant SRP module waits about 30 seconds before it takes over from the primary SRP module.
- Example

  host1(config)#**disable-switch-on-error**

- Use the **no** version to revert to the default situation, in which the redundant SRP module takes over if the primary SRP module experiences a software failure.

synchronize

- Use to force the NVS file system of the redundant SRP module to synchronize with the NVS file system of the primary SRP module.
- If you synchronize the redundant SRP module with the primary SRP module and the redundant module is armed with a release different from the one it is currently running, the redundant SRP module is automatically rebooted to load the armed release.
- Optionally, you can use the **low-level-check** keyword to force the router to validate all files or only configuration files in NVS, and to synchronize all files that failed the checksum test during the **flash-disk-compare** command as well as any other files that are unsynchronized. See *Validating and Recovering Redundant SRP File Integrity* on page 347 for details.
- Examples

  host1#**synchronize**
  host1#**synchronize low-level-check all**
  host1#**synchronize low-level-check configuration**

- There is no **no** version.

Switching to the Redundant SRP Module

To switch immediately from the primary SRP module to the redundant SRP module, issue the **redundancy force-switchover** command or the **srp switch** command. You can configure the router to prompt you if the modules are in a state that could lead to loss of configuration data or NVS corruption.

redundancy force-switchover

- Use to force the router to switch from the primary line module in the specified slot or the primary SRP module to the spare line module or SRP module.
- The command causes a single switchover. When you reboot, the router reverts to the configured setting for this slot.
- With the **srp** option, the command is equivalent to the **srp switch** command.
- The **redundancy force-switchover** command overrides the **redundancy lockout** command.
- Example

  host1#**redundancy force-switchover 5**

- There is no **no** version.

srp switch

- Use to switch from the primary SRP module to the redundant SRP module.
- When the high availability state is active, this command delays until all transaction data, up to when you issue the command, has been mirrored to the standby SRP module. This preserves legacy behavior requiring that SRP modules be synchronized before the switchover.

- If you specify the **force** keyword, the procedure fails if the SRP modules are in certain states, such as during a synchronization. In these cases, the router displays a message that indicates that the procedure cannot currently be performed and the reason why. However, if the SRP modules are in other states that could lead to a loss of configuration data or an NVS corruption, the router displays a message that explains the state of the SRP modules, and asks you to confirm (enter yes or no) whether you want to proceed.
- If you do not specify the **force** keyword, the procedure fails if the SRP modules are in any state that could lead to a loss of configuration data or an NVS corruption, and the router displays a message explaining the command failure.
- When you issue this command, the router prompts you for a confirmation before the command takes effect.
- If you issue the **disable-switch-on-error** command and later issue the **srp switch** command, the redundant SRP module waits about 30 seconds before it takes over from the primary SRP module.
- If the router does not contain a redundant SRP module, this command has no effect.
- Example

  host1#**srp switch**
  host1#**srp switch force**

- There is no **no** version.

Upgrading Software on a Redundant SRP Module

For information about upgrading software on SRP modules on ERX-7xx models, ERX-14xx models, or the ERX-310 router, see *Chapter 3, Installing JUNOSe Software*.

Monitoring the Status LEDs

You can determine the redundancy state of line modules and SRP modules by examining their status LEDs. See Table 43 for a description of the LEDs functions. In addition, if you issue the **show version** command, the state field for the slot that contains the redundant SRP module should be standby.

Table 43: Function of the Online and Redundant LEDs

Online LED	Redundant LED	State of the Module
Off	Off	Module is booting or is an inactive primary line module.
On	Off	Module is active, but no redundant module is available.
Off	On	Module is in standby state.
On	On	Module is active, and a redundant module is available.

Monitoring Line Module and SRP Module Redundancy

You can use **show** commands to monitor the status of redundancy groups, line modules, and SRP modules.

NOTE: For more information about monitoring high availability, see *Chapter 7, Managing High Availability*.

show environment

- Use to display information about the hardware installed for redundancy.
- See *Chapter 5, Managing the System*, for details and examples.

show hardware

- Use to display detailed information about the line modules and SRP modules.
- See *Monitoring Modules* on page 370 for details and examples.

show redundancy

- Use to display the configuration for line module redundancy and SRP redundancy.
- Field descriptions
  - SRP
    - high-availability state—State of the high availability mode (disabled, active, or pending)
    - current redundancy mode—Redundancy mode currently being used by this router (high-availability or file-system-synchronization)
    - last activation type—Last type of activation that occurred on this router (that is, the method by which the SRP last booted [cold-start or warm-start])
  - Criteria Preventing High Availability from being Active—Criteria required for HA to be active.
  - slot—Slot in which the line module resides
  - hardware role—Function of the line module: primary or spare
  - lockout config—Status of redundancy on this line module
    - protected—Line module redundancy is enabled
    - locked out—Line module redundancy is disabled
  - backed up by slot—Slot that contains the line module that is a spare for this primary line module
  - sparing for slot—Slot that contains the primary line module for which this line module is a spare
  - revert at—Time at which you want the line module to revert
  - midplane type—Identifier for the type of midplane

- midplane rev—Hardware revision number of the redundancy midplane
- fabric slice redundancy—Status of the fabric slice on the SRP modules or SFMs on the E120 and E320 routers
  - slot—Slot in which the fabric slice resides
  - slice state—State of the fabric slice (online, not present)
  - type—Identifier for the type of hardware (SRP module or SFM)

- Example 1

  In the following example, the user issues a **show redundancy** command, and then a **redundancy force switchover** command. Finally, the user issues the **show redundancy line-card** command to display information specific to the line modules. The two displays show how the states of the primary and spare line modules change.

```
host1#show redundancy

SRP
---

high-availability state:  disabled
current redundancy mode:  file-system-synchronization
last activation type:     cold-start

Criteria Preventing High Availability from being Active
-------------------------------------------------------
            criterion                met
---------------------------------   ---
High Availability mode configured?   No
Mirroring Subsystem present?         No

Line Card
---------

automatic reverting is off

                              backed
                                up      sparing
       hardware    lockout      by       for      revert
slot     role      config      slot     slot       at
----   --------   ---------   ------   -------   ------
 0      spare        ---       ---       ---      ---
 2     primary    protected    ---       ---      ---
 12      ---         ---       ---       ---      ---

        midplane   midplane
slots     type       rev
-----   --------   --------
0 - 5      6          0

host1#redundancy force-switchover 2
host1#show redundancy line-card

automatic reverting is off
```

```
                                backed
                                  up      sparing
       hardware     lockout       by        for      revert
slot     role       config       slot      slot       at
----   --------   ----------   ------   -------   ------
 0      spare        ---        ---        2       ---
 2     primary    protected     0         ---      ---
 12      ---         ---        ---       ---      ---

        midplane   midplane
slots     type       rev
-----   --------   --------
0 - 5      6          0
```

- Example 2—Displays the redundancy status on an E320 router

```
host1#show redundancy

SRP
---

high-availability state:  active
current redundancy mode:  high-availability
last activation type:     cold-start

Line Card
---------

automatic reverting is off

                                backed
                                  up      sparing
       hardware     lockout       by        for      revert
slot     role       config       slot      slot       at
----   --------   ----------   ------   -------   ------
 0      spare        ---        ---       ---      ---
 2     primary    protected     ---       ---      ---
 4     primary    protected     ---       ---      ---


fabric slice redundancy: none
slot   state     type
----   ------   -------
6      online   SFM-100
7      online   SFM-100
8       ---       ---
9       ---       ---
10      ---       ---
```

show version

- Use to display information about each module in the router.

  See *Chapter 5, Managing the System*, for details and examples.

Managing Flash Cards on SRP Modules

Each SRP module contains a flash card that stores system files. On the E120 router and the E320 router, each SRP module can have an additional flash card; the second card is reserved for the storage of core dumps.

In this documentation, the flash card on the primary SRP module is referred to as the primary flash card; the flash card on the redundant SRP module is referred to as the redundant flash card.

If you have two SRP modules installed in a router, you can use flash cards of different capacities on the SRP modules. The effective capacity of the higher-capacity flash card equals that of the lower-capacity flash card.

Flash Features

The software contains a number of features that optimize the way the router restores its configuration if it is shut down improperly:

- The router tracks improper shutdowns.
- After an improper shutdown, the router runs an investigation of the file allocation table (FAT) the next time it reboots.
- The router creates backups of critical files.
- When you install a new flash card or restart the router after shutting it down incorrectly, a utility scans the flash card to detect corrupt sectors. If the utility finds files or directories that contain corrupt sectors, it removes the files and directories, because they can no longer be used. The utility also fixes problems with unused sectors. If the utility cannot correct a corrupt sector, it marks the sectors so that they cannot be reused. Errors in the boot block, FAT, or root directory are fatal and cannot be corrected by the scan utility.
- In a router that contains two SRP modules, if the scanning utility detects corrupt sectors in flash on the primary SRP module during rebooting, the primary SRP module reboots again. Both SRP modules now have standby status and reboot. The first SRP module to complete rebooting becomes the primary. Because the former redundant module started to reboot first, it likely becomes the primary. When the former primary module has rebooted and the scan utility has fixed corrupt sectors in its flash card, the SRP modules will synchronize. Any files or directories removed by the scan utility are restored during the synchronization.
- If you reboot the router before it has completely written configuration updates to the flash card, the router starts with the last saved configuration. If you reboot the router after it has written the configuration updates to the flash card, but before it has applied those updates to actual configuration data, the configuration update process resumes immediately following the reboot and is completed before any application accesses its configuration data.

Flash Features on the E120 Router and the E320 Router

The E120 router and the E320 router can have a second flash card installed with its SRP modules. Device names are reserved for the E120 and E320 router flash card slots: disk0, disk1, standby-disk0, and standby-disk1. For backward compatibility, you can use the name standby, which is equivalent to standby-disk0. You can use the second card (disk1 or standby-disk1) only for storage of core dump (.dmp) files. When the a card is installed and mounted as disk1 or standby-disk1, all .dmp files are automatically stored on this card. You must use the card mounted as disk0 or standby-disk0 for all other file types. Core dump files are stored on disk0 or standby-disk0 only when a second card is not installed.

The **copy**, **dir**, **delete**, and **rename** commands all recognize the device names, as in the following examples. Disk1 and standby-disk1 accept only dump files. This means that you can copy only .dmp files to the second disk, delete only .dmp files from the second disk, and rename only .dmp files on the second disk.

```
host1#copy reset05.dmp server2:reset05.dmp
host1#copy disk0:051802.dmp server2:reset05.dmp

host1#delete disk1:reset05.dmp
host1#delete standby:reset05.dmp
host1#delete standby-disk0:reset05.dmp
host1#delete standby-disk1:reset05.dmp

host1#rename standby-disk1:foo.dmp standby-disk1:bar.dmp
host1#rename foo.dmp /outgoing/bar.dmp

host1#dir
Please wait...

active/standby file systems are synchronized

   unshared                                                              in
     file                   size         size         date (UTC)        use
--------------            ---------    --------   -------------------   ---
disk0:reboot.hty             654336      654336   03/01/2005 16:08:28
disk0:system.log               3644        3644   11/30/2004 20:48:18
disk0:special.rel          159256660    61695156   02/18/2005 10:31:48
disk0:lm4_12.dmp           344200394   344200394   02/12/2005 12:12:12
standby-disk0:lm4_13.dmp   344200394   344200394   02/13/2005 13:13:13
disk1:lm4_14.dmp           344200394   344200394   02/14/2005 14:14:14
standby-disk1:lm4_15.dmp   344200394   344200394   02/15/2005 15:15:15
disk0:boston.scr               833         833   02/22/2005 17:46:18
disk0:bulkstats.scr            170         170   02/13/2006 17:34:30
ram:bulkstats1.sts             737         737   03/07/2006 09:07:52

              Disk capacity
              -------------
          Capacity      Free      Reserved
Device    (bytes)      (bytes)    (bytes)
------   ----------   ---------   --------
disk0:   1025482752   342066375   68157440
ram:        5767168     5734400          0
```

Because the device names are reserved, if you upgrade from a release where you previously used those names for remote hostnames, an error message appears when you try to use that remote hostname:

```
%ambiguous file name, reserved disk device name "disk1" must be removed from
host table
```

To prevent corruption of flash cards, always issue the **halt** command before you remove an SRP module. See *Removing an SRP Module* on page 313. Issue the **halt** command before you remove a flash card installed as disk 0 or standby disk 0. Flash cards installed and mounted as disk1 or standby disk1 can be safely removed by issuing the **no mount** command for the card and then ejecting the card. Always reboot the router using the rebooting procedure. See *Chapter 11, Booting the System*. Do not reboot the router by switching it off and on.

Installing and Removing Flash Cards

For information about replacing flash cards, see *ERX Hardware Guide, Chapter 4, Installing Modules*, or *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*.

Before you remove the second flash card (disk1) on the SRP 120 module or the SRP 320 module, you must first unmount the card with the **no mount** command. This command causes the file system to reject all subsequent requests for opening files on the flash card and closes all open files. When this is accomplished, the disk is marked as safely unmounted and a status message indicates that is safe to eject the disk. A status message is displayed when you issue the **mount** or **no mount** command:

- When you issue the **mount** command:

  ```
  % Device is mounted
  % Device is already mounted
  % Device is not present
  ```

- When you issue the **no mount** command:

  ```
  % Device is dismounted
  % Device is already dismounted
  % Device is not present
  % Command failed, files are open on device
  ```

CAUTION: When you eject a mounted disk 0 while the router is in an operational state, the SRP module initiates a reload. When you eject a mounted disk 1, data on the disk can be corrupted, but the router does not reboot.

mount

- Use to mount the disk. If the disk was not safely unmounted previously, then before mounting the file system and permitting user access the command initiates disk and file system integrity checks. These checks are the same ones that are automatically performed when a disk is installed and the SRP module is reloaded.
- This command applies only to the flash card installed in slot 1 on an SRP 320 module. The command is rejected if you specify disk0, because that card is required for system operation and cannot be unmounted.
- Example

  host1#**mount disk1**

- The **no** version prepares the flash card for safe removal. The router subsequently behaves as if the second flash card is no longer present. To access the second card, you must either eject and re-insert the card, or issue the mount command for the card. You can use the **force** keyword to force the dismount even when files on the flash disk are open for modification.

Synchronizing Flash Cards

NOTE: The information in this section does not apply to the ERX-310 router, which does not support SRP module redundancy.

When the router contains two SRP modules, the contents of the modules' flash cards need to be synchronized. Synchronization prevents the redundant flash card from overwriting saved files on the primary flash card if the primary SRP module fails and the redundant SRP module takes control.

By default, autosynchronization is enabled on the router. Autosynchronization runs as a background process every 5 minutes, tracking changes in image, configuration, and script files, and keeping the two SRP modules synchronized. You can also synchronize the SRP modules manually by issuing the **synchronize** command.

Before synchronization, the router does the following:

- Verifies that critical files on the primary SRP module are present. If files are missing, the router does not proceed with the synchronization.
- Verifies whether there is enough space on the redundant flash card to copy all the new or changed files from the primary flash card.

Depending on the outcome of the space verification, the router proceeds as follows:

- If the card has enough space, the router copies new or changed files from the primary flash card to the redundant flash card without deleting any files on the redundant flash card. If the router is interrupted while it is synchronizing with this method, the synchronization resumes when it has recovered from the interruption.

- If the card does not have enough space, the router deletes any files on the redundant flash card that do not appear on the primary flash card, then copies new or changed files from the primary flash card to the redundant flash card. If the router is interrupted while it is synchronizing with this method, it does not resume the synchronization when it has recovered from the interruption.

If an SRP synchronization is in progress or has failed and the router is recovering, the router prevents the redundant SRP module from taking the primary role while the primary is rebooting and for 30 seconds after the primary module has rebooted. These conditions prevent a redundant SRP module with corrupted or missing files from becoming the primary and overwriting files or directories on the primary module.

synchronize

- Use to force the file system of the redundant SRP module to synchronize with the flash file system of the primary SRP module.
- If you synchronize the redundant SRP module with the primary SRP module and the redundant module is armed with a release different from the one it is currently running, the redundant SRP module is automatically rebooted to load the armed release.
- Optionally, you can use the **low-level-check** keyword to force the router to validate all files or only configuration files in NVS, and to synchronize all files that failed the checksum test during the **flash-disk-compare** command as well as any other files that are unsynchronized. See *Validating and Recovering Redundant SRP File Integrity* on page 347 for details.

NOTE: In most cases, use the **synchronize** command instead of the **synchronize low-level-check** command. The **synchronize low-level-check** command is provided for troubleshooting, and is intended to be used under direction from JTAC.

- Examples

  host1#**synchronize**
  host1#**synchronize low-level-check all**
  host1#**synchronize low-level-check configuration**

- There is no **no** version.

Synchronizing Flash Cards of Different Capacities

If the capacity of the primary flash card is equal to or smaller than that of the redundant flash card, the router copies all the files from the primary flash card to the redundant flash card. However, if the capacity of the primary flash card exceeds that of the redundant flash card, the router creates a hidden synchronization reserve file on the primary flash card, provided enough space is available for the file.

The purpose of the synchronization file is to prevent the creation of data that cannot fit on the redundant flash card. The file contains no useful data, and does not appear when you view the files in NVS. The size of the file is equal to the difference in capacities of the two flash cards. For example, if the primary flash card has a capacity of 224 MB, and the redundant flash card has a capacity of 220 MB, the size of the synchronization file is 4 MB, and only 220 MB of space is available on the primary flash card.

If the primary flash card does not have enough space to create the synchronization reserve file, the **synchronize** command fails, and you see a warning message on the console. To resolve this issue, either delete unwanted files from the primary flash card or replace the redundant flash card with a higher-capacity flash card.

Disabling Autosynchronization

If autosynchronization is enabled while you are copying long scripts or installing new software releases, it detects a disparity between the modules during the middle of the process. This feature causes significant unnecessary synchronization, resulting in prolonged copy times.

If you have installed a redundant SRP module, perform the following steps before copying long scripts:

1. Turn off autosynchronization with the **disable-autosync** command.
2. Perform the installation or copy the script.
3. Reenable autosynchronization with the **no disable-autosync** command.
4. Manually synchronize the modules with the **synchronize** command.

Refer to the commands and guidelines in the previous section and in the sections that follow.

disable-autosync

- Use to turn off automatic synchronization between the primary and redundant SRP modules.
- Example

  host1(config)#**disable-autosync**

- Use the **no** version to revert to the default situation, in which automatic synchronization runs as a background process every 5 minutes.

Validating and Recovering Redundant SRP File Integrity

NOTE: The information in this section does not apply to the ERX-310 router, which does not support SRP module redundancy.

Even when flash cards on the primary and redundant SRP modules are synchronized, differences can exist in the content of files that reside on the primary flash card and the redundant flash card. You can use the **flash-disk compare** command to detect these differences so you can validate and, if necessary, recover the file integrity of the redundant SRP module.

The **flash-disk compare** command validates only those files that are synchronized between the primary and redundant SRP modules. It does not compare files that are normally excluded from the synchronization process, such as log files and core dump files. The command uses a simple checksum error detection algorithm to compare the contents of a file residing on the flash card of the primary SRP module with the contents of the same file residing on the flash card of the redundant SRP module.

To validate and recover redundant SRP file integrity:

1. Ensure that the file systems on the primary flash card and the redundant flash card are synchronized. (See *Synchronizing Flash Cards* on page 344 for details.)

2. Issue the **flash-disk compare** command, specifying whether to perform the checksum validation for all files in NVS or only for configuration files.

   host1#**flash-disk compare all**
   host1#**flash-disk compare configuration**

   The **flash-disk compare configuration** command, which validates only configuration files, excludes larger files such as software releases and scripts from the validation process. As a result, this command takes less time to complete than the **flash-disk compare all** command, which validates all NVS files.

3. Review the **flash-disk compare** output to determine whether any files failed the checksum validation.

   If the **flash-disk compare** command detects differences in the content of one or more files, the router reports a checksum test failure.

4. If one or more files failed the checksum validation, determine whether the corrupted files reside on the primary SRP module or on the redundant SRP module.

5. If the corrupted file resides on the primary SRP module, issue the **srp switch** command to force a switch from the primary SRP module to the redundant SRP module.

   This action ensures that the error-free version of the file will be on the SRP module that takes control after the switch.

6. Issue the **synchronize** command with the **low-level-check** keyword to force the router to:

   - Validate all files in NVS (when you use the **all** keyword) or only configuration files in NVS (when you use the **configuration** keyword).
   - Synchronize all files that failed the checksum test during the **flash-disk compare** command, as well as any other unsynchronized files.

   host1#**synchronize low-level-check all**
   host1#**synchronize low-level-check configuration**

   This action resolves any file discrepancies between the primary and redundant SRP modules and restore SRP file integrity.

NOTE: Both the **flash-disk compare** and **synchronize low-level-check** commands perform CPU-intensive processing that can take several minutes to complete. For best results, do not run these commands simultaneously on the same router. In addition, do not run multiple instances of the **flash-disk-compare** command simultaneously on the same router.

flash-disk compare

- Use to perform a checksum validation that compares the contents of the NVS file system on the primary SRP module with the contents of the NVS file system on the redundant SRP module.
- The command validates only those files that are synchronized between the primary and redundant SRP modules; it does not validate log files, core dump files, and other files that are excluded from the system synchronization process.
- Specify one of the following keywords:
  - **all**—Compares all files in NVS; this option can take several minutes to complete.
  - **configuration**—Compares only configuration files; this option takes less time to complete because it compares only a subset of the files in the NVS file system.
- If all files pass the validation test, the router reports that all checksums matched and displays the total number of files and total number of bytes of information compared.
- If one or more files fail the validation test, the router reports a checksum test failure and does not display the total number of files and bytes compared.
- If one or more of the following conditions exist, the command fails and the router displays a message that explains why it cannot perform the checksum test:
  - The file systems on the primary flash card and the redundant flash card are not synchronized.
  - The router does not contain a redundant SRP module.
  - The redundant SRP module is offline.

- Example 1—Shows output when all files passed the validation test

```
host1#flash-disk compare all
WARNING: This command may take several minutes to complete.
Proceed? [confirm]
WARNING: No changes should be made to the system while this command is in
         progress.
Please wait.....................................................
All file checksums matched.
Number of Files = 866
Number of Bytes = 61660650
```

- Example 2—Shows output when one or more configuration files failed the validation test

```
host1#flash-disk compare configuration
WARNING: This command may take several minutes to complete.
Proceed? [confirm]
WARNING: No changes should be made to the system while this command is in
         progress.
Please wait......
At least one configuration file failed checksum test.
```

- There is no **no** version.

synchronize

- Use to force the NVS file system of the redundant SRP module to synchronize with the NVS file system of the primary SRP module.
- If you synchronize the redundant SRP module with the primary SRP module and the redundant module is armed with a release different from the one it is currently running, the redundant SRP module is automatically rebooted to load the armed release.
- Optionally, you can use the **low-level-check** keyword to force the router to validate all files or only configuration files in NVS, and to synchronize all files that failed the checksum validation test during the **flash-disk-compare** command as well as any other files that are unsynchronized.
- When you use the **low-level-check** keyword, you must also specify one of the following keywords:
  - **all**—Validates all files in NVS, and synchronizes all files that failed the checksum test as well as any other unsynchronized files; this option can take several minutes to complete.
  - **configuration**—Validates all configuration files in NVS, and synchronizes all files that failed the checksum test as well as any other unsynchronized files; this option takes less time to complete because it validates only a subset of the files in the NVS file system.
- If one or more of the following conditions exist when you use the **low-level-check** keyword, the command fails and the router displays a message that explains why it cannot perform the synchronization:
  - The router does not contain a redundant SRP module.
  - The redundant SRP module is offline.
  - The armed releases are different on the primary SRP and redundant SRP.

- Examples

  host1#**synchronize**
  host1#**synchronize low-level-check all**
  host1#**synchronize low-level-check configuration**

- There is no **no** version.

Reformatting the Primary Flash Card

You can reformat the primary flash card. To do so:

1. Access Boot mode.

   a. From Privileged Exec mode, enter the **reload** command. Information about the reloading process is displayed.

   b. When the countdown begins, press the mb key sequence (case-insensitive).

      The CLI enters Boot mode (:boot## prompt). If you do not press the mb key sequence, the reloading process continues and returns the CLI to the normal User Exec mode.

2. Issue the **flash-disk initialize** command.

flash-disk initialize

- Use to reformat the flash card.
- You can perform a low-level format of the flash card.
- On the E120 and E320 routers only, you can use this command to format a second flash card installed as disk1. You can issue this command in Boot mode for either flash card. In Privileged Exec mode, you can use the **disk1** keyword to access the unmounted second flash card while the router is in an operational state.
- This command is available for disk1 in Privileged Exec mode only on SRP 320 modules. This command is not accepted for disk0 in Privileged Exec mode.
- Example 1

```
host1#halt primary-srp
host1#reload
WARNING: Execution of this command will cause the system to reboot.
Proceed with reload? [confirm]
Reload operation commencing, please wait...
[ Press mb]
:boot##flash-disk initialize
```

- Example 2—On an SRP 320 module

```
host1#no mount disk1
% Device is dismounted
host1#flash-disk initialize disk1
WARNING: Execution of this command will cause the contents of disk1 to be
erased.
Proceed with Flash disk initialization? [confirm]
Please wait.............................
```

- There is no **no** version.

Copying the Image on the Primary SRP Module

NOTE: The information in this section does not apply to the ERX-310 router, which does not support SRP module redundancy.

You can copy the contents of NVS on the primary SRP module to a spare flash card. To do so:

1. Access Boot mode.

   a. From Privileged Exec mode, enter the **reload** command. Information about the reloading process is displayed.

   b. When the countdown begins, press the mb key sequence (case-insensitive).

      This CLI enters Boot mode (:boot## prompt).
      If you do not press the mb key sequence, the reloading process continues and returns the CLI to the normal User Exec mode.

2. Issue the **flash-disk duplicate** command.

3. Follow the instructions on the screen. When prompted, insert the original or spare flash card in the primary SRP module.

flash-disk duplicate

- Use to copy the contents of the primary flash card to a spare flash card.
- The primary and spare flash cards must be from the same manufacturer and must have the same size.

NOTE: This command is available only in Boot mode.

- When you issue the **flash-disk duplicate** command, insert the original and spare flash cards when prompted. The router copies the flash card contents incrementally, so you may need to exchange the flash cards several times.

- Example

```
host1#halt primary-srp
host1#reload
WARNING: Execution of this command will cause the system to reboot.
Proceed with reload? [confirm]
Reload operation commencing, please wait...
[ Press mb]
:boot##flash-disk duplicate
```

- There is no **no** version.

Scanning Flash Cards

You can find both structural errors in the data in NVS and physical errors in the flash card. You can also remove files with errors, and attempt to repair structural or physical errors.

check-disk

- Use to find and repair structural inconsistencies and damage in the DOS file system in NVS on the primary SRP module.
- If the router contains primary and redundant modules, only NVS on the primary SRP module is scanned.
- On the E120 and E320 routers only, you can use this command to check and repair a second flash card installed as disk1. You can issue this command in Boot mode for either flash card. In Privileged Exec mode, you can use the **disk1** keyword to access the unmounted second flash card while the router is in an operational state.
- This command is available for disk1 in Privileged Exec mode only on SRP 320 modules. This command is not accepted for disk0 in Privileged Exec mode.
- Example

```
:boot##check-disk disk0
Copyright (c) 1993-1996 RST Software Industries Ltd. Israel. All rights reserved
ver: 2.6 FCS

Disk Check In Progress ...


        total disk space (bytes) :                    512,122,880
        bytes in each allocation unit :               8,192
        total allocation units on disk :              62,515
        bad allocation units :                        1
        available bytes on disk :                     120,651,776
        available clusters on disk :                  14,728
        maximum available contiguous chain (bytes) :  120,651,776
        available space fragmentation (%) :           0
        clusters allocated :                          47,786
Done Checking Disk.
```

- There is no **no** version.

flash-disk scan

- Use to find and repair files with physical errors in NVS. These errors are created if the router is not powered down or reset correctly.
- If the router contains primary and redundant modules, only NVS on the primary SRP module is scanned.
- Use the **repair** keyword to fix nonfatal errors found on the disk. If the repair fails, the router no longer uses the corrupted areas.
- On the E120 and E320 routers only, you can use this command to find and repair files on a second flash card installed as disk1. You can issue this command in Boot mode for either flash card. In Privileged Exec mode, you can use the disk1 keyword to access the unmounted second flash card while the router is in an operational state.
- This command is available for disk1 in Privileged Exec mode only on SRP 320 modules. This command is not accepted for disk0 in Privileged Exec mode.
- Example
  In this example, the user scans NVS and finds one file with an error. The user then issues the **flash-disk scan** with the **repair** keyword to remove the file. Finally, the user scans NVS again, and finds no files with errors.

```
:boot##flash-disk scan
Proceed with Flash disk scan? [confirm]
Srp PCMCIA Card Scan...
Boot Block OK
File Allocation Table OK
Root Directory OK
Checking File Space
Please Wait...
Checking Free Space
Please Wait...
PCMCIA Card Scan Detected Errors in:
\\images\ct1Diag\ct1Diag3c440e9e.cmp

PCMCIA Card Scan successful!


:boot##flash-disk scan repair
WARNING: Execution of this command may cause the contents of the Flash disk
to be modified.
Proceed with Flash disk scan? [confirm]
Srp PCMCIA Card Scan...
Boot Block OK
File Allocation Table OK
Root Directory OK
Checking File Space
Please Wait...
Checking Free Space
Please Wait...
PCMCIA Card Scan Removed:
\\images\ct1Diag\ct1Diag3c440e9e.cmp

PCMCIA Card Scan successful!


:boot##flash-disk scan
Proceed with Flash disk scan? [confirm]
Srp PCMCIA Card Scan...
Boot Block OK
File Allocation Table OK
```

```
Root Directory OK
Checking File Space
Please Wait...
Checking Free Space
Please Wait...
PCMCIA Card Scan successful!
```

- There is no **no** version.

Monitoring Flash Cards

Use the **show nvs** command to monitor the status of NVS on the primary SRP module. Use the **show flash** command to view information about the flash card.

show flash

- Use to display information about the flash card.
- Field descriptions
  - Active System Controller—Information for flash cards on the active SRP module
  - disk0—Flash card installed in slot 0 of the SRP module
  - disk1—Flash card installed in slot 1 of the SRP module; available only on SRP modules for the E120 and E320 routers
  - Manufacturer—Name of manufacturer of the installed flash card
  - Capacity—Total capacity of the flash card, in bytes
  - Standby System Controller—Information for flash cards on the standby SRP module
- Example

```
host1#show flash

          Active System Controller:
          -------------------------
Device    Manufacturer     Capacity    Status
------   --------------   ----------   -------
 disk0   SILICONSYSTEMS   1047126528   mounted
 disk1   STI              1024966656   mounted

             Standby System Controller:
             --------------------------
   Device         Manufacturer     Capacity    Status
-------------   --------------   ----------   -------
standby-disk0   SILICONSYSTEMS   1047674880   mounted
standby-disk1   SILICONSYSTEMS   1047674880   mounted
```

show nvs

- Use to monitor NVS status.
- Field descriptions
  - total nvs file sizes—Sum of sizes of all files in NVS, in bytes
  - total nvs file errors—Number of read and write errors in all files in NVS
  - nvs flash in use—NVS used, in bytes
  - available nvs flash—NVS available, in bytes
- Example

```
host1#show nvs
total nvs file sizes =  228864
total nvs file errors = 0
nvs flash in use =      1265152
available nvs flash =   35435008
```

Updating the Router with JUNOSe Hotfix Files

A JUNOSe hotfix is a file or collection of files that you can apply to update an operational E-series router to address one or more specific, critical software issues. The hotfix can replace or add functionality to one or more software components. Hotfixes also enable the delivery of software updates without having to load an entire software release. Hotfixes can also deploy debugging code to collect data that facilitates troubleshooting of software issues.

Although most hotfixes can also be manually activated without reloading the router, some hotfixes cannot. You can configure any hotfix to be activated automatically when the router reloads.

A hotfix consists of a .hfx file and possibly other supporting files. The .hfx file manages the associated files in much the same way that a .rel file manages supporting files associated with a release image.

To use a hotfix, you must use the **copy** command to download the file from a network host to the router. You cannot copy the hotfix to an FTP file server. You can use file system commands such as **dir**, **rename**, and **delete** with the hotfix. After a hotfix is copied to the local flash card, it remains there until you explicitly delete it.

Hotfixes must be activated to take effect. A *startup* hotfix is automatically activated during system initialization. A *hot-patchable* hotfix does not require a reload to become active; it takes effect immediately if compatibilities and dependencies are correctly met. You can manually install hot-patchable hotfixes with the **hotfix activate** command. Hot-patchable hotfixes can also be configured to be activated as a startup hotfix.

Arming a hotfix prepares it for activation after a system reload. You can configure hotfixes in several ways with the **boot hotfix** and **hotfix activate** commands, as in the following examples:

- Activated immediately on an active router but not armed as a startup hotfix. In this case, the hotfix is activated only until the SRP module reloads. If the SRP module reloads, then you must manually activate the hotfix again (if desired) with the **hotfix activate** command.

- Activated immediately on an active router and armed as a startup hotfix. In this case the hotfix is automatically activated after every reload.

- Armed as a startup hotfix with the **boot hotfix** command but not immediately activated. In this case the hotfix is activated when the SRP module reloads.

When a system reloads with the backup settings specified by the **boot backup** command, no armed hotfixes are activated. The currently armed hotfix settings are retained in the event that the router reverts back to its normal boot settings.

Hotfix Compatibility and Dependency

Hotfixes can have compatibility and dependency requirements. A given hotfix is compatible with one or more releases. It can be dependent on one or more other hotfixes being active. Compatibility and dependency requirements are stored as part of the hotfix. The requirements are enforced at the time of arming or activation. If the software installed and active on the router does not match the requirements specified in the hotfix, then activation of the hotfix fails. Such a failure generates appropriate error and log messages.

The following restrictions can apply to a hotfix:

- Dependency—A hotfix that must be active or armed before another hotfix can be activated or armed.

- Safe With—A list of hotfixes with which another hotfix is compatible and can safely be concurrently armed or activated. This list applies only to hotfixes that have some patched functionality in common and are armed or activated concurrently.

- Unsafe With—A list of hotfixes with which another hotfix is not compatible and cannot safely be concurrently armed or activated. The CLI displays a warning message when you try to activate a hotfix that is unsafe with one or more active or armed hotfixes.

- Manual Activate [Active / Standby] Srp—The name of a binary flag that indicates whether manual activation of the hotfix is allowed on the active and standby SRP modules. When the flag is set to false, you cannot manually activate the hotfix; instead, the hotfix can only be activated as a startup hotfix. The CLI displays a warning message when you try to activate a hotfix that cannot be manually activated.

- Manual Deactivate [Active / Standby] Srp—The name of a binary flag that indicates whether manual deactivation of the hotfix is allowed on the active and standby SRP modules. When the flag is set to false, you cannot manually deactivate the hotfix. You must disarm the hotfix and reload the router. The CLI displays a warning message when you try to deactivate a hotfix that cannot be manually deactivated.

- Line card requires reload—The name of a binary flag that indicates whether line modules require a reload for the hotfix to become active on the module. The CLI displays a warning message if the line modules must be reloaded. If the warning is confirmed, the SRP module reloads each line module. The flag applies to all line modules targeted by the hotfix that are installed in the router.

Hotfixes remain armed only for compatible releases. If you change the armed release by issuing the **boot system** command, hotfixes that are not compatible with the new release are no longer armed. However, if you subsequently rearm a compatible release, the previously armed hotfixes for that release are automatically armed again.

Removing Hotfixes

You can deactivate, disarm, and delete hotfixes from a router. When you deactivate a hotfix, any functionality that was added as part of the hotfix is automatically removed (even though the .hfx file remains on the router).

You cannot deactivate a hotfix that is a dependency for other hotfixes until you deactivate the dependent hotfixes. When a hotfix is no longer active, you can use the **delete** command to remove the hotfix file from the flash card.

Hotfixes and Backup Settings

The **boot backup** command does not explicitly support hotfix files. When a system reloads with the backup settings specified by the **boot backup** command, no armed hotfixes are activated. However, the armed hotfix settings are retained in the event that the system reverts to its normal (nonbackup) boot settings. If that happens, these hotfixes are automatically rearmed and reactivated after a reload.

Hotfixes and Standby SRP Modules

Hotfixes are supported in redundant SRP module configurations. Hotfix files are synchronized between the active and standby SRP modules by both automatic and manual synchronization. Hotfix activation restrictions are enforced identically on the active and standby SRP modules. A hotfix that is hot-patchable on the active module is hot-patchable on the standby module. A hotfix that requires startup activation on the active SRP module also requires startup activation on the standby SRP module.

Hotfixes are synchronized from the active SRP module to the standby SRP module. The standby SRP automatically activates the hotfixes that are armed as startup hotfixes. However, if the synchronization reveals that the set of active hotfixes on the standby SRP module is different from the set of armed hotfixes on the active SRP module, then the standby SRP module automatically reboots. This action causes the standby SRP module to activate the startup hotfixes. When you activate or arm a hotfix for startup activation, compatibility and dependency checks are performed independently on the active and standby SRP modules.

Hotfixes and Line Modules

For line modules, a hotfix consists of one or more image fixes specific to a particular model of module or to a module type, depending on the fix. When a hotfix is activated, each image fix contained in the hotfix is activated on all applicable modules that are installed in the router. When existing line modules come online during startup and when new line modules are inserted in the chassis, image fixes for that particular line module are requested and activated during module startup.

Line module image hotfixes that have been armed as startup hotfixes are activated before application configuration occurs on the line module.

Only image fixes contained in hotfixes that are active on the primary SRP module can be activated on the line modules during startup. Hotfixes that are armed but not active on the primary SRP module are not activated on line modules.

A hotfix can contain a combination of image fixes. System controller (SC) and interface controller (IC) image fixes are cumulative and activated in the order in which they were armed. For forwarding controller (FC) image fixes, the last one armed is the only one applied.

NOTE: Because image fixes are activated in a particular order, we recommend that you create a list of any hotfixes that you are currently running or intend to run with a new FC image fix. JTAC can then provide you with the correct order of activation.

A hotfix cannot be partially activated on a router. If activation of any image hotfix fails on any corresponding module, the entire activation fails for all applicable line modules. Activation failure results in the generation of an appropriate log message. E-series routers do not support activation of a hotfix on a per-slot basis or a per-subsystem basis.

For example, suppose that a hotfix contains an image fix for the SRP module and the GE-2 line module. The SRP image fix is successfully activated on the SRP module, but the activation of the GE-2 image fix fails for some reason. In this case, the SRP module image fix is deactivated and no further attempts are made to activate the image fix on other GE-2 modules.

boot hotfix

- Use to arm the specified hotfix as a startup hotfix that is automatically activated the next time the SRP module reboots.
- Arming fails if the specified hotfix depends on a hotfix that is not already armed. In this event, the CLI displays an error message similar to the following:

  ```
  % The hotfix, 975, requires the following hotfixes to be armed:
        990
  ```

- Arming fails if the hotfix is not compatible with the armed release. The CLI displays the following error message:

  ```
  % Hotfix is incompatible with armed release.
  ```

- When a router reverts to its backup boot settings, as specified by the **boot backup** command, no armed hotfixes are activated. The armed hotfix settings are retained in the event the router reverts back to its normal boot settings.
- Example

  host1(config)#**boot hotfix hf63037.hfx**

- Use the **no** version to disarm a specified hotfix. You can disarm all hotfixes armed for all releases by specifying the **all-releases** keyword. If any startup hotfixes are armed, the CLI then prompts you to confirm the deletion,

If the hotfix being disarmed is a dependency for another armed hotfix, the command fails and the CLI displays an error message similar to the following:

```
The hotfix, 990, has the following armed dependents which must be disarmed
first:
        975

% Disarming failed
```

When you disarm hotfixes that have dependencies, you must disarm them in the reverse sequence from which they were armed. However, if you have issued the **all-releases** keyword, the disarming automatically takes place in the correct order.

no boot hotfix all-releases

- Use in Boot mode to disarm all armed hotfixes for all releases.
- Example

  :boot##**no boot hotfix all-releases**

- There is no affirmative version of this command; there is only a **no** version.

hotfix activate

- Use to manually activate the specified hotfix.
- Each image fix contained in the hotfix is downloaded from the local flash card to the SRP module and any corresponding line module, and then activated on the modules.
- When a new line module is inserted in the router, all applicable image fixes are activated during initialization of the module. Activation is performed by the line module operational image before application configuration takes place on the module.
- An activation failure for any image fix on its corresponding line module causes the entire activation to fail. The image fix is then deactivated on any modules on which it was successfully activated.
- Activation fails if the specified hotfix is incompatible with the running release, In this event, an error message similar to the following is displayed:

  ```
  % Hotfix is incompatible with running release.
  ```

- Activation fails if the specified hotfix depends on other hotfixes that have not been activated. The CLI displays an error message similar to the following:

  ```
  The hotfix, 975, requires the following hotfixes to be activated:
          990

  % Activation failed
  ```

- Startup hotfixes cannot be manually activated. If you attempt to manually activate a startup hotfix, the operation fails and generates the following error message:

  ```
  % Manual activation not allowed
  ```

- Example

  host1#**hotfix activate hf63037.hfx**

- Use the **no** version to manually deactivate the specified hotfix. Deactivation restores the system to the state that existed before the hotfix was activated. You can specify the **all** keyword to deactivate all active hotfixes.

  When you deactivate hotfixes that have dependencies, you must deactivate them in the reverse sequence from which they were armed. However, if you have issued the **all** keyword, the disarming automatically takes place in the correct order.

Monitoring Hotfixes

Several commands provide information about hotfixes that have been loaded on the router. You can use the **show hotfix** command to discover the armed and activation status of all hotfixes or a specific hotfix. The output lists the hotfix by name and a unique ID number, which is useful if the filename has been changed. This command also displays dependencies for each hotfix; that is, other hotfixes that must be activated before that hotfix can be activated. For more usage details and sample output, see **show hotfix** on page 362.

The **dir** command displays all hotfixes present on the local flash card. The in use field indicates that the hotfix is either currently activated or armed to be activated as a startup hotfix for the currently armed release.

```
host1#dir

*** Active/standby file systems are not synchronized. ***

Active System Controller:
                                      unshared                          in
          file                 size       size          date (UTC)       use
-------------------------   ---------   ---------   -------------------   ---
reboot.hty                     596288      596288   03/07/2005 19:35:52
system.log                       6762        6762   03/07/2005 17:30:08
haIpSetup.mac                    4874        4874   03/24/2004 10:02:08
6-0-1p0-5.rel                148489185   148489185   02/28/2005 18:17:32   !
hf63035.hfx                      30445       30445   03/07/2005 14:04:02   !
hf63030.hfx                      28675       28675   03/05/2005 18:22:32
...
```

You can use the **show version** command to display a summary of each of the hotfixes currently activated on the system, including the hotfix name and hotfix ID.

```
host1#show version

Juniper Edge Routing Switch ERX-1400
Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
System Release: 6-0-1p0-5.rel
        Version: 6.0.1 patch-0.5   (January 28, 2005  14:55)
        Active hotfixes:
                  hf63036.hfx (Id: 1020)
                  hf63037.hfx (Id: 1030)
System running for: 7 days, 3 hours, 55 minutes, 5 seconds
        (since FRI FEB 04 2005 13:01:30 UTC)
```

The **show boot** command displays the current boot settings, including armed hotfixes that will be activated when the router reboots.

```
host1#show boot

System Release:   6-0-1p0-5.rel
        Armed Hotfixes: hf63035.hfx
        hf63036.hfx
        hf63037.hfx
System Configuration: running-configuration
```

The header of the **show configuration** command output includes the armed hotfix summary. You can issue the **show configuration system file-system** command to display the **boot hotfix** commands that restore the router to its current configuration when you issue the configuration script on a router configured with factory defaults.

Hotfixes that are active when you issue the **show configuration** command are not part of the command output or the resulting configuration script. Only armed hotfixes are part of the **show configuration** script.

```
host1#show configuration system file-system

! Configuration script being generated on TUE MAR 22 2005 16:43:41 UTC
! Juniper Edge Routing Switch ERX-1400
! Version: 6.0.1 patch-0.5   (January 28, 2005  14:55)
!     Active hotfixes: hf63036.hfx (Id: 23453036)
!                      hf63037.hfx (Id: 34563037)
! Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 15
!
boot config running-configuration
boot system 6-0-1p0-5.rel
boot hotfix hf63036.hfx
boot hotfix hf63037.hfx
no boot backup
no boot subsystem
no boot backup subsystem
no boot force-backup
```

show hotfix

- Use to display the name, ID, activation and arming status, and dependencies for all hotfixes or a specific hotfix available on the local file system.
- You can issue the **detail** keyword to additionally display a synopsis of the hotfix behavior. The detailed output for a specific hotfix also indicates compatible and incompatible hotfixes and lists modules affected by the hotfix.
- Field descriptions
  - name—Filename of the hotfix
  - id—Number uniquely identifying the hotfix; nonconfigurable so that you can identify the hotfix if the filename has been changed
  - active—Status of hotfix activation; X indicates that the hotfix is active

- armed—Status of hotfix arming; X indicates that the hotfix is armed to be activated; only hotfixes armed for the currently armed release are displayed as armed
- requires—Hotfix ID number or numbers identifying hotfix dependencies, which are hotfixes that must be activated before this hotfix can be activated
- synopsis—Brief description of the functionality or behavior of the hotfix
- Description—More detailed description of the functionality or behavior of the hotfix
- Dependencies—Hotfix ID number or numbers identifying hotfix dependencies, which are hotfixes that must be activated before this hotfix can be activated
- Safe to repatch—Hotfix ID number or numbers of hotfixes that can be concurrently active with this hotfix; applies only to hotfixes that fix the same existing functionality
- Unsafe with—Hotfix ID number or numbers of hotfixes that are incompatible and cannot be activated at the same time as this hotfix
- Notes—Restrictions on manual activations or deactivations

- Example 1

```
host1#show hotfix

      name          id    active   armed   requires
----------------   ----   ------   -----   ----------
sleep.hfx           975     X        X          990
clock.hfx           990     X        X
showHotfix.hfx     2010
incompatible.hfx    410
hfActivate.hfx      960
```

- Example 2—The **detail** keyword additionally displays a synopsis of the hotfix.

```
host1#show hotfix detail

      name          id    active   armed   requires
----------------   ----   ------   -----   ----------
sleep.hfx           975     X        X          990
clock.hfx           990     X        X
showHotfix.hfx     2010
incompatible.hfx    410
hfActivate.hfx      960
      name                          synopsis
----------------   ------------------------------------------------
sleep.hfx          Modify the output of the sleep command.
clock.hfx          Modify the behavior of show clock.
showHotfix.hfx     Changes the output of show hotfix.
incompatible.hfx   Changes the output of show hotfix.
hfActivate.hfx      Change log message severity for hotfix activate.
```

- Example 3—The **detail** keyword for a particular hotfix displays the most detailed information.

```
host1#show hotfix clock.hfx detail
HotfixId: 990

Synopsis: Modify the behavior of show clock.

Active: Yes
Armed: Yes

Description:  Changes the output of the show clock command.

Affected modules: SRP, GE, VTM

Dependencies:

Safe to repatch:

Unsafe with:

Notes:
1) This hotfix can only be activated when the active SRP reloads
2) Arming this hotfix will cause the standby SRP to reload
```

Example: Using and Monitoring Hotfixes

This example presents several aspects of hotfix use. In this example, 6-0-1p0-5.rel is the currently armed and active release. Hotfix hf63035.hfx is compatible with this release and is currently activated and armed as a startup hotfix.

```
host1#dir

Active System Controller:
                                        unshared                          in
          file                  size        size          date (UTC)       use
-------------------------   ---------   ---------   -------------------   ---
reboot.hty                      596288      596288   03/07/2005 19:35:52
system.log                        6762        6762   03/07/2005 17:30:08
haIpSetup.mac                     4874        4874   03/24/2004 10:02:08
6-0-1p0-5.rel                125987342   125987342   02/30/2005 18:17:32    !
6-1-0.rel                    148489185   148489185   02/28/2005 20:19:20
hf63035.hfx                       30445       30445   03/07/2005 14:04:02   !
hf63036.hfx                       27445       27445   03/07/2005 16:12:05
hf63037.hfx                       28324       28324   03/07/2005 16:13:25

host1#show hotfix detail

   name         id     active  armed   requires
-----------  --------  ------  -----   -----------
hf63035.hfx  12343035    X       X
hf63036.hfx  23453036
hf63037.hfx  34563037                  23453036

    name            synopsis
-----------      -------------------------------------------
hf63035.hfx      Fix for CQ63035, bgp crash, out of resources
hf63036.hfx      Fixed show version formatting issue
hf63037.hfx      Increased max session limit on ERX310 to 32,000
```

```
host1(config)#boot hotfix hf63037.hfx
% The hotfix, 34563037, requires the following hotfix(es) to be armed:
        23453036
```

The hf63036.hfx hotfix must be armed as a startup hotfix:

```
host1(config)#boot hotfix hf63036.hfx
```

This command succeeds because hf63036.hfx is compatible with the currently armed release, 6-1-0.rel, and has no dependencies on other hotfixes.

Now the attempt to arm hf63037.hfx succeeds because its dependency on hf63036.hfx has been met.

```
host1(config)#boot hotfix hf63037.hfx
```

Now suppose the user reloads the router:

```
host1#reload
```

As the router loads the armed release, 6-1-0.rel, the hotfix loader discovers three armed startup hotfixes, hf63035.hfx, hf63036.hfx, and hf63037.hfx. Only hf63036.hfx and hf63037.hfx are activated. Hotfix hf63035.hfx is disarmed because it is incompatible with the new running release. The router therefore becomes operational running 6-1-0.rel with hf63036.hfx and hf63037.hfx activated.

```
host1#dir

                                        unshared                          in
          file                  size        size          date (UTC)       use
-------------------------   ---------   ---------   --------------------   ---
reboot.hty                     596288      596288   03/07/2005 19:35:52
system.log                       6762        6762   03/07/2005 17:30:08
haIpSetup.mac                    4874        4874   03/24/2004 10:02:08
6-0-1p0-5.rel                125987342   125987342   02/30/2005 18:17:32
6-1-0.rel                    148489185   148489185   02/28/2005 20:19:20   !
hf63035.hfx                      30445       30445   03/07/2005 14:04:02
hf63036.hfx                      27445       27445   03/07/2005 16:12:05    !
hf63037.hfx                      28324       28324   03/07/2005 16:13:25    !
```

```
host1#show hotfix

   name      active  armed   requires
-----------  ------  -----   --------
hf63035.hfx
hf63036.hfx    X       X
hf63037.hfx    X       X      23453036
```

Now suppose the user attempts to deactivate hf63036.hfx:

```
host1#no hotfix activate hf63036.hfx
The hotfix, 23453036, has the following active dependents which must be
deactivated first:
        34563037
% De-activation failed.
```

The command fails because hf63037.hfx is dependent on hf63036.hfx. Interdependent hotfixes must be deactivated and disarmed in the reverse order that they were activated.

When 6-0-1p0-5.rel is re-armed and the router reloaded, the hotfix loader determines that the startup hotfixes, hf63036.hfx and hf63037.hfx, are incompatible with the release. It disarms these hotfixes. The user decides to delete the now unnecessary hotfixes from the router.

```
host1#delete hf63036.hfx
host1#delete hf63037.hfx

host1#dir

Active System Controller:
                                        unshared                          in
          file                  size       size          date (UTC)        use
--------------------------   ---------  ---------   -------------------   ---
reboot.hty                      596288     596288   03/07/2005 19:35:52
system.log                        6762       6762   03/07/2005 17:30:08
haIpSetup.mac                     4874       4874   03/24/2004 10:02:08
6-0-1p0-5.rel                125987342  125987342   02/30/2005 18:17:32   !
6-1-0.rel                    148489185  148412851   02/28/2005 20:19:20
hf63035.hfx                      30445      30445   03/07/2005 14:04:02   !

host1#show hotfix detail

   name         active     armed   requires
-----------  ------------  -----   --------
hf63035.hfx       X          X         ---
```

Managing the Ethernet Port on the SRP Module

You can configure the Fast Ethernet management port to access the router from a Telnet session or SNMP.

On ERX-7xx models, ERX-14xx models, and ERX-310 routers, the Fast Ethernet port is located on the SRP I/O module. For more information about configuring the Fast Ethernet port on an SRP I/O module, see *ERX Hardware Guide, Chapter 7, Accessing ERX Routers*.

Use the Fast Ethernet port on the SRP I/O module only as a router management port. Do not use this port to route traffic for Fast Ethernet or higher-level protocols such as transport or routing protocols, because doing so affects the performance of the router.

On the E120 router and the E320 router, the Fast Ethernet port is located on the SRP IOA. For more information about configuring the Fast Ethernet port on an SRP IOA, see *E120 and E320 Hardware Guide, Chapter 7, Accessing E-Series Routers*.

interface fastEthernet

- Use to select a Fast Ethernet interface on a line module or an SRP module.
- On ERX-7xx models, ERX-14xx models, and the ERX-310 router, specify the Fast Ethernet interface management port by using the *slot/port* format.
- On the E120 and E320 routers, you can specify the Fast Ethernet port on the SRP IOA by using the *slot/adapter/port* format. The port on the SRP IOA is always identified as 0.

- Example 1—Selects a Fast Ethernet management port on ERX-7xx models, ERX-14xx models, or the ERX-310 router

  host1(config)#**interface fastEthernet 0/0**

- Example 2—Selects a Fast Ethernet management port on the E320 router

  host1(config)#**interface fastEthernet 6/0/0**

- Use the **no** version to remove IP from an interface or subinterface.

Monitoring Statistics

You can set a baseline and view statistics on the Fast Ethernet port of the SRP module in the same way that you would for other Ethernet interfaces. See *JUNOSe Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

Monitoring the Ethernet Configuration for the SRP Module

Slots 0 and 1 are reserved for SRP modules on ERX-7xx models; slots 6 and 7 are reserved for SRP modules on ERX-14xx models, the E120 router, and the E320 router. When you configure the Fast Ethernet interface on an SRP module, the output of the **show configuration** command always indicates that the interface is configured in the lower of the two slots (slot 0 or slot 6). This indication is true if you configure the interface on a redundant SRP module in the higher slot or even if you have only one SRP module and it is installed in the higher slot, as shown in the following example:

```
host1#show version
Juniper Edge Routing Switch ERX-700
Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
System Release: erx_7-1-0.rel Partial
        Version: 7.1.0 [BuildId 4518]   (December 21, 2005  11:23)
System running for: 25 days, 3 hours, 31 minutes, 5 seconds
        (since THU DEC 22 2005 11:36:41 UTC)

slot  state     type     admin  spare  running release    slot uptime
---- ------- ---------- ------- ----- ------------------ --------------
0    standby SRP-10Ge   enabled  ---  erx_7-1-0.rel           ---
1    online  SRP-10Ge   enabled  ---  erx_7-1-0.rel      25d03h:28m:49s
2      ---      ---       ---    ---         ---              ---
3      ---      ---       ---    ---         ---              ---
4    online  CT3-12     enabled  ---  erx_7-1-0.rel      25d03h:24m:46s
5    online  OC3-4A-APS enabled  ---  erx_7-1-0.rel      25d03h:24m:22s
6    online  GE         enabled  ---  erx_7-1-0.rel      25d03h:24m:44s

host1#configure terminal
Enter configuration commands, one per line.  End with ^Z.
host1(config)#interface fastethernet 0/0
host1(config-if)#ip address 10.6.130.83 255.255.128.0
host1(config-if)#exit
host1(config)#ip route 0.0.0.0 0.0.0.0 10.6.128.1
host1(config)#exit
host1#show config
! Configuration script being generated on TUE SEP 14 2004 13:22:06 UTC
! Juniper Edge Routing Switch ERX-700
! Version: 6.0.0 beta-1.8 [BuildId 2538] (September 7, 2004  12:46)
! Copyright (c) 1999-2004 Juniper Networks, Inc.  All rights reserved.
!
! Commands displayed are limited to those available at privilege level 10
```

```
!
boot config running-configuration
boot system erx_6-0-0b1-8.rel
no boot backup
no boot subsystem
no boot backup subsystem
no boot force-backup
!
! Note:  The following commands are here to ensure that all virtual routers
and
! vrfs are created before other commands that may need to reference them.
! These commands will be repeated further on as each virtual router and vrf
! has its configuration presented.
!
virtual-router default
virtual-router vr8
!
!
hostname "host1"
exception protocol ftp anonymous null
!
controller t3 2/0
[...]
!
interface fastEthernet 0/0
 ip address 10.6.130.83 255.255.128.0
!
ip route 0.0.0.0 0.0.0.0 10.6.128.1
! Trap Source: <not configured>
! Note: SNMP server not running.
!
```

Enabling Warm Restart Diagnostics on Modules

You can enable the system to perform diagnostic tests on SRP modules and line modules when the specified module is warm restarted. The system performs all the diagnostic tests that normally run when the module is cold started.

SRP modules on all E-series routers support warm restart diagnostics. Table 44 lists the line modules that support warm restart diagnostics.

Table 44: Supported Line Modules

Line Module
cOCx FO
CT3/T3-F0
OCx/STMx ATM
GE/FE
GE-2
GE-HDE
OC3/STM1 GE/FE
OC48
ES2 4G LM
ES2 10G Uplink LM

The number of diagnostic tests that the system performs on line modules depends on whether you have configured line module redundancy. If you enable warm restart diagnostics on the spare line module when all other line modules are active, the system performs diagnostic tests on the spare line module including the spare I/O module.

Enabling warm restart diagnostics on a primary line module forces the line module to switch over to the spare line module.

To ensure complete diagnostic test coverage, we recommend that you disable line module redundancy using the **redundancy lockout** command before enabling warm restart diagnostics.

Enabling Warm Restart Diagnostics

Use the **diag** command to enable warm restart diagnostics on a module.

diag

- Use to restart the specified SRP module or line module and enable the system to perform diagnostic tests on the module.
- Use the **force** keyword to enable the system to manually confirm conflicting conditions when the slot of the active SRP module is specified.
- If you specify a slot on the E120 router and the E320 router that contains an SRP module, you can use the *subsystem* variable to perform diagnostic tests on a subsystem on the SRP module. We recommend that you perform diagnostic tests on one subsystem at a time to avoid interrupting network traffic transmitting through the fabric modules.
  - Use the **srp** keyword to perform diagnostic tests on the SC subsystem that resides on a specified SRP module.
  - Use the **fabric** keyword to run diagnostic tests on the fabric slice that resides on the specified SRP module.
- Example 1—Enables warm restart diagnostics on a line module

  host1#**diag 3 force**

- Example 2—Enables warm restart diagnostics on the fabric subsystem of an active SRP module on the E320 router

  host1#**diag 6 fabric**

- There is no **no** version.

Monitoring Modules

Use the following commands to view information about all router modules.

show hardware

- Use to display information about SRP modules, line modules, and I/O modules in ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- Use to display information about the chassis, SRP modules, SFMs, line modules, IOAs, and the fan tray in the E120 router and the E320 router.
- Field descriptions
  - slot—Physical slot that contains the module
  - type—Kind of module or chassis and fan tray in the E120 and E320 routers; an “e” at the end of an SRP module type (for example, SRP-5Ge) indicates that the module includes error-checking code (ECC) memory.
  - serial number—Serial number of the module, chassis, or fan tray
  - assembly number—Part number of the module, chassis, or fan tray
  - assembly rev.—Hardware revision of the module, chassis, or fan tray
  - ram (MB)—Memory capacity of the host processor
  - number of MAC addresses—Total number of Ethernet addresses on an I/O module or an IOA
  - base MAC address—Lowest Ethernet address on an I/O module or an IOA
  - Tray—Number of the fan tray in the E120 and E320 routers; 0 indicates the primary fan
  - Major/Minor rev—Revision number of the module on the E120 and E320 routers
- Example 1—Displays the status of hardware on an ERX-7xx model

```
host1#show hardware
                                serial      assembly    assembly   ram
slot        type                number       number       rev.     (MB)
----   ----------------   ----------   ----------   --------   ----
0      SRP-10Ge           4305358981   3500005472     A06      2048
1      SRP-10Ge           4305359020   3500005472     A06      2048
2            ---             ---          ---         ---      ---
3            ---             ---          ---         ---      ---
4      CT3-12             4305337201   3500010901     A07      128
5      OC3/OC12/DS3-ATM   4605300290   3500103958     A06      256
6      GE/FE              4605340294   3500104554     A08      256

                                                                number
                                                                  of
                          serial      assembly    assembly       MAC
slot       type           number       number       rev.     addresses
----   -------------   ----------   ----------   --------   ---------
0          ---             ---          ---         ---        ---
1      SRP-10Ge I/O    4605250426   3500003302     A02          1
2          ---             ---          ---         ---        ---
3          ---             ---          ---         ---        ---
4      CT3/T3-12 I/O   4305316605   3500010801     A02
5      OC3(8)-MM I/O   4304443600   4500001501     A03          4
6      GE-SFP I/O      4605310064   4500002001     A05          1
```

```
           base
slot    MAC address
----   --------------
0           ---
1      0090.1aa0.577a
2           ---
3           ---
4
5      0090.1a41.7c68
6      0090.1aa0.6216
```

- Example 2—Displays the status of hardware on the E320 router

```
host1#show hardware
```

```
                        Chassis
                        -------
           serial      assembly    assembly   Major/Minor
 type       number      number       rev.         rev
-------   ----------   ----------   --------   -----------
Chassis   5504200687   4400006402      01         0.101

                              Modules
                              -------
                  serial      assembly    assembly   ram    Major/Min
slot    type       number      number       rev.     (MB)      rev
----   -------   ----------   ----------   --------   ----   ---------
0        ---        ---          ---          ---      ---       ---
1        ---        ---          ---          ---      ---       ---
2      LM-4      4303470363   4500006301      01      256       1.101
3        ---        ---          ---          ---      ---       ---
4        ---        ---          ---          ---      ---       ---
5        ---        ---          ---          ---      ---       ---
6        ---        ---          ---          ---      ---       ---
6        ---        ---          ---          ---      ---       ---
7      SRP-100   4304218323   4500006601      03      1024      1.103
7      SFM-100   4304218323   4500006601      03      ---       1.103
8      SFM-100   4304206756   4500006701      04      ---       1.104
9      SFM-100   4304206762   4500006701      04      ---       1.104
10     SFM-100   4304206737   4500006701      04      ---       1.104
11       ---        ---          ---          ---      ---       ---
12       ---        ---          ---          ---      ---       ---
13       ---        ---          ---          ---      ---       ---
14       ---        ---          ---          ---      ---       ---
15       ---        ---          ---          ---      ---       ---
16       ---        ---          ---          ---      ---       ---

                            Adapters
                            --------
                                                              number
                                                                of
                  serial      assembly    assembly      MAC
slot    type       number      number       rev.     addresses
----   --------   ----------   ----------   --------   ---------
0/0      ---        ---          ---          ---        ---
0/1      ---        ---          ---          ---        ---
1/0      ---        ---          ---          ---        ---
1/1      ---        ---          ---          ---        ---
2/0    GE-4 IOA   4304020462   4500006800      11         4
2/1      ---        ---          ---          ---        ---
3/0      ---        ---          ---          ---        ---
3/1      ---        ---          ---          ---        ---
4/0      ---        ---          ---          ---        ---
```

```
4/1      ---          ---           ---          ---          ---
5/0      ---          ---           ---          ---          ---
5/1      ---          ---           ---          ---          ---
7/0    SRP IOA    4303470366   4500006500      02           2
11/0     ---          ---           ---          ---          ---
11/1     ---          ---           ---          ---          ---
12/0     ---          ---           ---          ---          ---
12/1     ---          ---           ---          ---          ---
13/0     ---          ---           ---          ---          ---
13/1     ---          ---           ---          ---          ---
14/0     ---          ---           ---          ---          ---
14/1     ---          ---           ---          ---          ---
15/0     ---          ---           ---          ---          ---
15/1     ---          ---           ---          ---          ---
16/0     ---          ---           ---          ---          ---
16/1     ---          ---           ---          ---          ---
            base        Major/Minor
slot    MAC address         rev
----   --------------   -----------
0/0         ---             ---
0/1         ---             ---
1/0         ---             ---
1/1         ---             ---
2/0    0090.1a00.17ec      1.111
2/1         ---             ---
3/0         ---             ---
3/1         ---             ---
4/0         ---             ---
4/1         ---             ---
5/0         ---             ---
5/1         ---             ---
7/0    0090.1a00.17ae      1.102
11/0        ---             ---
11/1        ---             ---
12/0        ---             ---
12/1        ---             ---
13/0        ---             ---
13/1        ---             ---
14/0        ---             ---
14/1        ---             ---
15/0        ---             ---
15/1        ---             ---
16/0        ---             ---
16/1        ---             ---

                              Fan(s)
                              ------
                      serial      assembly    assembly   Major/Minor
Tray      type        number       number      rev.         rev
----   -----------   ----------   ----------   --------   -----------
0      Primary FAN   4303370009   4400007000      01         1.101
---        ---          ---          ---         ---          ---
```

- Example 3—Displays the status of hardware on the E120 router

```
host1#show hardware
                          Chassis
                          -------
            serial      assembly    assembly   Major/Minor
 type       number       number      rev.         rev
-------   ----------   ----------   --------   -----------
Chassis   4307018011   4580002602      01         0.101
```

```
                                    Modules
                                    -------
                    serial        assembly     assembly    ram     Major/Minor
slot    type        number        number       rev.        (MB)        rev
----    --------    ----------    ----------   --------    ----    -----------
0         ---         ---           ---          ---       ---         ---
1       LM-10       4306493492    4500009501     08        1024       1.108
2       LM-10       4306493502    4500009501     08        1024       1.108
3         ---         ---           ---          ---       ---         ---
4         ---         ---           ---          ---       ---         ---
5         ---         ---           ---          ---       ---         ---
6       SRP-120     4306483377    4501008401     02        4096       1.102
6       SFM-120     4306483377    4501008401     02        ---        1.102
7       SRP-120     4306483378    4501008401     02        4096       1.102
7       SFM-120     4306483378    4501008401     02        ---        1.102
8       SFM-120     4306493692    4501008501     02        ---        1.102
9       SFM-120     4306493725    4501008501     02        ---        1.102
10      SFM-120     4306493734    4501008501     02        ---        1.102

                                   Adapters
                                   --------
                                                                    number
                                                                      of
                    serial        assembly     assembly              MAC
slot    type        number        number       rev.                addresses
----    --------    ----------    ----------   --------            ---------
0/0       ---         ---           ---          ---                 ---
0/1       ---         ---           ---          ---                 ---
1/0       ---         ---           ---          ---                 ---
1/1     GE-8 IOA    4306472048    4500009102     A04                  8
2/0       ---         ---           ---          ---                 ---
2/1     GE-8 IOA    4306362247    4500009102     A03                  8
3/0       ---         ---           ---          ---                 ---
3/1       ---         ---           ---          ---                 ---
4/0       ---         ---           ---          ---                 ---
4/1       ---         ---           ---          ---                 ---
5/0       ---         ---           ---          ---                 ---
5/1       ---         ---           ---          ---                 ---
6/0     SRP IOA     4306483232    4501006502     A00                  2
          base          Major/Minor
slot    MAC address         rev
----    --------------    -----------
0/0         ---               ---
0/1         ---               ---
1/0         ---               ---
1/1     0090.1a42.7327        2.4
2/0         ---               ---
2/1     0090.1a42.5223        2.3
3/0         ---               ---
3/1         ---               ---
4/0         ---               ---
4/1         ---               ---
5/0         ---               ---
5/1         ---               ---
6/0     0090.1a42.76c4        2.0

                                     Fan(s)
                                     ------
                      serial        assembly     assembly    Major/Minor
Tray      type        number        number       rev.            rev
----    -----------   ----------    ----------   --------    -----------
0       Primary FAN   4306505285    4400010001     01          1.101
```

show utilization

- Use to display information about the resources that modules consume.
- When you issue this command, the router releases available memory on the SRP module immediately; however, the display appears a few seconds later.
- To display detailed information about the average CPU utilization percentage calculated over 5-second, 1-minute, and 5-minute intervals for each module installed in the router, use the **detail** keyword.
- Field descriptions
  - slot—Slot in which the module resides
  - type—Type of module
  - heap (%)—Percentage of the RAM that is currently in use by software running on the module
  - cpu (%)—Percentage of the module CPU capacity currently used; this field appears only when the **detail** keyword is omitted
  - bw exceed—Status of bandwidth oversubscription for this slot; this field appears only when bandwidth oversubscription is configured
    - Y indicates that this slot is in an oversubscribed slot group
    - --- indicates that no module is installed or slot has no bandwidth oversubscription
  - The following additional fields appear when the **detail** keyword is used:
    - last available cpu (%)—Average CPU utilization percentage for each installed module during the last 5-second interval for which data was available. If the current CPU utilization data for a module is *not* available at any point, the last available cpu (%) field displays the last available 5-second CPU utilization percentage, which is the same value that appears in the cpu (%) field when the **detail** keyword is omitted. If the current 5-second CPU utilization data is available, the last available cpu (%) field and the 5 sec cpu (%) field display the same value.
    - 5 sec cpu (%)—Average CPU utilization percentage for each installed module during the most recent 5-second interval
    - 1 min cpu (%)—Average CPU utilization percentage for each installed module during the most recent 1-minute interval
    - 5 min cpu (%)—Average CPU utilization percentage for each installed module during the most recent 5-minute interval
  - Depending on the output of the **show utilization** command when you use the **detail** keyword, some or all of the following symbols and explanatory notes might appear:
    - --- indicates an empty slot on ERX-7xx models, ERX-14xx models, or the ERX-310 router. For the E120 and E320 routers, this symbol indicates either an empty slot, or a fabric slice that resides on an SRP module or on a switch fabric module (SFM).
    - ??? indicates that the current CPU utilization data is unavailable for the specified interval. Data might be unavailable for one or more of the following reasons:

- A slot is in an inactive state.
- A line module is very busy (that is, using 100 percent of its CPU capacity) and is unable to send its CPU utilization data to the SRP module.
- A line module is experiencing communication problems that prevent it from sending its CPU utilization data to the SRP module.

- *** indicates that a module installed in the slot is running an incompatible version of JUNOSe software.

- Example 1—Displays basic information about the resources consumed on the router

```
host1#show utilization
Please wait....
        System Resource Utilization
        ---------------------------
                      heap   cpu     bw
slot       type       (%)    (%)   exceed
----   ------------   ----   ---   ------
0          ---        ---    ---    ---
1      OC12Atm(P2)     59    44      Y
2      OC3/OC12-ATM    67    53      Y
3          ---        ---    ---    ---
4          ---        ---    ---    ---
5      OC3d            79     0     ---
6      SRP-10G         27     1     ---
7          ---        ---    ---    ---
8          ---        ---    ---    ---
9          ---        ---    ---    ---
10         ---        ---    ---    ---
11         ---        ---    ---    ---
12         ---        ---    ---    ---
13         ---        ---    ---    ---
```

- Example 2—Displays detailed information about the average CPU utilization percentage calculated over 5-second, 1-minute, and 5-minute intervals for each module installed in an ERX-7xx model, ERX-14xx model, or ERX-310 router

  In this example, slot 12 is empty (as indicated by the --- symbol), the CPU utilization for the FE-8 module installed in slot 10 is unavailable (as indicated by the ??? symbol), and the SRP module installed in slot 7 is running an incompatible version of JUNOSe software (as indicated by the *** symbol).

```
host1#show utilization detail
Please wait...
                  System Resource Utilization
                  ---------------------------
                                                    5      1      5
                            last                   sec    min    min
                   heap   available      bw       cpu    cpu    cpu
slot      type     (%)     cpu (%)     exceed    (%)    (%)    (%)
----   ----------  ----   ---------   ------   ---    ---    ---
0      OC3-4A       63      76          ---     76     70     71
1      COC3/COC12   11       2          ---      2      4      3
2      COC3-4       39      11          ---     11     17     20
3      OC3-4A       58      61          ---    ???    ???     68
4      OC3-4A       88     100          ---    100     96     92
5      OC3-4A       94     100          ---    100     93     87
```

```
6       SRP-40G+       11       84          ---      84      85     73
7       SRP-40G+       18       29          ---     ***     ***    ***
8       OC3-4P         25       20          ---      20      17     22
9       FE-8           61       48          ---      48      53     47
10      FE-8          ???      ???          ---     ???     ???    ???
11      CT3-12         11        2          ---       2       4     10
12        ---         ---      ---          ---     ---     ---    ---
13      CT3-12         32       16          ---      16      12     16

Note: '---' indicates empty slots.
      '???' indicates data not available.
      '***' indicates board running incompatible version of software.
```

- Example 3—Displays detailed information about the average CPU utilization percentage calculated over 5-second, 1-minute, and 5-minute intervals for each module installed in an E320 router.

  In this example, slots 3, 5, 12, 14, and 16 are empty (as indicated by the *---* symbol), fabric slices are present on the SFM-100 modules in slots 8, 9, and 10 (also indicated by the *---* symbol), the CPU utilization for the LM-4 module installed in slot 1 is unavailable (as indicated by the ??? symbol), and the SRP-100 module installed in slot 7 is running an incompatible version of JUNOSe software (as indicated by the *** symbol).

```
host1#show utilization detail
Please wait...
                  System Resource Utilization
                  ---------------------------

                                                      5     1     5
                                 last                sec   min   min
                    heap      available      bw      cpu   cpu   cpu
slot      type      (%)        cpu (%)     exceed    (%)   (%)   (%)
----   ----------   ----    ----------    ------    ---   ---   ---
0       LM-4         9          1           ---      1     1     1
1       LM-4        ???        ???          ---     ???   ???   ???
2       LM-4         23         3           ---     ???    4     8
3         ---       ---        ---          ---     ---   ---   ---
4       LM-4         60         1           ---      1     1     1
5         ---       ---        ---          ---     ---   ---   ---
6       SRP-100      15         3           ---      3     2     3
7       SRP-100      10         1           ---     ***   ***   ***
8       SFM-100     ---        ---          ---     ---   ---   ---
9       SFM-100     ---        ---          ---     ---   ---   ---
10      SFM-100     ---        ---          ---     ---   ---   ---
11      LM-4         60         1           ---      1     1     1
12        ---       ---        ---          ---     ---   ---   ---
13      LM-4         68         3           ---      3     3     3
14        ---       ---        ---          ---     ---   ---   ---
15      LM-4         66         1           ---      1     1     1
16        ---       ---        ---          ---     ---   ---   ---
  Note: '---' indicates empty slots or fabric Slices.
        '???' indicates data not available.
        '***' indicates board running incompatible version of software.
```

Chapter 7

Managing High Availability

This chapter describes how to manage Juniper Networks high availability (HA) software features for the E-series router. Use this chapter with *Chapter 6, Managing Modules* to fully manage the SRP and high availability features.

This chapter contains the following sections:

- Understanding High Availability on page 377
- Platform Considerations on page 378
- Redundancy Modes of Operation on page 379
- Understanding SRP State Behavior on page 381
- Application Support on page 384
- Before Activating High Availability on page 389
- Activating High Availability on page 389
- Deactivating High Availability on page 390
- Upgrading Software on page 391
- Monitoring High Availability on page 391

Understanding High Availability

High availability is the idea of reducing or eliminating single points of failure. When applied to the E-series router, high availability provides both hardware-specific and software-specific methods to ensure minimal downtime and ultimately improve the performance of your network.

For hardware components, Juniper Networks provides redundancy solutions to ensure that the router continues to operate in the event of a hardware fault. This redundancy can exist on various router models in the form of multiple power supplies, cooling fans, switching planes, routing engines and, in some cases, interfaces. Redundancy also allows for hot-swapping various components within your Juniper Networks router.

NOTE: For information about E-series hardware redundancy features, see the *ERX Hardware Guide* or the *E120 and E320 Hardware Guide*.

Platform Considerations

High availability is supported on all E-series routers except for the ERX-310 router.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models and ERX-14xx models.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Module Requirements

The following table lists which SRPs support or do not support the high availability mode (stateful SRP switchover) feature.

SRP Model	Supported
SRP-5G	No
SRP-5G+	Yes
SRP-10G	Yes
SRP-40G	No
SRP-40G PLUS	Yes
SRP-100	Yes

NOTE: High availability requires two SRP modules with 1 GB of memory or more.

Redundancy Modes of Operation

The switch route processor (SRP) modules can operate in one of two redundancy modes—file system synchronization and high availability.

File System Synchronization Mode

File system synchronization is the default behavior mode for E-series routers that contain redundant SRPs. Available only to SRP modules, this mode has been available since the 2.x release. In this mode:

- Files and data (for example, configuration files and releases) in nonvolatile storage (NVS) remain synchronized between the primary and standby SRP modules.
- SRP modules will reload all line modules and restart from saved configuration files.
- If the active SRP module switches over to the standby SRP, the router cold-restarts as follows:
  - All line modules are reloaded.
  - User connections are lost, and forwarding through the chassis stops until the router SRP module recovers.
  - The standby SRP module boots from the last known good configuration from NVS.

For additional information about the default SRP functionality, see *Chapter 6, Managing Modules*.

High Availability Mode

Currently applicable to the SRP module, the Juniper Networks high availability mode uses an initial bulk file transfer and subsequent, transaction-based mirroring to ensure rapid SRP module recovery after a switchover. This process is referred to in this chapter as *stateful SRP switchover*.

In addition to keeping the contents of NVS, high availability mode keeps state and dynamic configuration data from the SRP memory synchronized between the primary and standby SRP modules.

When stateful SRP switchover is enabled, an SRP switchover keeps line modules up and forwarding data, and the newly active SRP module continues from the point of switchover.

By using transaction-based mirroring instead of file synchronization, high availability mode keeps the standby SRP module synchronized with the active SRP module. Mirroring occurs from memory on the active SRP module to memory on the standby SRP module by way of transactions. When a transaction is committed on the active SRP module, the data associated with the transaction is sent to the standby SRP module.

In high availability mode:

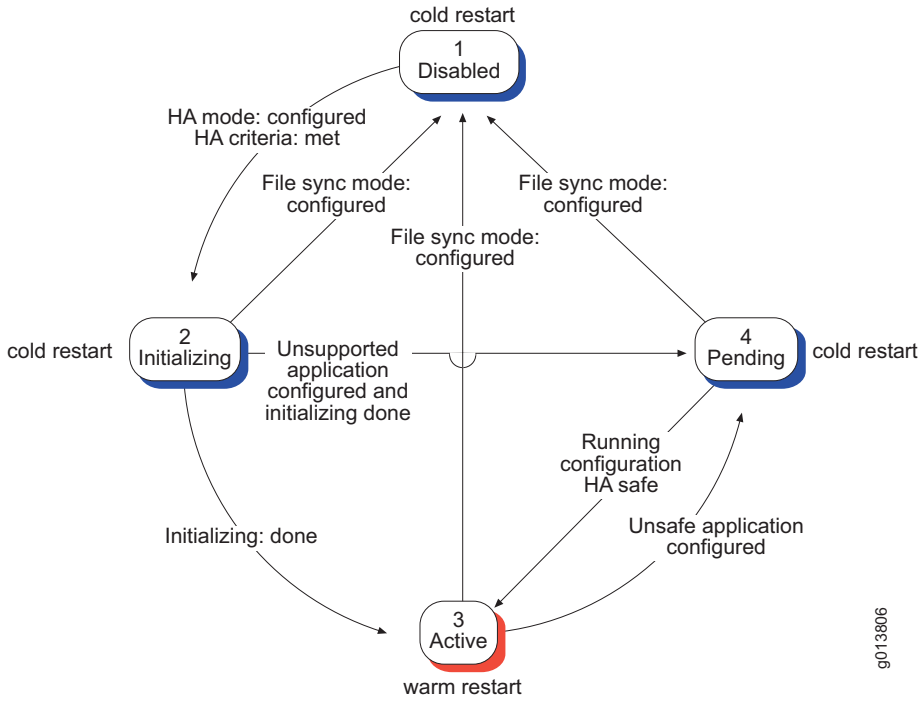
- The contents of the NVS in the primary and standby SRP modules remain synchronized.
- If a switchover occurs:
  - The standby SRP module warm-restarts using the mirrored data to restore itself to the state of the system before the switchover.
  - During the warm restart:
    - User connections remain active, and forwarding continues through the chassis.
    - New user connection attempts during switchover are denied until switchover is complete.
    - New configuration changes are prevented until switchover is complete (or after 5 minutes).

NOTE: If the switchover does not finish within 5 minutes, the SRP module cancels the operation and reenables CLI configuration.

Understanding SRP State Behavior

The SRP progresses through various high availability states. These states are illustrated in Figure 27.

Figure 27: High Availability States



Disabled State

The initial, default state for high availability mode is disabled. While in this state, the router continues to use file system synchronization. If a switchover occurs while the router is in this state, the standby SRP module performs a cold restart.

The router enters this state when you power up the router or when the router warm-restarts from an SRP switchover.

Once you enable high availability, the system must meet the following criteria before it can enter the initializing state:

- High availability mode is configured.
- Active SRP hardware supports high availability.
- Network core dump feature is disabled.
- Running configuration will allow high availability to operate (that is, no unsupported applications are configured).
- Standby SRP hardware supports high availability.

- Standby SRP module is online and capable of mirroring.
- Standby SRP module is running the same release.

During the disabled state:

- If any one criterion is not met, the system remains in the disabled state, until the criterion is met.
- If a switchover occurs while the system is in the disabled state, the system cold-restarts.

While in the disabled state, the system operates as if it were configured for file system synchronization (for example, NVS is synchronized every 5 minutes, if autosynchronization is enabled).

If all criteria are met, high availability mode transitions to the initialization state.

Initializing State

After the SRP module transitions into the initializing state, bulk synchronization of the memory and NVS occurs. This includes the following:

- File synchronization of the primary NVS with the standby NVS
- Mirroring of appropriate state and dynamic configuration information from the active SRP (memory) to the standby SRP (memory)

NOTE: Depending on the size of the configuration, this process can take several minutes.

During the initializing state:

- If an unsupported application is configured during initialization, the system completes initializing and enters the pending state.
- If any other criterion becomes false (or is no longer met), the system enters the disabled state.
- If a switchover occurs while the system is in this state, the system cold-restarts.

Once initialization is completed, the system enters the active state.

Active State

During the active state, the data that was synchronized from the active SRP module to the standby SRP module during initialization remains synchronized through mirroring updates.

Mirroring updates occur as follows:

1. When making changes or updates, applications create individual transactions, perform the updates on the active SRP module, and post the transactions.

2. Following the updates, the active SRP module sends the changes to the standby SRP module.

3. The standby SRP module replays the updates (in the order in which they were committed on the active SRP module) and makes the appropriate changes for each changed application.

4. Updates that need to be stored in NVS (that is, for static configurations) are updated in NVS.

NOTE: While in the active and pending states, the CLI **synchronize** command does not update configuration files; these files are updated by the mirroring process.

During the active state:

- If a switchover occurs while the router is in the active state, the standby SRP module performs a warm restart (that is, stateful SRP switchover is in effect); the standby SRP module uses the configuration located in NVS.

- If an unsupported application is configured, the system transitions to the pending state.

- If any other criterion changes (is no longer met), the system transitions to the disabled state.

NOTE: Changes made in manual commit mode are maintained, uncommitted, in the standby SRP memory until a trigger to commit occurs; if a switchover occurs while in this mode, the standby SRP module uses the configuration in memory.

Pending State

The system transitions to the pending state if an unsupported application is configured. When a transition to the pending state occurs, the system generates SNMP traps and log messages.

How the router behaves depends on which HA state the application is in when it shifts to a pending state:

- From disabled state—The router remains in the disabled state.
- From initializing state—The router completes the initializing state and transitions to the pending state after initialization is complete.
- Active State—The router transitions to the pending state.

The system remains in the pending state until the configuration of the unsupported application is removed. However, even though it is in the pending state, the system continues mirroring updates from the primary SRP module to the standby SRP module.

NOTE: You can use the **show redundancy srp** command to display the name of any unsupported applications that are configured.

If a switchover occurs while the system is in the pending state, the system cold-restarts.

Application Support

Applications are either supported or unsupported by high availability.

- Supported—You can configure supported applications without having any adverse impact to high availability. When a switchover occurs, supported applications can react to switchovers in one of two different ways:
  - Gracefully recover using mirrored static and dynamic information (for example, IP, PPP, and PPPoE)
  - Recover using static configuration only; that is, no runtime state is restored after a switchover. Dynamic configuration and state information are lost. (For example, CLI sessions are restarted, telnet sessions are dropped, multicast routes must be rebuilt, and so on.)
- Unsupported—We recommend that you not configure unsupported applications on a chassis running in high availability mode. Although configured unsupported applications suspend high availability or prevent high availability from becoming active, they do not cause any problems with the function of the router.

Table 45 indicates which applications support or do not support stateful SRP switchover.

Table 45: Application Support for Stateful SRP Switchover

Application	Supported	Unsupported	Notes
Physical Layer Protocols			
DS1	✔	–	–
DS3	✔	–	–
HDLC	✔	–	–
SONET/SDH	✔	–	–
SONET/SDH VT	✔	–	–
Link-Layer Protocols			
ATM	✔	–	Static and dynamic interfaces, with the exception of ATM subscribers, are supported. In this case, *ATM subscribers* refers to a technology on the E-series router where the ATM layer does authentication (that is, not PPP or IP subscriber manager).
ATM 1483 bulk configuration of dynamic interfaces	✔	–	–
Bridged Ethernet	✔	–	–
Cisco HDLC	✔	–	–
Ethernet (with and without VLANs)	✔	–	–
Frame Relay	✔	–	–
PPP	✔	–	–
PPPoE	✔	–	–
Transparent bridging	✔	–	–
Unicast Routing			
Access Routes	✔	–	–
BGP	✔	–	Supported only when the graceful restart extension is enabled.
FTP	✔	–	Static recovery support only.
IP	✔	–	–
IPv6	–	✔	–
IPSec Transport	–	✔	–
IPSec Tunnels	✔	–	Completed IKE phase 1 and phase 2 negotiations supported only.
IS-IS	✔	–	Supported only when the graceful restart extension is enabled.

Table 45: Application Support for Stateful SRP Switchover (continued)

Application	Supported	Unsupported	Notes
OSPF	✔	–	Supported only when the graceful restart extension is enabled.
RIP	✔	–	Static recovery support only.
Static Routes	✔	–	–
Telnet	✔	–	Static recovery support only.
IPv4 Multicast Routing			
Multicast Routing	✔	–	Static recovery support only. During switchover, the system mirrors the multicast queue so that IP can use the same queue without needing to recreate a different connection.
DVMRP	✔	–	Static recovery support only. DVMRP gives the restart complete indication to the IP routing table after getting a peer update (60-second time-out).
IGMP	✔	–	IC IGMP deletes its interface and membership state on SRP failover (controller down). As part of SRP warm start, IGMP interfaces are reconfigured from NVS and dynamic IGMP interfaces are reconfigured from mirrored storage. IGMP hosts are queried as IP interfaces come back up, the join state is re-established, and SC IGMP state is created. After the maximum query response time (across all interfaces) expires to allow hosts to re-establish join state, IGMP notifies MGTM that graceful restart is complete.
PIM	✔	–	Static recovery support only. For warm start, PIM interfaces are reconfigured from NVS and a Hello message with a new Generation ID is issued as IP interfaces come up. A neighbor that receives this Hello determines that the upstream neighbor has lost state and needs to be refreshed. A VR-global configurable graceful restart timer is required for PIM to time out the re-establishment of the join state for sparse-mode interfaces. After this timer expires, PIM notifies MGTM that graceful restart is complete.
IPv6 Multicast Routing			No multicast routing state information remains following a switchover. Incremental support for multicast routing is planned for future releases.
Multicast Routing	–	✔	–
MLD	–	✔	–
PIM	–	✔	–

Table 45: Application Support for Stateful SRP Switchover (continued)

Application	Supported	Unsupported	Notes
Multiprotocol Label Switching			
MPLS	✔	–	MPLS is HA-unsafe during a graceful restart. It is HA-unsafe until all the configured MPLS signaling protocols have completed their graceful restart procedures and any stale forwarding elements have been flushed from the line modules. If you force an SRP switchover while MPLS is HA-unsafe, the SRP module switches but the SRP module and the line modules undergo a cold restart. If the primary SRP module resets while MPLS is HA-unsafe, the router undergoes a cold restart.
BGP signaling	✔	–	
LDP signaling	✔	–	To provide uninterrupted service during an SRP switchover in a scaled configuration, such as one with 32,000 Martini circuits, set the LDP graceful restart reconnect time to the maximum 300 seconds and set the LDP graceful restart recovery timer to the maximum 600 seconds. This requirement is true for all SRP switchovers, including those in the context of a unified in-service software upgrade.
RSVP signaling	✔	–	
Local cross-connects between layer 2 interfaces using MPLS	✔	–	–
Policies and QoS			
Policies	✔	–	–
QoS	✔	–	Static recovery support only.
Remote Access			
AAA	✔	–	–
DHCP External Server and Packet Trigger	✔	–	Following a switchover, the DHCP lease (that is, time remaining) is recalculated based on when the lease started. When the release timer for a client expires, the client is deleted and the access route is removed, along with the dynamic subscriber interface if it was created. If the client requests a new lease, DHCP external server resynchronizes with the new lease time.
DHCP Packet Capture	✔	–	–

Table 45: Application Support for Stateful SRP Switchover (continued)

Application	Supported	Unsupported	Notes
DHCP Proxy Client	–	✔	–
DHCP Relay Proxy	–	✔	–
DHCP Relay Server	✔	–	Before HA support, clients identified by the DHCP relay server were maintained on a switchover (their state was stored to NVS); DHCP relay server always had some level of HA support. Currently, following a switchover, the DHCP lease (that is, time remaining) is reset. When the release timer for a client expires, the client requests a new lease. The E-series router DHCP relay server then synchronizes with the new state.
DHCPv4 Local Server	✔	–	–
DHCPv6 Local Server	–	✔	HA does not support IPv6.
L2TP	✔	–	
L2TP Dialout	–	✔	–
Local Address Pools	✔	–	The internal local address server state supports only static recovery. However, the AAA application reallocates active addresses on a switchover. The resulting effect is the local address server having full HA support.
RADIUS Client	✔	–	Similar to local address server, AAA recovers disrupted RADIUS communication on a switchover. The resulting effect is the RADIUS client having full HA support.
RADIUS Dynamic-Request Server	✔	–	Static recovery support only.
RADIUS Initiated Disconnect	✔	–	–
RADIUS Relay Server	✔	–	–
RADIUS Route-Download Server	✔	–	–
SRC Client	✔	–	–
TACACS+	✔	–	Static recovery support only.
Miscellaneous			
Firewall	✔	–	–
J-Flow (IP flow statistics)	✔	–	–
Line Module Redundancy	✔	–	–

Table 45: Application Support for Stateful SRP Switchover (continued)

Application	Supported	Unsupported	Notes
Network Address Translation	✔	–	–
NTP	✔	–	–
Resource Threshold Monitor	✔	–	–
Response Time Reporter	✔	–	–
Route Policy	✔	–	Static recovery support only.
Subscriber Interfaces	✔	–	–
Tunnels (GRE and DVMRP)	✔	–	–
VRRP	✔	–	Static recovery support only.

CAUTION: When IP tunnels are configured on an HA-enabled router and the Service Module (SM) carrying these tunnels is reloaded, HA transitions to the pending state. HA remains in the pending state for 5 minutes after the successful reloading of the SM. This amount of time allows for IP tunnel relocation and for the tunnels to become operational again on the SM. If an SRP switchover occurs while HA is in the pending state, the router performs a cold restart.

Before Activating High Availability

Before you activate high availability on the SRP modules, review *Chapter 6, Managing Modules* and any high availability–related changes to SRP management commands.

Activating High Availability

You activate high availability (stateful SRP switchover) by launching Redundancy Configuration mode and issuing the **mode high-availability** command.

When activating high availability, keep the following in mind:

- In an E-series router that supports stateful SRP switchover, both SRP modules must be running the same software release version in order to activate high availability mode.
- If high availability mode cannot become active because of different releases on the active and standby SRP modules, the system reverts to its default mode (file system synchronization).

- When active or pending, the router configuration files are mirrored from the active SRP module to the standby SRP module. All other files shared between the active and standby SRP modules are automatically synchronized using legacy synchronization methods.

To enable high availability, enter the following:

```
host1(config)#redundancy
host1(config-redundancy)#mode high-availability
```

mode

- Use the redundancy **mode** command to enable high availability.
- The **high-availability** keyword enables high availability mode for stateful SRP switchover. In this mode, the router uses mirroring to keep the configuration and state of the standby SRP module coordinated with the configuration and state of the active SRP module.

NOTE: High availability mode is currently available only on ERX-1440, ERX-1400, and ERX-700 routers that support dual SRPs.

- The **file-system-synchronization** keyword reverts the redundancy mode to its default. In this mode, the router uses file synchronization to keep the configuration of the standby SRP module coordinated with the configuration of the active SRP module.
- Example

  ```
  host1(config-redundancy)#mode high-availability
  ```

- Use the **no** version to return high availability mode operation to its default (file system synchronization).

redundancy

- Use to enter Redundancy Configuration mode.
- Example

  ```
  host1(config)#redundancy
  host1(config-redundancy)#
  ```

- There is no **no** version.

Deactivating High Availability

To deactivate high availability support, enter the following:

```
host1(config)#redundancy
host1(config-redundancy)#mode file-system-synchronization
```

or

```
host1(config)#redundancy
host1(config-redundancy)#no mode
```

Upgrading Software

As already mentioned, you cannot activate high availability when a different release of software is running on the standby SRP module. The router determines whether a release is the same by viewing the build date, the release file name, and the internal version number for the software on each SRP module.

The most efficient way to upgrade the software is to ensure that the standby SRP module is armed with the new release and then reload the standby SRP module. This reload occurs automatically after you download and arm a new release onto the active SRP module and the active SRP module subsequently synchronizes with the standby SRP module.

After reloading, and even though high availability mode is configured, the active SRP module reverts to using the file-system-synchronization operational mode for synchronizing updates. To complete the upgrade and place the system back in high-availability operational mode, you must execute the **srp switch** command to force the standby SRP module to take over as the active SRP module.

NOTE: Executing the **srp switch** command results in a cold restart of the router.

Once the switchover is initiated, the formerly active SRP module reloads the software and starts running the same release as the newly active SRP module. When the formerly active SRP module becomes operational as the standby SRP module, the newly active SRP module detects that the release it is running is the same as that on the standby SRP module and allows the originally active SRP module to resume the high-availability operational mode.

If a fault occurs when the active SRP module is in file-system-synchronization operational mode, the standby SRP module detects the fault and takes over, and the router cold-restarts. For this reason, it is important that you arm the new release only when you can accept the resulting window of vulnerability where high availability is disabled (that is, until the active and standby SRP modules are again running the same release).

Monitoring High Availability

This section shows how to use the **show** commands to view your high availability configuration and how to clear the high availability switchover history for the router.

High Availability show Commands

You can monitor various aspects of high availability using **show** commands. These aspects include redundancy modes and status, redundancy clients, historical information about redundancy on the router, and specific redundancy information for line modules and SRPs.

show redundancy

- Use to display the supported redundancy modes and other status relating to high availability. In particular, the output indicates any conditions that are preventing high availability from operating.
- Field descriptions
  - SRP
    - high-availability state—State of the high availability mode (disabled, active, or pending)
    - current redundancy mode—Redundancy mode currently being used by this router (high-availability or file-system-synchronization)
    - last activation type—Last type of activation that occurred on this router (that is, the method by which the SRP last booted [cold-start or warm-start])
  - Criteria Required for High Availability to be Active—criteria required for high availability to be active.

NOTE: All criteria must be “yes” for high availability to be active.

  - Line Card
    - automatic reverting—State of automatic reverting (on or off)
    - slot(s)—Slots in which the line modules reside
    - hardware role—Function of the line module: primary or spare
    - lockout config—Status of redundancy on this line module (protected—line module redundancy is enabled; locked out—line module redundancy is disabled)
    - backed up by slot—Slot that contains the line module that is a spare for this primary line module
    - sparing for slot—Slot that contains the primary line module for which this line module is a spare
    - revert at—Time at which you want line module to revert
    - midplane type—Identifier for the type of midplane
    - midplane rev—Hardware revision number of the redundancy midplane
    - fabric slice redundancy—Status of the fabric slice on the SRP modules or SFMs on the E120 and E320 routers
    - slot—Slot in which the fabric slice resides
    - slice state—State of the fabric slice (online, not present)
    - type—Identifier for the type of hardware (SRP module or SFM)

- Example 1—Displays a summary of the redundancy status of an ERX-14xx model

```
host1#show redundancy

SRP
---

high-availability state:  disabled
current redundancy mode:  high-availability
last activation type:     cold-switch

Criteria Preventing High Availability from being Active
-------------------------------------------------------
                  criterion                      met
-------------------------------------------------   ---
Standby SRP is online and capable of mirroring?   No

Line Card
---------

automatic reverting is off

                             backed
                               up     sparing
       hardware    lockout      by       for     revert
slot     role      config      slot     slot       at
----   --------   ---------   ------   -------   ------
 3       ---         ---       ---       ---      ---
 8      spare        ---       ---       ---      ---
 12    primary    protected    ---       ---      ---

         midplane   midplane
slots      type       rev
------   --------   --------
8 - 13      6          0
```

- Example 2—Displays the redundancy status of an ERX-14xx model in detail

```
host1#show redundancy detail

SRP
---

high-availability state:  disabled
current redundancy mode:  file-system-synchronization
last activation type:     cold-start

   Criteria Required for High Availability to be Active
   ----------------------------------------------------
                     criterion                        met
-----------------------------------------------------   ---
Active SRP hardware supports High Availability?        Yes
High Availability mode configured?                     No
Mirroring Subsystem present?                           Yes
Mirroring activity levels within limits?               Yes
Network Core Dumps disabled?                           Yes
Running configuration is safe for High Availability?   Yes
Standby SRP hardware supports High Availability?       Yes
Standby SRP is online and capable of mirroring?        Yes
Standby SRP is running the same release?               Yes
```

```
Line Card
---------

automatic reverting is off

                                backed
                                  up     sparing
       hardware    lockout       by       for     revert
slot     role      config       slot     slot       at
----   --------   ---------   ------   -------   ------
 3       ---         ---       ---       ---      ---
 8      spare        ---       ---       ---      ---
 12    primary    protected     ---       ---      ---

         midplane   midplane
slots      type       rev
------   --------   --------
8 - 13      6          0
```

show redundancy clients

- Use to display high availability clients and their various levels of high availability support.
- Specify an optional client type that you want to view (all, supported, unsafe, unsupported)

NOTE: Issuing this command without the optional client type results in showing only unsupported high availability clients (the default).

- Field descriptions
  - client—High availability client
  - mode—Whether the client is supported or unsupported for high availability
  - configuration—Safety level of the configuration based on whether or not the client is supported or unsupported and, in the case of those unsupported, whether or not the client has been configured (for example, if an unsupported client is configured on a router with high availability enabled, the configuration would read “unsafe”)
- Example 1

```
host1#show redundancy clients

Unsupported High Availability Clients
 -------------------------------------
       client           configuration
--------------------   -------------
DHCP Proxy Client           safe
Global Ipv6                 safe
IPsec Transport (ITM)       safe
l2tpDialoutGenerator        safe
DHCPv6 Local Server         safe
Radius Relay Server         safe
```

- Example 2

```
host1#show redundancy clients all

High Availability Client Information
        ------------------------------------
       client               mode       configuration
--------------------   -----------   -------------
atm1483DataService      supported        safe
AA83                    supported        safe
aaaServer               supported        safe
atmAal5                 supported        safe
AAQS                    supported        safe
atm                     supported        safe
Bridged Ethernet        supported        safe
Transparent Bridging    supported        safe
dcm                     supported        safe
dhcpExternal            supported        safe
DHCP Proxy Client      unsupported       safe
DS1                     supported        safe
DS3                     supported        safe
ethernet                supported        safe
Flow Inspection         supported        safe
frameRelay              supported        safe
FT1                     supported        safe
Global Ipv6            unsupported       safe
Global Ip               supported        safe
HDLC                    supported        safe
IKEP                    supported        safe
ipflowstats             supported        safe
IpSubscriberManager     supported        safe
IPTU                    supported        safe
IPVR                    supported        safe
IPsec Transport (ITM)  unsupported       safe
l2tpDialoutGenerator   unsupported       safe
l2tp                    supported        safe
LMGR                    supported        safe
DHCPv4 Local Server     supported        safe
DHCPv6 Local Server    unsupported       safe
MPLS                    supported        safe
PMGR                    supported        safe
pppoe                   supported        safe
ppp                     supported        safe
qos                     supported        safe
Radius Relay Server    unsupported       safe
RSVP                    supported        safe
SCM                     supported        safe
slotHelper              supported        safe
Cisco HDLC              supported        safe
ServiceManager          supported        safe
Sonet                   supported        safe
SonetPath               supported        safe
SonetVT                 supported        safe
IPsec Tunnel (ST)       supported        safe
```

show redundancy history

- Use to display information about dates, times, and the number of occurrences for starts and switchovers.
- Use the **srp** keyword to view SRP module-specific information.
- Use the **detail** keyword to view additional history information.

- Field descriptions
  - system up time—Amount of time elapsed since the last cold boot
  - last cold start—Date and time the router experienced the last cold start
  - last cold switchover—Date and time the router experienced the last cold switchover
  - last warm switchover—Date and time the router experienced the last warm switchover
  - cold starts—Total number of cold starts the router has experienced
  - switchovers—Number of cold, warm, and consecutive warm switchovers the router has experienced
- Example 1

```
host1#show redundancy history

system up time:        0 00:08:01
last cold start:       2004-07-26 10:44:25
last cold switchover:  2004-07-25 18:51:56
last warm switchover:  2004-07-25 20:58:57

activation statistics:
    cold starts:           92
    switchovers:
        cold:              21
        warm:              147
        consecutive warm:  0
```

- Example 2

```
host1#show redundancy history detail

system up time:        0 00:08:01
last cold start:       2004-07-26 10:44:25
last cold switchover:  2004-07-25 18:51:56
last warm switchover:  2004-07-25 20:58:57

activation statistics:
    cold starts:           92
    switchovers:
        cold:              21
        warm:              147
        consecutive warm:  0

                                          system
SRP activation time      type      slot   uptime    running release
-------------------   ----------   ----   ------   -----------------
2004-09-08 15:10:40   cold-start    00     ---     erx_6-0-0b1-8.rel
2004-09-08 14:39:10   cold-start    00     ---     erx_6-0-0b1-1.rel
```

show redundancy line-card

- Use to display line-module-specific redundancy information.
- Field descriptions
  - automatic reverting—State of automatic reverting (on or off)
  - slot(s)—Slots in which the line modules reside
  - hardware role—Function of the line module: primary or spare
  - lockout config—Status of redundancy on this line module (protected—Line module redundancy is enabled; locked out—Line module redundancy is disabled)
  - backed up by slot—Slot that contains the line module that is a spare for this primary line module
  - sparing for slot—Slot that contains the primary line module for which this line module is a spare
  - revert at—Time at which you want line module to revert
  - midplane type—Identifier for the type of midplane
  - midplane rev—Hardware revision number of the redundancy midplane
- Example

```
host1#show redundancy line-card

automatic reverting is off

                                backed
                                  up      sparing
       hardware     lockout       by        for      revert
slot     role       config       slot      slot       at
----   --------   ----------   ------   --------   ------
 3       ---          ---       ---       ---       ---
 8      spare         ---       ---       ---       ---
 12    primary     protected     ---       ---       ---

         midplane   midplane
slots      type       rev
------   --------   --------
8 - 13      6          0
```

show redundancy srp

- Use to display SRP-module-specific redundancy information.
- Use the brief keyword to display summary information about SRP redundancy.

- Field descriptions
  - SRP
    - high-availability state—State of the high availability mode (disabled, active, or pending)
    - current redundancy mode—Redundancy mode currently being used by this router (high-availability or file-system-synchronization)
    - last activation type—Last type of activation that occurred on this router (that is, the method by which the SRP last booted [cold start or warm start])
  - Criteria Required for High Availability to be Active—Criteria required for high availability to be active.

NOTE: All criteria must be "yes" for high availability to be active.

- Example 1

```
host1#show redundancy srp


high-availability state:  active
current redundancy mode:  high-availability
last activation type:     warm-switch
```

- Example 2

```
host1#show redundancy srp detail

high-availability state:  disabled
current redundancy mode:  file-system-synchronization
last activation type:     cold-start

   Criteria Required for High Availability to be Active
   ----------------------------------------------------
                    criterion                          met
-------------------------------------------------------   ---
Active SRP hardware supports High Availability?        Yes
High Availability mode configured?                     No
Mirroring Subsystem present?                           Yes
Mirroring activity levels within limits?               Yes
Network Core Dumps disabled?                           Yes
Running configuration is safe for High Availability?   Yes
Standby SRP hardware supports High Availability?       Yes
Standby SRP is online and capable of mirroring?        Yes
Standby SRP is running the same release?               Yes
```

show redundancy switchover-history

- Use to display the high availability switchover history for the chassis.
- Field descriptions
  - SRP activation time—Amount of time the SRP module has been active
  - type—Type of switchover
  - slot—Slot in which the SRP module resides
  - system uptime—Amount of time the chassis has been operational
  - running release—Release running on the SRP module at the time of the switchover
- Example

```
host1#show redundancy switchover-history

                                        system
SRP activation time      type       slot    uptime          running release
-------------------   -----------   ----   ----------   -------------------------
2004-07-26 10:44:25   cold-start     07       ---       L-07-25-60b1mrg-e.rel
2004-07-25 20:58:57   warm-switch    06    0 00:15:08   L-07-25-60b1mrg-e.rel
2004-07-25 20:53:41   warm-switch    07    0 00:09:51   L-07-25-60b1mrg-e.rel
2004-07-25 20:44:43   cold-start     06       ---       L-07-25-60b1mrg-e.rel
2004-07-25 19:32:01   cold-start     06       ---       L-07-25-60b1mrg-d.rel
2004-07-25 18:58:01   warm-switch    06    0 00:12:01   L-07-25-60b1mrg-c.rel
2004-07-25 18:51:56   cold-switch    07    0 00:05:56   L-07-25-60b1mrg-c.rel
2004-07-25 18:46:54   cold-start     06       ---       L-07-25-60b1mrg-c.rel
2004-07-25 17:44:48   warm-switch    06    0 00:14:32   L-07-25-60b1mrg-b.rel
2004-07-25 17:31:07   cold-start     07       ---       L-07-25-60b1mrg-b.rel
2004-07-25 16:05:08   cold-start     07       ---       L-07-25-60b1mrg-a.rel
2004-07-24 23:25:09   warm-switch    07    0 16:27:03   L-07-24-60b1mrg-b.rel
2004-07-24 23:18:23   cold-switch    06    0 16:20:17   L-07-24-60b1mrg-b.rel
```

Clearing the Redundancy History

You can use the **clear redundancy history** command to clear the high availability switchover history for the router.

clear redundancy history

- Use to clear the detailed high availability switchover history for the router.
- Example

```
host1#show redundancy history detail

system up time:        0 00:08:01
last cold start:       2004-07-26 10:44:25
last cold switchover:  2004-07-25 18:51:56
last warm switchover:  2004-07-25 20:58:57

activation statistics:
    cold starts:           92
    switchovers:
        cold:              21
        warm:              147
        consecutive warm:  0
```

```
                                          system
SRP activation time      type       slot     uptime          running release
-------------------   -----------   ----   ---------- -------------------------
2004-07-26 10:44:25   cold-start     07       ---       L-07-25-60b1mrg-e.rel
2004-07-25 20:58:57   warm-switch    06    0 00:15:08   L-07-25-60b1mrg-e.rel
2004-07-25 20:53:41   warm-switch    07    0 00:09:51   L-07-25-60b1mrg-e.rel
2004-07-25 20:44:43   cold-start     06       ---       L-07-25-60b1mrg-e.rel
2004-07-25 19:32:01   cold-start     06       ---       L-07-25-60b1mrg-d.rel
2004-07-25 18:58:01   warm-switch    06    0 00:12:01   L-07-25-60b1mrg-c.rel
2004-07-25 18:51:56   cold-switch    07    0 00:05:56   L-07-25-60b1mrg-c.rel

host1#clear redundancy history

host1#show redundancy history

system up time:        0 00:08:01
last cold start:       2004-07-26 10:44:25
last cold switchover:  2004-07-25 18:51:56
last warm switchover:  2004-07-25 20:58:57

activation statistics:
    cold starts:           92
    switchovers:
        cold:              21
        warm:              147
        consecutive warm:  0

                                          system
SRP activation time      type       slot     uptime          running release
-------------------   -----------   ----   ---------- -------------------------
```

- There is no **no** version.

Chapter 8

Configuring a Unified In-Service Software Upgrade

This chapter describes how to prepare for and perform a unified in-service software upgrade (unified ISSU) of JUNOSe software on E120 and E320 routers. A unified in-service software upgrade provides a way to upgrade to a higher-numbered release while minimizing the effect of the upgrade on traffic forwarded through the router.

- Unified ISSU Overview on page 401
- Unified ISSU Platform Considerations on page 403
- Unified ISSU Terms That Describe SRP and Line Module Behavior on page 403
- Unified ISSU References on page 404
- Unified ISSU Phases Overview on page 404
- Application Support for Unified ISSU on page 412
- Unexpected Application-Specific Behavior During Unified ISSU on page 418
- Before You Begin a Unified In-Service Software Upgrade on page 430
- Upgrading Router Software with Unified ISSU on page 432
- Halting the Unified ISSU Process and Restoring the Original State of the Router on page 435
- Monitoring a Unified In-Service Software Upgrade on page 437

Unified ISSU Overview

In software releases numbered lower than Release 6.0, all line modules are reloaded when an SRP switchover occurs. This reload disconnects user sessions and disrupts forwarding through the chassis. Stateful SRP switchover was introduced in JUNOSe Release 6.0 to minimize the impact to the router of a stateful switchover from the active SRP module to the standby SRP module. Stateful SRP switchover (high availability) maintains user sessions during the switchover and data forwarding through the router continues to flow with little impact, thus improving the overall availability of the router.

The unified in-service software upgrade (unified ISSU) feature further extends router availability. Unified ISSU enables you to upgrade the router to a higher-numbered software release without disconnecting user sessions or disrupting forwarding through the chassis.

A conventional software upgrade—one that does not use the unified ISSU process—causes a router-wide outage for all users. Only static configurations (stored on the flash card) are maintained across the upgrade; all dynamic configurations are lost. A conventional upgrade takes 30-40 minutes to complete, with additional time required to bring all users back online.

When you perform a unified in-service software upgrade on a router that has one or more modules that do not support unified ISSU, these modules alone are upgraded by means of the legacy, conventional upgrade process. The unsupported modules undergo a cold reboot at the beginning of the unified ISSU process, and are held down until the in-service software upgrade is completed. Connections that pass through the unsupported modules are lost. The interfaces on these modules pass into a down state, which causes the physical layer and link layer to go down during the in-service software upgrade for those modules.

Applications that do not support unified ISSU applications cannot maintain state and configuration with minimal traffic loss across the upgrade to a higher-numbered release. When you attempt a unified in-service software upgrade on a router on which an ISSU-challenged application is configured, the in-service software upgrade cannot proceed.

Router Behavior During a Unified In-Service Software Upgrade

The following behaviors are characteristic of a unified in-service software upgrade.

- Connections that were established before you begin the in-service software upgrade are maintained across the upgrade. Any such connection that was forwarding data continues to do so during and after the upgrade.
- New connections are denied until the upgrade is completed.
- Packet loss during the upgrade is limited. Bandwidth through the modules is reduced, but the impact is minimal.
- Graceful restart protocols do not time out during the in-service software upgrade.
- The in-service software upgrade has a minimal effect on the control and data planes. During the SRP module upgrade phase, forwarding through the fabric is interrupted for about 1 second. During the line module upgrade phase, forwarding through the chassis is interrupted for about 30 seconds.
- Diagnostic software is not run on any modules during a unified in-service software upgrade.

- The router will undergo a cold restart if you attempt to upgrade the software to a lower-numbered version with unified ISSU. The in-service software upgrade must be to a higher-numbered release than the running release.
- Additional memory is consumed during a unified in-service software upgrade. Available memory on a line module might not be sufficient due to the module's configuration. Unified ISSU can detect this limitation during the upgrade procedure and exit the process.

Unified ISSU Platform Considerations

Unified ISSU is supported on E120 and E320 routers.

For information about modules supported on E120 and E320 routers:

- 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 modules that support unified ISSU.

Redundant SRP modules are required for unified ISSU support.

Unified ISSU is not supported on the ERX-7xx models, ERX-14xx models, and the ERX-310 router.

Unified ISSU Terms That Describe SRP and Line Module Behavior

Table 46 defines terms relevant to module behavior during a unified in-service software upgrade.

Table 46: Unified ISSU-Related Terms

Term	Meaning
Cold boot	The SRP module or line module loads diagnostics from the flash file system and runs them. When the diagnostics successfully complete, the operational image is loaded from the flash file system and then cold started.
Cold start	The SRP module or line module is initialized from the loaded operational image. The line modules are reloaded and the configuration is read from flash memory. When the line modules are operational, their configuration data is bulk downloaded and their interfaces become operational.
Cold restart	If the active SRP module fails, the standby SRP module assumes the role of active SRP module. When high availability is not configured, the cold restart is similar to the cold start, except that the applications are already loaded into memory on the standby SRP module and ready to be started. The line modules are reloaded.

Table 46: Unified ISSU-Related Terms (continued)

Term	Meaning
Warm restart	If the active SRP module fails, the standby SRP module takes the role of active SRP module. Mirrored configuration data as well as any mirrored volatile data are already resident in memory. The line modules continue to forward data (with a small loss of packets when the fabric is switched from the formerly active SRP module to the newly active SRP module). The protocols and other applications re-initialize from the mirrored data and resynchronize communications with the line modules. When resynchronization is completed, the router resumes normal operations, including updates of any routing tables that result from changes that occurred during the warm restart.

Unified ISSU References

For more information about stateful SRP switchovers see *Chapter 7, Managing High Availability*.

For more information about SRP module redundancy, see *Chapter 6, Managing Modules*.

Unified ISSU Phases Overview

The JUNOSe software includes software modules that operate the following hardware components:

- SRP module
- Line module control plane
- Line module forwarding plane

A unified in-service software upgrade replaces the currently operating software on each of these components with a higher-numbered release. The unified ISSU also upgrades or re-creates the state and configuration data of the configured applications.

Before you begin the in-service software upgrade, you must first prepare the router for the upgrade. See *Before You Begin a Unified In-Service Software Upgrade* on page 430 for more information.

The in-service software upgrade takes place in three phases:

1. Initialization Phase—When you issue the **issu initialize** command, unified ISSU verifies whether all prerequisites for the upgrade have been met. The router is prepared for the upgrade. The configuration that has been mirrored to the standby SRP module is upgraded according to the upgrade release. This phase can last from a few minutes up to 40 minutes depending on the number of software releases across which the router is being upgraded.

2. Upgrade Phase—When you issue the **issu start** command, unified ISSU again verifies whether all prerequisites for the upgrade have been met. During this phase the line module control plane and forwarding plane are upgraded and all three hardware components are resynchronized.

3. Service Restoration Phase—This phase automatically begins without user intervention when the upgrade phase has completed. During this final phase, the router is returned to a normal, runtime state.

The following sections describe these phases in more detail.

Unified ISSU Initialization Phase Overview

When you issue the **issu initialize** command, unified ISSU first verifies whether all requirements for the upgrade are met. The verification process examines the running release, the SRP modules, the line modules, line module redundancy, and the router configuration.

The **issu initialize** command does not interrupt or disrupt any of the runtime operations of the router. The command has no effect on changes of authorization, forwarding, or subscribers (except that the rate of logins might be affected). You cannot manually change the file system redundancy mode from high availability to file synchronization until the unified in-service software upgrade is completed.

NOTE: We recommend that you make no configuration changes after you have issued the **issu initialization** command. As a best practice, ensure that your configuration is complete before you start the software upgrade.

During the initialization phase, you can halt the in-service software upgrade at any time and revert either to a normal SRP module switchover or to the previous state of the router. To stop the unified ISSU process, you must issue the **issu stop** command. If instead you simply exit the CLI session, the unified ISSU initialization phase continues.

The action taken when a requirement is not met depends on the requirement. For some failed verifications, the CLI warns you of the issue and prompts you to proceed or quit the upgrade process. More serious failures cause the CLI to exit the command and provide a message describing the issue.

NOTE: We recommend that you issue the **show issu** command before beginning the in-service software upgrade. The output of the command lists any necessary conditions that are not currently met on the router. You can therefore correct these failures before entering into the upgrade. You can issue the **show issu** command at any time.

NOTE: On E120 and E320 routers, you can hot swap an IOA during the initialization phase without affecting the in-service software upgrade. However, we strongly recommend that you perform any necessary hot swaps before you issue the **issu initialize** command.

If the standby SRP module reloads during the initialization phase, unified ISSU is halted. You must begin again by issuing the **issu initialize** command.

Application Data Upgrade on the Standby SRP Module

Synchronized modules can become unsynchronized because you can change the router configuration at any time until you issue the **issu start** command. When the verification process is completed, unified ISSU starts up the stateful SRP switchover process to maintain synchronization between the active SRP module and the standby SRP module during the SRP module upgrade phase.

NOTE: An SRP switchover from the active SRP module to the standby SRP module at this point in the in-service software upgrade causes a cold restart of the router because the SRP modules are running two different releases. The current release is on the active SRP module and the upgrade release is on the standby SRP module.

The application and configuration data that has been mirrored to the standby SRP module is upgraded as required by the new software release. The CLI displays the progress of the SRP module upgrade.

While data on the standby SRP module is upgraded, any new changes that are mirrored from the primary SRP module to the standby SRP module are also upgraded to the version required by the armed release.

NOTE: This process consumes significant CPU resources on the redundant SRP module and can take a considerable amount of time to complete. Performance of the active SRP module might be affected during the SRP module upgrade.

When the upgrade release has been synchronized to the standby SRP module, stateful SRP switchover is disabled until the in-service software upgrade is completed.

If you configure an application that does not support unified ISSU during the initialization phase, the initialization phase completes, but the **issu start** command subsequently fails.

Line Module Arming

When the upgrade of the application data on the standby SRP upgrade is completed, unified ISSU temporarily arms the line modules with the upgrade release in a backup region of the memory.

NOTE: If a line module reloads at this point, it it is held down for the duration of the upgrade and then undergoes a cold boot to the running release; the line module has no effect on the unified ISSU process.

SNMP Traps

When you issue the **issu initialization** command, the SNMP agent generates a juniSystemIssuStateChange trap with juniSystemIssuState set to initializing. When the unified ISSU initialization is completed, the SNMP agent generates a juniSystemIssuStateChange trap with juniSystemIssuState set to initialized.

Unified ISSU Upgrade Phase Overview

During the upgrade phase, the CLI supports only a reduced set of administrative commands. You cannot interrupt the upgrade phase. The upgrade phase cannot commence if any CLI commands outside of this set are executing when you issue the **issu start** command.

NOTE: Although you can use any CLI session to issue the **issu start** command, we recommend that you issue the command from a session to the management console port. When the standby SRP module switchover takes place, all management network connections through the Ethernet management port are dropped, and you can access the router only through a console port until the service restoration phase is completed.

When you issue the **issu start** command, unified ISSU performs the following operations:

1. Verifies that the unified ISSU requirements on the router are still met.
2. Verifies that the active and standby SRP modules are synchronized. If they are not synchronized, forces a synchronization to ensure that all configuration and file system changes are propagated to the standby SRP module before proceeding with the upgrade.
3. Copies the NVS configuration from a backup memory area to the flash card on the standby SRP module. During the initialization phase, this configuration data was mirrored from NVS on the active SRP module and upgraded as required by the armed release.
4. Upgrades the control plane on each line module at the same time.
5. Switches control from the primary SRP module (running the current release) to the standby SRP module (running the armed upgrade release).
6. Upgrades the forwarding plane on each line module at the same time. The fabric is switched and upgraded.

You can view the status of the router and the progress of the upgrade at any time by issuing the **show issu** command from another terminal session to the router.

NOTE: While a unified ISSU operation is in progress, do not remove the SRP modules or attempt to reset them. Removing the SRP modules anytime during unified ISSU has an adverse impact.

After the unified ISSU operation is completed, issue the **show version** command. The output should indicate the following:

- The formerly active SRP module has rebooted and come up as the new standby SRP module.
- The newly active SRP module indicates that the formerly active SRP has rebooted and has come up as standby SRP module

You can then remove an SRP module after issuing the **halt** command.

Exceptions During the Upgrade Phase

Table 47 describes the behavior of the router during the upgrade phase when certain exceptional events take place outside the context of the in-service software upgrade.

Table 47: Router Response to Undesirable Events During the Upgrade Phase

Event	Router Action
The router reloads.	■ The unified ISSU operation halts. ■ The router undergoes a cold restart. ■ The router boots with the armed upgrade release. ■ The line modules reboot.
The primary SRP module switches over to the standby SRP module.	■ The unified ISSU operation halts. ■ The router undergoes a cold restart. ■ The router boots with the armed upgrade release. ■ The line modules reboot.
The standby SRP module reloads.	■ The unified ISSU operation halts. ■ The router undergoes a cold restart. ■ The router boots with the armed upgrade release. ■ The line modules reboot.
A line module reloads.	■ The line module is held down and prevented from rebooting until the service restoration phase is completed. The line module then undergoes a cold reboot to the running (pre-upgrade) release.
An IOA is hotswapped.	■ Hot swapping is disabled during the upgrade phase. The line module undergoes a cold reboot and hot swapping is reenabled when the service restoration phase is completed,
An application that does not support unified ISSU is configured.	■ This event can take place only before the **issu start** command is issued, because that command disables CLI configuration commands. When you issue the **issu start** command, after configuring such an application, the command exits and generates an error message.

Verification of Requirements

Because some time may have passed since unified ISSU verified the requirements for the upgrade during the initialization phase, unified ISSU reverifies all the same conditions.

Unified ISSU also verifies that no CLI configuration sessions are open, that no scripts or macros are running, and that any SNMP requests or CLI commands in progress complete within 5 seconds.

If any of the required conditions are not met, the CLI either exits the command with an error message or provides an informative message and prompts you to proceed or halt.

When all the conditions are met, the CLI prompts you to proceed. If you continue, then you can subsequently halt the upgrade only by reloading the router. If you exit the command, the router remains in the unified ISSU initialized state.

Upgrade Setup

At this stage all the preconditions have been met. The unified ISSU process shuts down all management interfaces to the router in order to prevent changes in the configuration.

Final preparation for the upgrade phase includes the following actions:

- SNMP—The SNMP agent generates a juniSystemIssuStateChange trap with juniSystemIssuState set to upgrading to indicate that the final phase of the operation has begun. When the trap is issued with this state value, the SNMP agent stops accepting any new SNMP gets or sets and does not issue any further traps.

- CLI—Most CLI commands are disabled. Only **reload**, **show issu**, and **show version** commands are available to you until the service restoration phase completes. These commands are available on the console and are not available to Telnet sessions.

- External events—Externally created events from sources other than the CLI are ignored. These events typically come from user connections, RADIUS servers, SRC software and SDX software, and SNMP, and include login requests, COA requests, multicast join requests, packet mirroring requests, and so on. Logout requests are cached and processed at a later stage.

- Routing protocols—The unified ISSU process prompts you to consider raising the link costs for each routing protocol that is configured on the router. Raising the link cost for routes through the upgrading router enables neighbors to recompute better routes to those destinations. If you choose to raise the link cost, the higher costs can take some time to propagate through the network. Because the router is unable to determine when this has completed, it waits for 2 minutes before proceeding to the next step in the upgrade.

  The reason for raising the link cost is that once the upgrade of the line module control plane begins, routing protocol updates cannot be installed in the line modules until that upgrade completes. That period can be in the range 2–15 minutes. During the control plane upgrade, the routing protocols can still accept new routes and communicate with their neighbors but cannot install the routes.

- Routing protocols—The unified ISSU process prompts you to consider raising the link costs for each routing protocol that is configured on the router.

  Once the upgrade of the line module control plane begins, routing protocol updates cannot be installed in the line modules until that upgrade completes. That period can be in the range 2–15 minutes. During the control plane upgrade, the routing protocols can still accept new routes and communicate with their neighbors but cannot install the routes.

  Raising the link cost for routes through the upgrading router enables neighbors to recompute better routes to those destinations that do not pass through the upgrading router. If you choose to raise the link cost, the higher costs can take some time to propagate through the network. Because the router is unable to determine when this has completed, it waits for 2 minutes before proceeding to the next step in the upgrade.

- Unsupported line modules—Any unsupported line modules that are present are held down after the start of this phase when you can no longer gracefully exit from the unified ISSU process. The modules are held down for the duration of the in-service software upgrade and are then undergo a cold boot to the original running release.

- IGMP requests—The router cannot handle IGMP requests for channel changing for IPTV implementations.

Line Module Control Plane Upgrade

At this point, the upgrade release is preserved on each line module in some backup region. When signaled by the active SRP module, all supported line modules simultaneously reload and restart with the new release. Forwarding through the forwarding subsystem on the line modules—through the fabric of the system—is not be affected by the reload.

The line modules then simultaneously recover any application data preserved in memory on the line module and upgrade that data into a format that is understood by the applications running on the new release. This operation can take in the range of 1–10 minutes depending on the size of the data and the upgrade path of the data. Each line module restores its operational state, running the new release with all data upgraded to a version acceptable to the new software.

If the upgrade process fails for any line module, that module undergoes a cold restart, but none of the other line modules is affected.

SRP Module Switchover

At this stage the primary SRP module is running the current release, the redundant SRP module is running the armed release, and the control plane on each supported line module is running the armed release.

When the primary SRP module has verified that all line modules are up, the redundant SRP module takes over control of the router by becoming the active SRP module. The primary, and formerly active, SRP module reboots to the armed release and serves as the standby SRP module.

All applications on the newly active SRP module are restarted. Each application reconstructs itself from the mirrored data, restoring its state and configuration as it was before the switchover. Forwarding through the fabric is interrupted for about one second.

The SRP switchover restarts the routing protocols and triggers a graceful restart because the routes need to be recomputed. This recalculation can take up to 90 seconds. Data continues to be forwarded through routes that were learned before the upgrade of the line module control planes.

Line Module Forwarding Plane Upgrade

While the applications on the SRP module and the line modules reconstruct themselves, they also begin to build up the new state for the forwarding subsystem. All applications on the line module signal the system when they are ready to start the forwarding upgrade.

Because upgrading the forwarding plane affects forwarding through the chassis for up to 30 seconds, unified ISSU does not proceed until the routing protocols have signaled that route reconvergence has completed. Unified ISSU then informs all line modules to simultaneously upgrade their forwarding subsystems.

The line modules then perform the following steps:

1. Halt forwarding through the line modules. Although any links to external devices remain up, incoming data is dropped.
2. Update any changed programmable hardware devices.
3. Update the forwarding subsystem with the new release and upgraded configuration data.
4. Update the routing tables with the reconverged routes.
5. Resume forwarding.

Unified ISSU Service Restoration Phase Overview

This is the final unified ISSU phase. At this point, all three major components of the router—the SRP modules, the line module control planes, and the line module forwarding planes—have been upgraded and forwarding has resumed through the chassis. The following actions take place during this phase:

- The CLI is re-enabled. All commands are made available to users.
- The SNMP agent is restarted and bulk statistics are collected and available for review.
- New login requests and logout requests are processed. The router begins to accept externally created events from sources other than the CLI and SNMP. These events typically come from user connections, RADIUS servers, and SRC software and SDX software, and include login requests, COA requests, multicast join requests, and so on.

- Logout requests that were cached at the start of the in-service software upgrade are processed.
- After the flash memory on the newly active SRP module is updated, stateful SRP switchover is available to the router.

At this point the in-service software upgrade is completed, and the router is restored to normal operation. Any line modules that reloaded during the upgrade phase and were therefore held down are now rebooted to the original running release.

Application Support for Unified ISSU

When an application supports unified ISSU, you can configure the application on the router and proceed with the unified in-service software upgrade with no adverse impact to the upgrade.

Applications that do not support unified ISSU cannot maintain state and configuration with minimal traffic loss across the upgrade. When you attempt the unified in-service software upgrade on a router that is configured with an ISSU-challenged application, the in-service software upgrade is halted and cannot proceed unless you change the configuration. An application that does not support high availability cannot support unified ISSU.

Table 48 indicates which applications support or do not support a unified in-service software upgrade, as well as limitations on their behavior.

Table 48: Application Support for Unified In-Service Software Upgrades

Application	Supported	Unsupported	Notes
Physical Layer Protocols			
DS1	✔	–	–
DS3	✔	–	–
HDLC	✔	–	–
SONET/SDH	✔	–	E120 and E320 routers do not support APS.
SONET/SDH VT	–	✔	–
Link-Layer Protocols			
ARP	✔	–	ARP entries in the ARP cache do not time out because no ARP aging occurs during unified ISSU. When the unified ISSU is completed, the ARP cache contains the same entries as it had before the unified ISSU began.
ATM	✔	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
ATM 1483 bulk configuration of dynamic interfaces	✔	–	–
ATM bulk configuration of static interfaces	✔	–	–
Bridged Ethernet	✔	–	–
Cisco HDLC	✔	–	–
Ethernet (with and without VLANs)	✔	–	–
Frame Relay	✔	–	–
PPP	✔	–	–
PPPoE	✔	–	–
Transparent bridging	✔	–	–
Unicast Routing			
Access Routes	✔	–	–
BGP	✔	–	–
FTP	–	✔	–
IP	✔	–	–
IPv6	–	✔	Unified ISSU does not support IPv6.
IPSec Transport	Not applicable	Not applicable	E120 and E320 routers do not support IPSec.
IPSec Tunnels	Not applicable	Not applicable	E120 and E320 routers do not support IPSec.
IS-IS	✔	–	Support only when graceful restart is configured.
OSPF	✔	–	Support only when graceful restart is configured.
RIP	✔	–	–
Static Routes	✔	–	–
Telnet	✔	–	Authentication and command authorizations on Telnet sessions fail during the upgrade phase and Telnet sessions are dropped.

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
IPv4 Multicast Routing			
Multicast Routing	✔	–	–
ANCP (L2C)	✔	–	Unified ISSU can proceed if ANCP is configured. However, ANCP has no graceful restart extensions and therefore it cannot maintain its dynamic state across the upgrade. Consequently, all ANCP sessions are brought down and then restored when the upgrade is completed.
DVMRP	✔	–	–
IGMP	✔	–	–
PIM	✔	–	–
IPv6 Multicast Routing			
Multicast Routing	–	✔	Unified ISSU does not support IPv6.
MLD	–	✔	Unified ISSU does not support IPv6.
PIM	–	✔	Unified ISSU does not support IPv6.
Multiprotocol Label Switching			
MPLS	✔	–	–
BGP signaling	✔	–	–
LDP signaling	✔	–	–
RSVP-TE signaling	✔	–	–
Local cross-connects between layer 2 interfaces using MPLS	✔	–	–
Policies and QoS			
Policies	✔	–	–
QoS	✔	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
Remote Access			
AAA	✔	–	The following configuration is not supported: The subscriber username and password are on an ATM circuit in Bridged Ethernet over ATM or IP over ATM configurations.
DHCP External Server and Packet Trigger	–	✔	–
DHCP Packet Capture	✔	–	Configuration of DHCP packet capture does not prevent unified ISSU from proceeding. However, the capturing of packets on the line modules is halted when the unified ISSU upgrade phase commences. Packet capture resumes automatically during the unified ISSU service restoration phase.
DHCP Proxy Client	–	✔	–
DHCP Relay Proxy	–	✔	–
DHCP Relay Server	–	✔	–
DHCPv4 Local Server	✔	–	Ensure that DHCP clients have a minimum lease of 120 minutes before you begin unified ISSU to prevent unwanted lease expirations due to the length of the unified ISSU process.
DHCPv6 Local Server	–	✔	Unified ISSU does not support IPv6.
L2TP	✔	–	Unified ISSU forces an L2TP failover for all established tunnels. L2TP failover resynchronization is required for successful recovery of a tunnel and its sessions following the upgrade.
L2TP Dialout	–	✔	–
Local Address Pools	✔	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
Local Authentication Server	✔	–	–
RADIUS Client	✔	–	–
RADIUS Dynamic-Request Server	✔	–	
RADIUS Initiated Disconnect	–	✔	–
RADIUS Relay Server	–	✔	–
RADIUS Route-Download Server	✔	–	–
SRC Client	✔	–	–
Service Manager	✔	–	–
Subscriber Manager	✔	–	–
TACACS+	✔	–	–
Miscellaneous			
Bulk statistics	✔	–	–
Denial of Service (DoS) protection	✔	–	–
Firewall	✔	–	–
HTTP server	✔	–	–
IOA hot swap	–	✔	–
J-Flow (IP flow statistics)	✔	–	–

Table 48: Application Support for Unified In-Service Software Upgrades (continued)

Application	Supported	Unsupported	Notes
Line Module Redundancy	✔	–	When you issue the **issu initialization** command, line module redundancy is made inactive until the upgrade is completed. If a line module in the redundancy group fails during this period of inactivity, unified ISSU holds that module down. The redundant line module cannot take over for the failed line module until the unified ISSU is completed. The primary line modules in the redundancy group must be active for the unified ISSU to proceed. If instead the redundant module is active, validation fails and unified ISSU is halted. You must revert to the primary module in the redundancy group to proceed with the upgrade.
Mobile IP Home Agent	–	✔	–
Network Address Translation	✔	–	–
NTP	✔	–	–
Resource Threshold Monitor	✔	–	–
Response Time Reporter	✔	–	–
Route Policy	✔	–	–
SNMP	✔	–	–
Subscriber Interfaces	✔	–	–
Tunnels (GRE and DVMRP)	✔	–	–
VRRP	✔	–	–

Unexpected Application-Specific Behavior During Unified ISSU

This section describes the behavior of applications that vary from the expected behavior during a unified in-service software upgrade.

- AAA Authentication and Authorization Disabled on page 418
- ATM Affected Behaviors on page 418
- DHCP Affected Behaviors on page 419
- DoS Protection State Freeze on page 420
- Ethernet Affected Behaviors on page 420
- FTP Server File Transfers Halted on page 421
- IS-IS Effects on Graceful Restart and Network Stability on page 421
- L2TP Failover of Established Tunnels on page 423
- OSPF Effects on Graceful Restart, Timeouts, and Network Stability on page 423
- PIM Suspended During Unified ISSU on page 425
- Subscriber Logins and Logouts Suspended During Unified ISSU on page 426
- SONET/SDH Behavior During Unified ISSU on page 426
- TACACS+ Services Not Available on page 427
- Interruption in Traffic Forwarding for Layer 3 Routing and Signaling Protocols on page 427
- Recommended Routing Protocol Timer Settings on page 429

AAA Authentication and Authorization Disabled

Authentication and command authorization are temporarily disabled on the serial console connection during the upgrade phase. You can connect to the serial console and issue the **reload**, **show issu**, and **show version** commands without the action of authentication and authorization servers, such as RADIUS or TACACS+.

ATM Affected Behaviors

The following aspects of ATM behavior during unified ISSU are different than the behavior during normal router operations.

ILMI Sessions Not Maintained

The router does not maintain ILMI sessions during a unified in-service software upgrade. The router terminates all ILMI sessions and restarts them during the upgrade. If the ILMI protocol is enabled on any port, you are warned during the initialization phase when unified ISSU is verifying the prerequisites for the upgrade. You can choose to continue the upgrade—and bring down the sessions—or to halt the in-service software upgrade.

OAM CC Effects on VCC

When an ATM VC is configured as an OAM CC source, periodic OAM cells are generated for about 15 seconds. The device configured as the OAM CC sink is likely to declare the VCC down during this time. Unified ISSU generates a warning when it detects an OAM CC source configuration during the initialization phase while unified ISSU is verifying the prerequisites for the upgrade. You can choose to continue or halt the in-service software upgrade

When an ATM VC is configured as OAM CC sink, it cannot receive OAM CC cells generated by the source for about 15 seconds. The OAM CC does not time out and the VCC is not declared down. OAM CC cell generation resumes when the unified ISSU operation is completed.

OAM VC Integrity Verification Cessation

During the unified ISSU operation, verification of OAM VC integrity stops. This verification resumes when the unified ISSU operation is completed.

ATM does not respond to incoming OAM loopback cells during the upgrade for a period of less than 30 seconds. The lack of response might cause ATM peers to declare VCC (VPC) down.

Port Data Rate Monitoring Cessation

The monitoring of ATM port data rates is halted during a unified in-service software upgrade. Monitoring resumes immediately after the unified ISSU operation is completed. The data rates reported by the **show atm interface** command are inaccurate for the period of one configured load interval after unified ISSU is completed.

VC and VP Statistics Monitoring Halts Unified ISSU Progress

A unified in-service software upgrade cannot proceed if VC or VP statistics monitoring is in progress.

DHCP Affected Behaviors

DHCP Common Component Information Suspended

The common DHCP component supports unified ISSU. This component configures option 60 vendor-option strings when you issue the **set dhcp vendor-option** command. The DHCP common component ceases all CLI and SNMP operations when you issue **issu start** command. You can therefore obtain no information about the common DHCP infrastructure until the in-service software upgrade is completed.

DHCP External Server Prevents Unified ISSU Operation

The DHCP external server application does not support unified ISSU. You must completely unconfigure this application from all virtual routers to perform a unified in-service software upgrade.

DHCP Relay and DHCP Relay Proxy Prevent Unified ISSU

The DHCP relay and DHCP relay proxy applications do not support unified ISSU. You must completely unconfigure these applications from all virtual routers to perform a unified in-service software upgrade.

DHCP Packet Capture Halted on Line Modules

The DHCP packet capture application supports unified ISSU in that its configuration does not halt a unified in-service software upgrade. However, packet capture on line modules is halted during the upgrade phase. Packets are not captured and buffered for later forwarding to the SRP module during this phase. Capture resumes automatically during the service restoration phase.

DoS Protection State Freeze

The denial-of-service (DoS) protection application freezes its state when the in-service software upgrade is initiated. Any suspicious control flow, protocol, or priority remains suspicious until unified ISSU completes.

Freezing the DoS protection state prevents any active control flows from interfering with the system while the unified ISSU is in progress. However, no new control flows, protocols, or priorities are monitored for suspicious activity, and no suspicious activity can be detected until the upgrade is completed.

NOTE: Because of this limitation on DoS functionality, we recommend that you do not initiate unified ISSU until all suspicious control flows, protocols, and priorities have been resolved.

When the in-service software upgrade is completed, the DoS protection application resumes attending to all dynamic state that was frozen at the beginning of the unified ISSU process.

Some suspicious control flows might remain in a suspicious list based on your configuration. If the upgrade software version has DoS protection classification algorithms that are better or different than in the previous version, you might want to clear these suspicious control flows to enable the classification algorithms to determine whether the flow is still considered to be suspicious.

Ethernet Affected Behaviors

The following aspects of Ethernet behavior during a unified in-service software upgrade are different than during normal router operations.

ARP Packets Briefly Not Sent or Received

There is a brief period at the end of the upgrade phase when ARP packets are not sent or received. This event can affect ARP entries on attached devices that were in the process of being aged out.

Link Aggregation interruption

During the in-service software upgrade, LACP PDUs are not generated or received for about 15 seconds on Ethernet ports configured with LACP,

This interruption has no effect on the local side of the link because JUNOSe software generates LAC PDU packets every 30 seconds. The link is not declared down unless packets are missed three times. LACP packet generation continues when the unified ISSU operation is completed.

If a device on the other end of the link is configured with the short timeout of one second, then the device is likely to declare the link to be down and remove the link from the LAG bundle.

Port Data Rate Monitoring Halted

The monitoring of Ethernet port data rate is halted during a unified in-service software upgrade. Monitoring resumes immediately after the unified ISSU operation is completed. The data rates reported by the **show interface** command are inaccurate for the period of one configured load interval after unified ISSU is completed.

VLAN Statistics Monitoring Halts Unified ISSU Progress

A unified in-service software upgrade cannot proceed if VLAN statistics monitoring is in progress.

FTP Server File Transfers Halted

During a unified in-service software upgrade, file transfers that involve the FTP server are halted because of the SRP module switchover during the upgrade.

For this reason, the FTP server does not support unified ISSU. You can continue with the in-service software upgrade only when the FTP server is not enabled. You must disable the FTP server to perform the upgrade.

IS-IS Effects on Graceful Restart and Network Stability

IS-IS has the following issues to consider before you begin a unified in-service software upgrade:

- Graceful restart—Required
- Routing around the upgrading router—Optional

Configuring Graceful Restart Before Unified ISSU Begins

You must configure IS-IS graceful restart on the router and on all IS-IS neighbors before you begin the in-service software upgrade. When the unified ISSU process verifies the upgrade requirements during the initialization phase, it detects whether graceful restart is configured. If it is not configured, the CLI displays a warning message and prompts you to proceed or halt. You can stop at this point to configure graceful restart.

If instead you proceed, the in-service software upgrade can complete successfully, but the IS-IS neighbors are likely to break the adjacencies with the upgrading router and consider that routes formerly reached through this router are now unreachable. When the in-service software upgrade completes and the routing protocols restart, the IS-IS neighbors can relearn the routes through the router.

When you issue the **issu start** command, IS-IS lengthens its hello timer values and sends LSPs with the new values. The upgrade proceeds when the IS-IS neighbors have acknowledged the new values.

Configuring Graceful Restart When BGP And LDP are Configured

When BGP, IS-IS, and LDP are all configured on a router on which you will perform a unified in-service software upgrade, ensure that the IS-IS graceful restart timeout is longer than the LDP graceful restart timeout. The IS-IS graceful restart does not complete when the LDP graceful restart timeout is longer than the IS-IS graceful restart timeout. Configure IS-IS graceful timeout with the **nsf t3** command. Configure LDP graceful restart timeout with the **mpls ldp graceful-restart timers max-recovery** command.

Routing Around the Restarting Router to Minimize Network Instability

NOTE: The situation described in this section is very uncommon. This rare circumstance arises when you have redundant uplinks to the core and network topology changes cause routes to go through the upgrading router. In a typical network design, this is not an issue and you do not need to route peers around the upgrading router,

During the unified ISSU upgrade phase, network instability can result if the restarting router goes into an unstable state after the unified ISSU process fails. Some IS-IS traffic loss occurs during the resulting line module resets. For those reasons, you might want IS-IS peers to route around the router that is being upgraded.

You can use the **overload advertise-high-metric issu** command to cause the router to advertise a high metric to its neighbors so that they route around the upgrading router. When you issue the **issu start** command, the router raises the metric to the maximum link cost on all interfaces running IS-IS. The maximum value depends on the metric type. IS-IS neighbors then choose a path with lower metrics to reach any destination that was previously reached through the upgrading router. When unified ISSU is completed, IS-IS reverts the metrics back to the values that were configured before the in-service software upgrade.

When traffic engineering has been configured, the traffic engineering metrics are also increased. New tunnels are not established through the upgrading router and any tunnels undergoing re-optimization in other routers go around the upgrading router.

IS-IS support for unified ISSU does not depend on this configuration. If you do not issue the **overload advertise-high-metric issu** command, the in-service software upgrade can still proceed to successful completion without disrupting IS-IS functionality.

overload advertise-high-metric issu

- Use to cause IS-IS to advertise the maximum link metric on all interfaces to IS-IS neighbors when a unified in-service software upgrade is started.
- Example

  host1(config-router)#**overload advertise-high-metric issu**

- Use the **no** version to send the configured link costs to neighbors during the in-service software upgrade.

L2TP Failover of Established Tunnels

L2TP never declares itself as unified ISSU unsafe. However, unified ISSU forces an L2TP failover for all established tunnels. Successful recovery of a tunnel and its sessions following the in-service software upgrade requires a successful L2TP failover resynchronization, either by the L2TP silent failover method or the L2TP failover protocol.

When the unified ISSU operation attempts to verify the upgrade prerequisites, a warning message is generated if any tunnels are present for which failover resynchronization is disabled.

You can use the **show l2tp tunnel failover-resync disable** command to identify the tunnels referred to by the warning message. The command enables filtering based upon the effective failover resynchronization mechanism:

```
host1#show l2tp tunnel failover-resync disable
L2TP tunnel 2/1 is Up with 1 active session
1 L2TP tunnel found
```

If a successful failover resynchronization cannot be performed for a tunnel following the upgrade, then the tunnel and all of its sessions are subject to disconnection.

L2TP automatically detects a peer L2TP disconnect after the in-service software upgrade is completed by detecting a control channel failure.

When peer LNSs are not configured with PPP keepalives or inactivity timeouts, you must configure an inactivity timeout for L2TP on the LAC. This timeout enables the router to detect a PPP disconnect when signaling has been dropped during the unified ISSU forwarding interruption. In the absence of this configuration, the connection at the LAC and LNS is left as logged in for an extended period of time following the upgrade.

OSPF Effects on Graceful Restart, Timeouts, and Network Stability

OSPF has the following issues to consider before you begin a unified in-service software upgrade:

- Graceful restart—Required
- Dead interval—Required
- Routing around the upgrading router—Optional

Configuring Graceful Restart Before Unified ISSU Begins

You must configure OSPF graceful restart before you begin the in-service software upgrade. When the unified ISSU process verifies the upgrade requirements during the initialization phase, it detects whether graceful restart is configured. If it is not configured, the CLI displays a warning message and prompts you to proceed or halt. You can stop at this point to configure graceful restart.

If instead you proceed, the in-service software upgrade can complete successfully, but the OSPF neighbors are likely to break the adjacencies with the upgrading router and consider that routes formerly reached through this router are now unreachable. When the in-service software upgrade completes and the routing protocols restart, the IS-IS neighbors can relearn the routes through the router.

You must also ensure that the OSPF neighbors have been configured as graceful restart helper routers. During the unified ISSU initialization phase, OSPF graceful restart on the upgrading router cannot verify whether its neighbors are helper routers, and reports that fact by means of the CLI.

Configuring Graceful Restart When BGP And LDP are Configured

When BGP, LDP, and OSPF are all configured on a router on which you will perform a unified in-service software upgrade, ensure that the OSPF graceful restart timeout is longer than the LDP graceful restart timeout. The OSPF graceful restart does not complete when the LDP graceful restart timeout is longer than the OSPF graceful restart timeout. Configure OSPF graceful restart timeout with the **graceful-restart restart-time** command. Configure LDP graceful restart timeout with the **mpls ldp graceful-restart timers max-recovery** command.

Configuring a Longer Dead Interval Than Normal

To prevent OSPF from timing out to the OSPF neighbors, you must configure a dead interval that is longer than the period required for the in-service software upgrade to complete. You must use the value provided by unified ISSU in a warning message displayed during the initialization phase.

Routing Around the Restarting Router to Minimize Network Instability

NOTE: The situation described in this section is very uncommon. This rare circumstance arises when you have redundant uplinks to the core and network topology changes cause routes to go through the upgrading router. In a typical network design, this is not an issue and you do not need to route peers around the upgrading router,

During the unified ISSU upgrade phase, network instability can result if the restarting router goes into an unstable state after the unified ISSU process fails. Some OSPF traffic loss occurs during the resulting line module resets. For those reasons, you might want OSPF peers to route around the router that is being upgraded.

You can use the **overload advertise-high-metric issu** command to cause the router to advertise a high link cost to its neighbors so that they route around the upgrading router. When you issue the **issu start** command, the router raises the link cost to the maximum link cost on all interfaces running OSPF. The higher cost is advertised in the OSPF LSAs. OSPF neighbors then choose a path with lower metrics to reach any destination that was previously reached through the upgrading router. When unified ISSU is completed, OSPF reverts the link costs back to the values that were configured before the in-service software upgrade.

When traffic engineering has been configured, the traffic engineering metrics are also increased. New tunnels are not established through the upgrading router and any tunnels undergoing re-optimization in other routers go around the upgrading router.

OSPF support for unified ISSU does not depend on this configuration. If you do not issue the **overload advertise-high-metric issu** command, the in-service software upgrade can still proceed to successful completion without disrupting OSPF functionality.

overload advertise-high-metric issu

- Use to cause OSPF to advertise the maximum link cost on all interfaces to OSPF neighbors when a unified in-service software upgrade is started.
- Example

  host1(config-router)#**overload advertise-high-metric issu**

- Use the **no** version to send the configured link costs to neighbors during the in-service software upgrade.

PIM Suspended During Unified ISSU

You can minimize PIM traffic loss during the in-service software upgrade by issuing the **ip pim dr-priority** command to set a priority so that PIM neighbors do not forward traffic through the upgrading router. By default, a PIM interface has a priority of one. If you set the priority to one, the lowest possible priority, then the upgrading router is not selected to be a designated router in the PIM network if an interface on another router in that network has a higher priority.

ip pim dr-priority

- Use to set a priority by which a router is likely to be selected as the designated router.
- Example

  host1(config-if)#**ip pim dr-priority 1**

- Use the **no** version to restore the default value, 1.

Subscriber Logins and Logouts Suspended During Unified ISSU

All new subscriber logins are ignored during the upgrade phase. New subscriber logouts are cached and processed after the unified ISSU operation is completed.

Subscriber Statistics Accumulation or Deletion

All subscriber statistics present in the line modules are cleared when the line module forwarding planes are upgraded. For this reason, the router has to read the statistics from the forwarding plane before it is upgraded.

However, forwarding through the line modules continues after that point, until the line module forwarding plane is upgraded. Some statistics can therefore accumulate in the forwarding plane in the interval between these two events. These statistics are not preserved across the upgrade.

Statistics for subscribers that log out during the forwarding plane upgrade are collected and reported before the forwarding plane is reloaded. Statistics are not collected for any subscribers who are connected before you issue the **issu start** command but who log out before the forwarding plane upgrade is completed.

The following subscriber statistics are preserved across the upgrade:

- All policy statistics
- Accounting statistics reported by IP: in bytes, out bytes, in packets, out packets
- Accounting statistics reported by L2TP: in octets, out octets, in packets, out packets
- Accounting statistics reported by PPP: in octets, out octets, in packets, out packets

All other statistics are set to zero, including all statistics belonging to the SNMP generic interface MIB for every interface layer.

SONET/SDH Behavior During Unified ISSU

During a unified in-service software upgrade, several aspects of SONET behavior differ from normal operation.

- SONET APS is not supported.
- During a conventional software upgrade, a SONET loss-of-signal defect lasts more than 2.5 seconds, causing the router to declare an LOS failure. Devices on the remote end of SONET links detect the failure and bring down the link and the dynamic interface stacks built on the link.

  During a unified in-service software upgrade, the LOS does not last more than 2.5 seconds. The remote device detect a momentary LOS but does not perceive this short LOS as a link failure and does not bring the link down,

TACACS+ Services Not Available

During the upgrade phase of unified ISSU, TACACS + services are unavailable. If you have configured AAA authentication for Telnet (with the **aaa new-model command**) this lack of availability affects CLI authentication, authorization, and accounting activities.

Because there is no alternate method of accounting other than TACACS, CLI exec and command accounting does not work during this phase.

Interruption in Traffic Forwarding for Layer 3 Routing and Signaling Protocols

The routing protocols are affected by two interruptions in traffic forwarding caused by the in-service software upgrade during the upgrade phase.

- Switchover from active to standby SRP module—When the active SRP module running the current release switches over to the standby SRP module running the upgrade release, the routing protocols and all other applications restart. A control plane outage of 30–40 seconds prevents the protocols from sending hellos or keepalive messages.

  The protocols must gracefully restart to come back online, recover their routing state on the newly active SRP module, and respond to their peers. Therefore, you must enable graceful restart for all protocols before you begin the in-service software upgrade. All neighbors of the routing protocols must also be configured to support graceful restart.

  A data plane outage of about one second also takes place during the switchover of the fabric from the active primary SRP module to the standby SRP module.

- Upgrade of the forwarding plane for each line module—After the routing protocols reconverge with their peers and rebuild their routing tables, unified ISSU upgrades the forwarding plane on all line modules simultaneously. This upgrade halts forwarding through the chassis. This forwarding outage lasts about 15 seconds.

If capable, routing protocols temporarily lengthen their timers to survive the outages. During the initialization phase, unified ISSU checks for timers that are set too short and whether the protocol enables timer renegotiation. If these checks fail, unified ISSU generates a warning and enables you to reconfigure the protocols before you issue the **issu start** command.

We recommend that you configure timers to be longer than usual for the routing protocols that cannot renegotiate timers. You can use bidirectional forwarding detection (BFD) to quickly detect forwarding interruptions.

Table 49 describes how individual routing protocols behave during a unified in-service software upgrade.

Table 49: Behavior of Routing Protocols During a Unified In-Service Software Upgrade

Protocol	Behavior
BFD	BFD renegotiates its timers as needed. Typically, the timers are lengthened until the SRP module switchover takes place, then shortened for the forwarding plane upgrade, and finally shortened to the original configured values.
BGP	The configured BGP timers are typically long enough to survive the forwarding outages. If, not, unified ISSU generates a warning message. BGP sends out keepalive messages immediately before and immediately after both the SRP module switchover and the forwarding plane restart, independent of the interval since it last sent them.
IS-IS	If necessary, temporarily lengthens the hello timers.
LDP	Unified ISSU warns you if the hello timers or the keepalive timers are not long enough to survive the forwarding plane upgrade. LDP sends out hello messages and keepalive messages immediately before and immediately after both the SRP module switchover and the forwarding plane restart, independent of the interval since it last sent them.
OSPF	OSPF timers are not negotiable between peers. Unified ISSU generates a warning if the hello timers or the keepalive timers are not long enough to survive the forwarding plane upgrade. OSPF begins a graceful restart before the SRP module switchover. When you configure graceful restart before the in-service software upgrade, you must ensure that the graceful restart times are long enough to allow recovery. OSPF sends out hello messages and keepalive messages immediately before and immediately after forwarding plane restart, independent of the interval since it last sent them.
PIM	If necessary, temporarily lengthens the hold times in hello messages. PIM guarantees that at least one hello message with a lengthened hold time is sent to each neighbor. If necessary, increases the join-prune hold time. PIM guarantees that at least one join-prune message with a lengthened hold time is sent to each neighbor.
RIP	RIP timers do not affect unified ISSU.
RSVP-TE	If necessary, temporarily lengthens the graceful restart timers to survive the SRP module switchover. If necessary, lengthens the hello timers to survive the forwarding plane upgrade.

You might want some or all traffic to be routed around the upgrading router rather than accept a forwarding loss during the forwarding interruption. To do so, you must configure your routing protocols appropriately. For example, you might raise the link cost in IS-IS and OSPF, causing their neighbors to seek alternate routes that have lower link costs. In PIM, you can set the priority for the router interface to zero to ensure that the upgrading router is not selected as a designated router.

Recommended Routing Protocol Timer Settings

You can use the default values for many of the routing protocol timers with no adverse effect on a unified in-service software upgrade. For other timers, we recommend particular values, as described in Table 50.

Table 50: Recommended Routing Protocol Timer Settings

Protocol	Timers
BFD	Use the default timers.
BGP	Use the default timers, including graceful restart default timers.
DVMRP	Use the default timers.
IGMP	Use the default timers.
IS-IS	Use the default timers, including graceful restart default timers.
LDP	Use the default timers, including graceful restart default timers, except for the following: ■ Set the hello hold time to at least 901 seconds for a helper or a restarter configuration for a link-level adjacency or for LDP targeted sessions.
OSPF	Use the default timers, including graceful restart default timers, except for the dead interval. Set the OSPF dead interval to at least 301 seconds.
PIM	Set the query interval to at least 210 seconds. ISSU generates a warning for any of the following conditions, but you can ignore the warning without causing a higher FC outage: ■ The current router is a DR. ■ The current router is configured as an Auto RP mapping agent and is chosen as the RP for any group. ■ The current router is an elected or candidate BSR, or if BSR candidate RPs are configured. ■ The graceful restart timer is less than the default value, 30 seconds.
RIP	Use the default timers; graceful restart is not supported. For scaled configurations, such as for 2000 RIP interfaces, use the following values: ■ Flush interval: 600 seconds ■ Holddown time: 260 seconds ■ Invalid interval: 260 seconds ■ Update interval: 60 seconds

Table 50: Recommended Routing Protocol Timer Settings (continued)

Protocol	Timers
RSVP-TE	Use the default timers, including graceful restart default timers, except for the following: ■ For graceful restart, the hello timeout interval is the product of hello misses multiplied by the hello refresh interval. Determine which period is longer, the IC upgrade time or the forwarding upgrade time. Configure the hello refresh and hello miss values so that the hello timeout is greater than the longer of those two periods. ■ For node hellos, the product of the refresh misses multiplied by the hello refresh interval must be great than the FC outage time. For an outage time of less than 30 seconds, for example, configure the following values: ■ Set the node hello refresh interval to 8000. ■ Set the node hello refresh misses to 4.

Before You Begin a Unified In-Service Software Upgrade

The following hardware and software prerequisites must be met for the successful completion of unified ISSU. You can issue the **show issu** command to determine whether the routers meets these requirements.

Hardware Requirements for Unified ISSU

- The E120 or E320 router must support unified ISSU.
- Two SRP modules must be installed in the router.
- All installed combinations of line modules and IOAs must support unified ISSU. Unsupported modules that are online are reloaded during the unified ISSU, with consequent loss of connections and traffic forwarding.

  Do not install IOAs in the chassis while the unified ISSU operation is in process.
- The redundant SRP module must have at least 300 MB of free memory. Depending on their configuration, line modules require up to 75 MB of free memory.

For information about modules supported on E120 and E320 routers:

- 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 modules that support unified ISSU.

Software Requirements for Unified ISSU

- The running JUNOSe software release must support unified ISSU.

  You can upgrade to a software version that supports unified ISSU from a software version that does not support unified ISSU only by means of a conventional upgrade. During the conventional upgrade, all line modules are reloaded, all subscribers are dropped, and traffic forwarding is interrupted until the upgrade is completed.

- The armed (upgrade) release must be capable of being upgraded to from the currently running release; it must be higher-numbered than the running release.

- All applications that are configured on the router must support unified ISSU and stateful SRP switchover.

  If one or more unified ISSU-challenged applications are configured and you proceed with a unified in-service software upgrade, the unified ISSU process forces a conventional upgrade on the router. All line modules are reloaded, all subscribers are dropped, and traffic forwarding is interrupted until the upgrade is completed.

  You can avoid this circumstance by removing the configuration for the unified ISSU-challenged applications from the router before you begin the in-service software upgrade.

  See *Application Support for Unified ISSU* on page 412 for information about whether an application supports unified ISSU.

- Stateful SRP switchover must be configured on the router. Use the following commands to configure high availability:

  ```
  host1(config)#redundancy
  host1(config-redundancy)#mode high-availability
  ```

  See *Chapter 7, Managing High Availability* for information about high availability.

The following requirements must be met for traffic forwarding to continue. However, failing to meet these requirements does not halt the unified ISSU operation. The unified ISSU process offers the option to override or ignore these forwarding requirements.

- Graceful restart must be enabled for all configured routing protocols. The unified ISSU operation relies on graceful restart to keep the routing protocols alive through the various stages of the upgrade.

- All connected peers must be configured with graceful restart. Because some protocols cannot themselves confirm peer configuration for graceful restart, you must ensure that the peers are properly configured.

- For applications that exchange keepalive messages with peers, you must ensure that the poll times are adequate to maintain the peering session across any forwarding interruption caused by the unified ISSU operation.

Upgrading Router Software with Unified ISSU

To upgrade your router software by means of unified ISSU, perform the following steps.

1. Disable autosynchronization.

   host1(config)#**disable-autosync**

2. Copy the new release to the router.

NOTE: Be sure to specify the correct software release (.rel) filename for the router you are using, as described in the section *Identifying the Software Release File* in *Chapter 3, Installing JUNOSe Software*.

   host1#**copy /incoming/releases/ftpserver/quebec2.rel R2.rel**

3. Save the current configuration.

   host1#**copy running-configuration** *system2.cnf*

4. Determine whether the router hardware and the software release meet the criteria required for unified ISSU to operate successfully by using one of the following commands:

   host1#**show issu**
   host1#**show issu brief**
   host1#**show issu detail**

5. Arm the primary SRP module with the upgrade release.

   host1#**boot system R2.rel**

NOTE: You must arm any hotfixes that need to be loaded with the new release after you have armed the new release. The hotfixes are supplied when the modules to which they apply are rebooted.

6. Synchronize the NVS file system of the redundant SRP module with that of the primary SRP module.

   host1#**synchronize**

   Because the redundant SRP module is running a different release than the armed release, the module automatically reboots and runs the armed (upgrade) release, R2.rel.

   Wait for the redundant SRP module to boot, initialize, and reach the standby state. At this point, the REDUNDANT LED on the module is illuminated and the ONLINE LED is off. The State field in the **show version** display indicates that the redundant module is in the standby state.

7. Synchronize the file system of the primary module with that of the redundant module.

   The NVS file systems of the two SRP modules are unsynchronized because the redundant SRP module rebooted.

   host1#**synchronize**

8. Reenable autosynchronization.

   host1(config)#**no disable-autosync**

9. Determine whether unified ISSU is in the Idle state and whether all upgrade requirements have been met.

   host1#**show issu**

NOTE: If the results indicate that some requirements are not met, you must correct this situation before proceeding.

10. Ensure that stateful SRP switchover is configured on the router.

    host1#**show redundancy srp**

    If it is not already configured, do so now.

    host1(config)#**redundancy**
    host1(config-redundancy)#**mode high-availability**

11. For each configured protocol on the router and its neighbors, ensure that graceful restart is configured. See the relevant protocol configuration chapters in the JUNOSe document set for information about configuring graceful restart.

12. Begin the initialization phase of the in-service software upgrade.

    host1#**issu initialize**

    The CLI displays the status of the initialization as it proceeds.

13. (Optional) From a different CLI session, display the progress of the initialization.

    host1#**show issu**

    Unified ISSU must be in the Initialized state before you proceed to the next step. The time required for initialization varies with the system load and the complexity of the router configuration.

14. Start the upgrade phase.

    host1#**issu start**

    The router switches to the redundant SRP module running the upgrade release, R2.rel. Significant upgrade milestones are displayed as they occur.

15. When the console indicates that the upgrade is completed, you can verify that the router is back in the idle state and running the upgrade release, R2.rel.

    host1#**show issu**

    You can also verify the status of the SRP modules and line modules, as well as the running and armed releases.

    host1#**show version**

issu initialize

- Use to start the initialization phase of the unified ISSU process.
- This command displays the percentage completion for the process as it takes place.
- Example

  host1#**issu initialize**
  Verifying the ISSU criteria... verified
  Starting the ISSU initializing phase
  Upgrading the standby SRP- This phase can take a long time
  10% completed...

- There is no **no** version.

issu start

- Use to start the upgrade phase of the unified ISSU process after the initialization phase has completed.
- Example

  host1#**issu start**
  Verifying the ISSU criteria... verified
  The system will now enter the upgrading phase. This phase cannot be aborted.
  Do you wish to continue?
  Yes
  Starting the ISSU upgrade phase
  ... Upgrading the line card – Control plane
  ... Upgrading completed
  Switching from primary SRP to the standby SRP
  The system will resume on the SRP in slot 7 in a few minutes.

- There is no **no** version.

issu stop

- Use to gracefully stop a unified in-service software upgrade and place the process in an idle state.
- You can issue this command only when unified ISSU is in the initialized state. You cannot issue this command after you have issued the **issu start** command to begin the upgrade phase of unified ISSU.
- Example

  host1#**issu stop**
  The command will abort the ISSU operation. Do you wish to continue?
  Yes
  Stopping the ISSU upgrade process
  ...reloading standby SRP

- There is no **no** version.

Halting the Unified ISSU Process and Restoring the Original State of the Router

The options that are available to halt the in-service software upgrade depend on the phase that the upgrade is in when you attempt to halt it. The phase also affects the state of the router after the upgrade is halted.

Halting Unified ISSU During Initialization Phase

During the initialization phase, you can halt the unified ISSU process by issuing the **issu stop** command. This action reloads the redundant SRP module with the armed upgrade release. As a result, unified ISSU is placed in the idle state and the following releases are present on the router:

- Primary SRP module—Running (original) release
- Redundant SRP module—Upgrade release
- Line modules—Running (original) release

After you stop unified ISSU, you can return the router to the state it was in when you began the in-service software upgrade. To roll the router back to its beginning state with the redundant SRP module running the original release, you must perform the following steps to arm the redundant SRP module with the running release:

1. Turn off auto synchronization.

   host1(config)#**disable-autosync**

2. Specify that the router use the running release when it reboots.

   host1(config)#**boot system** *erx_x-y-z.rel*

3. Synchronize the NVS file system of the redundant module with that of the primary module.

   host1#**synchronize**

The redundant SRP module automatically reboots because the armed release (the original release) now differs from the software release it is currently running (the upgrade release).

4. Verify that stateful SRP switchover is enabled.

```
host1#show redundancy
```

Halting Unified ISSU During Upgrade Phase

During the upgrade phase—before the line module and control plane software is upgraded—the unified ISSU process provides an opportunity to cancel the upgrade. If you choose to cancel, the router remains in the unified ISSU initialized state. The CLI command set becomes fully accessible.

If you do not cancel at this point, then the process continues and any line modules that do not support unified ISSU are reloaded. Application sessions are brought down and traffic forwarding is interrupted for the unsupported modules.

If you do cancel in response to the CLI prompt, unified ISSU returns to the initialized state, and the following releases are present on the router:

- Primary SRP module—Running (original) release
- Redundant SRP module—Upgrade release; the module is in the unified ISSU initialized state
- Line modules—Running (original) release

To roll back from the unified ISSU initialized state, you must issue the **issu stop** command. The command reloads the redundant SRP module with the armed release and places unified ISSU in the idle state. As a result, the following releases are present on the router:

- Primary SRP module—Running (original) release
- Redundant SRP—Upgrade release
- Line modules—Running (original) release

After you stop unified ISSU, you can return the router to the state it was in when you began the in-service software upgrade. To roll the router back to its beginning state with the redundant SRP module running the original release, you must perform the following steps to arm the redundant SRP module with the running release:

1. Turn off auto synchronization.

   host1(config)#**disable-autosync**

2. Specify that the router use the running release when it reboots. For

   host1(config)#**boot system** *erx_x-y-z.rel*

3. Synchronize the NVS file system of the redundant module with that of the primary module.

   host1#**synchronize**

   The redundant SRP module automatically reboots because the software release that it is configured to run now differs from the software release it is running.

Monitoring a Unified In-Service Software Upgrade

You can use the **show issu** command to monitor the status of the router with regard to a unified in-service software upgrade.

show issu

- Use to display information about the current status of the router relative to a unified in-service software upgrade and of the upgrade itself.
- Field descriptions
  - ISSU state—State of the upgrade process, idle, initializing, initialized, or upgrading
  - ISSU description—State of the upgrade, including percent complete
  - criteria met—Whether prerequisites for the upgrade have been met and, generally, what errors occurred
  - running release—Filename of JUNOSe software release that is currently running on the SRP modules
  - armed release—Filename of JUNOSe software release that is armed to become the next running release when the router reboots
- Example 1—Displays the current unified ISSU state and identifies the active and armed releases

```
host1#show issu brief

ISSU state:       initializing
ISSU description: ISSU initialize is in-progress, 5% complete
criteria met:     No, upgrade error(s) found
running release:  release1.rel
armed release:    release2.rel
```

- Example 2—To the information displayed by **show issu brief**, adds a summary table of unified ISSU verification criteria

```
host1#show issu

ISSU state:       idle
ISSU description: ISSU is currently idle
criteria met:     No, upgrade error(s) found
running release:  release1.rel
armed release:    release2.rel

#                  ISSU Activation Criteria Summary                    Met
--   ------------------------------------------------------------   -----------
1    In-Service Software Upgrade ready?                             Yes
2    High-Availability ready?                                       No
3    Line modules ready?                                            Conditional
```

```
4    Configuration conversion support ready?                    Yes
5    CLI sessions ready?                                        Yes
6    Routing applications ready?                                Yes
7    Protocol timers ready?                                     Yes
```

- Example 3—To the information displayed by **show issu**, adds a detailed table of unified ISSU verification criteria that lists mandatory and conditional criteria that have not been met, the impact of this status, and the remedy as reported by router applications and system components that participate in the in-service software upgrade

```
host1#show issu detail

ISSU state:       idle
ISSU description: ISSU is currently idle
criteria met:     No, upgrade error(s) found
running release:  release1.rel
armed release:    release2.rel

#                  ISSU Activation Criteria Summary                  Met
--   ------------------------------------------------------------   -----------
1    In-Service Software Upgrade ready?                             Yes
2    High-Availability ready?                                       No
3    Line modules ready?                                            Conditional
4    Configuration conversion support ready?                        Yes
5    CLI sessions ready?                                            Yes
6    Routing applications ready?                                    Yes
7    Protocol timers ready?                                         Yes

#                      ISSU Criterion Detail                         Met
--   ------------------------------------------------------------   -----------
1    In-Service Software Upgrade ready?                             Yes
2    High-Availability ready?                                       No
->   Problem: The standby SRP must not be running the same releas   No
     e
    Reporting Slot: 6
     Impact: ISSU cannot be performed
     Remedy: boot a release compatible with ISSU on the standby S
     RP
3    Line modules ready?                                            Conditional
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 1, OC3/OC12/DS3-ATM, requires at least 256 MB
    Reporting Slot: 6
     Impact: If you continue, the card will immediately be reset
     and then cold started when ISSU Upgrade completes
     Remedy: data unavailable
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 8, CT3-12, requires at least 256 MB
    Reporting Slot: 6
     Impact: If you continue, the card will immediately be reset
     and then cold started when ISSU Upgrade completes
     Remedy: data unavailable
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 9, CT3-12, requires at least 256 MB
    Reporting Slot: 6
     Impact: If you continue, the card will immediately be reset
     and then cold started when ISSU Upgrade completes
     Remedy: data unavailable
->   Problem: Card does not support required memory configuration   Conditional
     : Slot 10, CT3-12, requires at least 256 MB
```

```
     Reporting Slot: 6
      Impact: If you continue, the card will immediately be reset
      and then cold started when ISSU Upgrade completes
      Remedy: data unavailable
->   Problem: Card not disabled or not online: Slot 1, OC3/OC12/D   Conditional
     S3-ATM, 0/0
     Reporting Slot: 6
      Impact: If you continue, the card will immediately be reset
      and then cold started when ISSU Upgrade completes
      Remedy: If not standby, Wait for card to come online before
      proceeding
->   Problem: Card not disabled or not online: Slot 8, CT3-12, 0/   Conditional
     0
     Reporting Slot: 6
      Impact: If you continue, the card will immediately be reset
      and then cold started when ISSU Upgrade completes
      Remedy: If not standby, Wait for card to come online before
      proceeding
4    Configuration conversion support ready?                       Yes
5    CLI sessions ready?                                           Yes
6    Routing applications ready?                                   Yes
7    Protocol timers ready?                                        Yes
```

Chapter 9

Passwords and Security

Passwords and security are of utmost importance for the security of your router. This chapter provides the information you need to configure your E-series router to be secure for all levels of users.

This chapter contains the following sections:

- Overview on page 441
- Platform Considerations on page 442
- Setting Basic Password Parameters on page 442
- Setting and Erasing Passwords on page 445
- Vty Line Authentication and Authorization on page 451
- Virtual Terminal Access Lists on page 458
- Secure System Administration with SSH on page 459
- Restricting User Access on page 470
- Denial of Service (DoS) Protection on page 474

Overview

One of your major management responsibilities is to secure your router. To do this, assign passwords or secrets to the router. In Global Configuration mode, you can set passwords or secrets to prevent unauthorized users from accessing the router in Privileged Exec mode.

Passwords and secrets have the same degree of security on your router, and they are used interchangeably. You can define either a password or a secret for your router, but not both.

Platform Considerations

Passwords and security are supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Setting Basic Password Parameters

This section shows how to set up basic passwords and secrets on your router. You cannot create your own encrypted passwords and secrets. You must use encrypted passwords and secrets that the router generates.

NOTE: See *Setting and Erasing Passwords* on page 445 for additional commands for erasing and monitoring passwords.

Creating Encrypted Passwords

This example encrypts password *t1meout1* and creates a password for privilege level 10.

1. Enable and configure the password. The **0** keyword specifies that you are entering an unencrypted password.

   host1(config)#**enable password level 10 0 t1meout1**

2. Display the encrypted password.

```
host1(config)#exit
host1#show secret
                Current Password Settings
                -------------------------
          encryption          encrypted
level        type           password/secret          mode
-----   ------------   --------------------   ----------
0
1
2
3
4
5
6
7
8
9
10      7 (password)   dq]XG`,%N"SS7d}o)_?Y   configured
11      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
12      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
```

```
13      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
14      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
15      7 (password)   dq]XG`,%N"SS7d}o)_?Y   inherited
```

You or users with high privilege levels can now use the encrypted password, *dq]XG`,%N"SS7d}o)_?Y*, with the **password** command.

Creating Secrets

This example generates a secret for the password *rocket*, and creates a secret for privilege level 15.

1. Enable and configure the secret. The **0** keyword specifies that you are entering an unencrypted secret.

   host1(config)#**enable secret level 15 0 rocket**

2. Display the secret.

```
host1(config)#exit
host1#show secret
              Current Password Settings
              -------------------------
        encryption        encrypted
level      type        password/secret         mode
-----   ----------   --------------------   ----------
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15      5 (secret)   bcA";+1aeJD8)/[1ZDP6   configured
```

You or users with high privilege levels can now use the encrypted password, *bcA";+1aeJD8)/[1ZDP6*, with the **password** command.

Encrypting Passwords in Configuration File

You can also direct the system software to encrypt passwords saved in the configuration file by using the **service password-encryption** command. This command is useful to keep unauthorized individuals from viewing your password in your configuration file. It is important to remember that this command uses a simple cipher and is not intended to protect against serious analysis. You can tell if a string is encrypted if it is preceded by an 8.

Commands and Guidelines

Use the following commands and guidelines to set passwords or secrets for the privilege levels.

enable password

- Use to set a password, which controls access to Privileged Exec mode and some configuration modes.
- Enter the password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted.
- The first time you define a password, you must enter it in plain text. To view its encrypted form, use the **show config** display. To redefine the password at a later date, you can enter the password in its encrypted form.
- You can use the following keywords:
  - **0** (zero)—Specifies an unencrypted password
  - **7**—Specifies an encrypted password
- Example 1 (unencrypted password)

  host1(config)#**enable password 0 mypassword**

- Example 2 (encrypted password)

  host1(config)#**enable password 7 x13_2**

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

enable secret

- Use to set a secret, which controls access to the Privileged Exec mode and some configuration modes.
- Enter the secret in plain text (its unencrypted form) or cipher text (its encrypted form). In either case, the system stores the secret as encrypted.
- The first time you define a secret, you must enter it in plain text. To view its encrypted form, use the **show config** display. To redefine the secret at a later date, you can enter the secret in its encrypted form.
- You can use the following keywords:
  - **0** (zero)—Specifies an unencrypted secret
  - **5**—Specifies an encrypted secret
- Example 1 (unencrypted secret)

  host1(config)#**enable secret 0 yalta45**

- Example 2 (encrypted secret)

  host1(config)#**enable secret 5 y13_x**

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

service password-encryption

- Use to encrypt passwords that are saved in the system's configuration file. The command converts plain text to cipher text. The default is no encryption.
- Use of this command prevents casual observers from viewing passwords, for example, in data obtained from **show config** displays. The command is not intended to provide protection from serious analysis.
- This command does *not* apply to passwords set with **enable secret**, **enable password**, or **password** (Line Configuration mode).
- This command does apply to authentication key passwords and BGP neighbor passwords.
- Example

  host1(config)#**service password-encryption**

- Use the **no** version to remove the encryption assignment.

Setting and Erasing Passwords

You can set the following passwords:

- Enable passwords that control access to different groups of commands.
- A console password that controls access to the console.
- Passwords for individual vty lines or groups of vty lines.

Privilege Levels

Different groups of commands are associated with privilege levels (Table 51). You can set enable passwords to allow users to access commands at different privilege levels.

Table 51: Commands Available at Different Privilege Levels

Privilege Level	Commands Available
0	**help**, **exit**, **enable**, and **disable** commands
1	User Exec commands plus commands at level 0
5	Privileged Exec **show** commands plus commands at levels 0 and 1
10	All commands except support commands
15	Support commands that Juniper Networks Technical Support may provide and all other commands

To maximize security and usability, set different passwords for levels 1, 5, 10, and 15. By default, no **enable** passwords exist.

Accessing Privilege Levels

If users have access to the console, they automatically have access to privilege level 0. To access higher levels of privilege, they must enter the **enable** *privilege-level* command. When users specify a privilege level, the system determines whether there is a password at that level. If there is not, the system prompts the user for the password for the lower level closest to the requested level.

Setting Enable Passwords

To set up enable passwords, use the commands described in *Setting Basic Password Parameters* on page 442.

Erasing Enable Passwords

If you forget an e**nable** password or secret, you can erase all **enable** passwords and secrets.

Two commands allow you to erase passwords and secrets: **erase secrets** and **service unattended-password-recovery.** It is important to fully understand the purpose of these commands and how they work with each other.

The **erase secrets** command can be used to delete all existing passwords. To use this command, you must be physically present at the router to complete the operation. After the command has been executed, you have a finite number of seconds to press the software reset button on the SRP module. You can execute this command from the console or any vty.

The **service unattended-password-recovery** command provides you with a way to delete existing passwords and secrets without physically being present at the router. You must have the proper privilege level to execute the command, and you can execute it from either the console or any vty.

When you execute **service unattended-password-recovery**, you change the behavior of **erase secrets**. You can now delete passwords and secrets from the console by executing **erase secrets** without a time restraint or having to be physically present at the router. When you use the **no** version of **service unattended-password-recovery**, you revert the functionality of erase secrets to the factory default setting.

To erase all enable passwords or secrets:

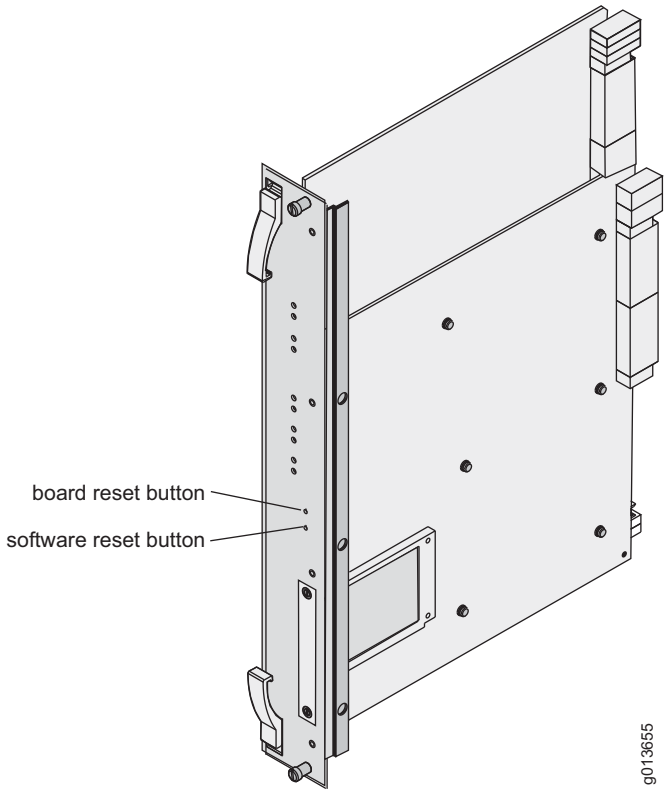
1. Log in to the router.

2. Erase the existing enable password or secret. Specify the number of seconds to allow for the erase operation.

   ```
   host1>erase secrets 60
   ```

3. Within the time limit that you specified for the **erase secrets** command, press the recessed software reset button on the primary SRP module (see Figure 28 on page 447).

Figure 28: Location of the Software Reset Button



NOTE: If you do not press the software reset button within the time limit, the system will not erase the password, and you will need to repeat the process.

erase secrets

- Use to delete all CLI passwords and secrets.
- After you issue this command, press the software reset button (see Figure 28) within the time you specify for this command.
- Allows you to set the number of seconds (1–60) for this procedure to be accomplished.
- Allows you to set a new password when you have forgotten your password.
- Can be used with the **service unattended-password-recovery** command.
- Example

  host1>**erase secrets 60**

- There is no **no** version.

service unattended-password-recovery

- Use to allow you to delete all passwords and secrets from the console without being physically present at the router.
- When executed, this command changes the behavior of the **erase secrets** command, which will not take any parameters and will not be available through a vty session.
- Example

  host1(config)#**service unattended-password-recovery**

- Use the **no** version to revert **erase secrets** to factory default settings.

Setting a Console Password

By default, there is no console password. To set a console password:

1. Make sure that you know the enable password for the system.

   If you need to reset the enable password, see *Privilege Levels* on page 445.

2. Access Privileged Exec mode, and enter the enable password if prompted.
3. Access Global Configuration mode.
4. Access Line Configuration mode.

   host1(config)#**line console 0**

5. Enable password checking at login.

   host1(config-line)#**login**

6. Specify a password.

   host1(config-line)#**password 7 dq]XG`,%N"SS7d}o)_?Y**

line

- Use to specify the vty lines or the console.
- Example

  host1(config)#**line vty 1 4**

- Use the **no** version to remove a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

login

- Use to enable password checking at login.
- The default setting is to enable a password.
- Example

```
host1(config)#line vty 1 4
host1(config-line)#login
```

- Use the **no** version to disable password checking and allow access without a password.

password

- Use to specify a password on the console, a line, or a range of lines.
- If you enable password checking, but do not configure a password, the system will not allow you to access virtual terminals.
- Use the following keywords to specify the type of password you will enter:
  - **0** (zero)—Unencrypted password
  - **5**—Secret
  - **7**—Encrypted password

NOTE: To use an encrypted password or a secret, you must follow the procedure in *Setting Basic Password Parameters* on page 442 to obtain the encrypted password or secret. You cannot create your own encrypted password or secret; you must use a system-generated password or secret.

- Example 1 (unencrypted password)

```
host1(config-line)#password 0 mypassword
```

- Example 2 (secret)

```
host1(config-line)#password 5 bcA";+1aeJD8)/[1ZDP6
```

- Example 3 (encrypted password)

```
host1(config-line)#password 7 dq]XG`,%N"SS7d}o)_?Y
```

- Use the **no** version to remove the password. By default, no password is specified.

Erasing the Console Password

If you forget the console password, you can erase the existing value and configure a new one. This action deletes all authentication for the console line. To erase existing passwords:

1. Reboot the router by pressing the recessed software reset button on the primary SRP module (see Figure 28 on page 447) and then pressing the mb key sequence during the countdown.

2. Disable authentication at the console level.

   :boot##**disable console authentication**

   If you remember the password at this point, you can override this action by entering:

   :boot##**no disable console authentication**

3. Reload the operating system.

   :boot##**reload**

When the operating system reloads, you can access the console without a password.

NOTE: You will be able to log in to the console without a password until you set a new password.

Monitoring Passwords

You can use the **show secrets** command to view all current passwords and secrets.

show secrets

- Use to display all passwords and secrets.
- Passwords and secrets appear in their encrypted form.
- In the mode column, *inherited* indicates whether a secret was inherited from a lower password level. The **show secrets** command displays only secrets configured by the user; it does not display inherited secrets.
- Example

```
host1#show secrets
                Current Password Settings
                -------------------------
         encryption          encrypted
level       type          password/secret          mode
-----   ------------   --------------------   ----------
0
1
2
3
4
5       7 (password)   zRFj_6>^]1OkZR@e!|S$   configured
6       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
7       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
```

```
8       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
9       7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
10      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
11      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
12      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
13      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
14      7 (password)   zRFj_6>^]1OkZR@e!|S$   inherited
```

Vty Line Authentication and Authorization

The router supports 30 virtual tty (vty) lines for Telnet, Secure Shell Server (SSH) and FTP services. Each Telnet, SSH, or FTP session requires one vty line. You can add security to your router by configuring the software to validate login requests. There are two modes of authentication for a vty line:

- Simple authentication—Password-only authentication through the local configuration
- AAA authentication—Username and password authentication through a set of authentication servers

You can enable AAA authorization, which allows you to limit the services available to a user. Based on information retrieved from a user's profile, the user is either granted or denied access to the requested server.

Configuring Simple Authentication

To configure simple authentication:

1. Specify a vty line or a range of vty lines on which you want to enable the password.

   host1(config)#**line vty 8 13**
   host1(config-line)#

2. Specify the password for the vty lines.

   host1(config-line)#**password 0 mypassword**

3. Enable login authentication on the lines.

   host1(config-line)#**login**

4. Display your vty line configuration.

   host1#**show line vty 8**
   no access-class in
   data-character-bits 8
   exec-timeout never
   exec-banner enabled
   motd-banner enabled
   login-timeout 30 seconds

line

- Use to specify the vty line(s) on which you want to enable the password.
- You can set a single line or a range of lines. The range is 0–29.
- Example

  host1(config)#**line vty 8 13**

- Use the **no** version to remove a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

login

- Use to enable password checking at login.
- The default setting is to enable a password.
- Example

  host1(config-line)#**login**

- Use the **no** version to disable password checking and allow access without a password.

password

- Use to specify a password on a single line or a range of lines.
- If you enable password checking but do not configure a password, the system will not allow you to access virtual terminals.
- Specify a password in plain text (unencrypted) or cipher text (encrypted). In either case, the system stores the password as encrypted.
- Use the following keywords to specify the type of password you will enter:
  - **0** (zero)—Unencrypted password
  - **5**—Secret
  - **7**—Encrypted password

NOTE: To use an encrypted password or a secret, you must follow the procedure in *Setting Basic Password Parameters* on page 442 to obtain the encrypted password or secret. You cannot create your own encrypted password or secret; you must use a system-generated password or secret.

- Example 1 (unencrypted password)

  host1(config-line)#**password 0 mypassword**

- Example 2 (secret)

  host1(config-line)#**password 5 bcA";+1aeJD8)/[1ZDP6**

- Example 3 (encrypted password)

  host1(config-line)#**password 7 dq]XG`,%N''SS7d}o)_?Y**

- Use the **no** version to remove the password. By default, no password is specified.

show line vty

- Use to display the configuration of a vty line.
- Field descriptions
  - access-class—Access-class associated with the vty line
  - data-character-bits—Number of bits per character
    - 7—Setting for the standard ASCII set
    - 8—Setting for the international character set
  - exec-timeout—Time interval that the terminal waits for expected user input
    - Never—Indicates that there is no time limit
  - exec-banner—Status for the exec banner: enabled or disabled. This banner is displayed by the CLI after user authentication (if any) and before the first prompt of a CLI session.
  - motd-banner—Status for the message of the day (MOTD) banner: enabled or disabled. This banner is displayed by the CLI when a connection is initiated.
  - login-timeout—Time interval during which the user must log in.
    - Never—Indicates that there is no time limit
- Example

```
host1#show line vty 0
no access-class in
data-character-bits 8
exec-timeout 3w 3d 7h 20m 0s
exec-banner enabled
motd-banner enabled
login-timeout 30 seconds
```

Configuring AAA Authentication and AAA Authorization

Before you configure AAA authentication and AAA authorization, you need to configure a RADIUS and/or TACACS+ authentication server. Note that several of the steps in the configuration procedure are optional.

To configure AAA new model authentication and authorization for inbound sessions to vty lines on your router:

1. Specify AAA new model authentication.

   host1(config)#**aaa new-model**

2. Create an authentication list that specifies the type(s) of authentication methods allowed.

   host1(config)#**aaa authentication login my_auth_list tacacs+ line enable**

3. (Optional) Specify the privilege level by defining a method list for authentication.

   host1(config)**aaa authentication enable default tacacs+ radius enable**

4. (Optional) Enable authorization, and create an authorization method list.

   host1(config)**aaa authorization commands 15 boston if-authenticated tacacs+**

5. (Optional) Disable authorization for all Global Configuration commands.

   host1(config)#**no aaa authorization config-commands**

6. Specify the range of vty lines.

   host1(config)#**line vty 6 10**
   host1(config-line)#

7. (Optional) Apply an authorization list to a vty line or a range of vty lines.

   host1(config-line)#**authorization commands 15 boston**

8. Specify the password for the vty lines.

   host1(config-line)#**password xyz**

9. Apply the authentication list to the vty lines you specified on your router.

   host1(config-line)#**login authentication my_auth_list**

aaa authentication enable default

- Use to allow privilege determination to be authenticated through the TACACS+ or RADIUS server. This command specifies a list of authentication methods that are used to determine whether a user is granted access to the privilege command level.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs+**, **none**, and **enable**.
- To specify that the authentication should succeed even if all methods return an error, specify **none** as the final method in the command line.
- Requests sent to a TACACS+ or RADIUS server include the username that is entered for login authentication.
- If the authentication method list is empty, the local **enable** password is used.
- Example

  host1(config)#**aaa authentication enable default tacacs+ radius**

- Use the **no** version to empty the list.

aaa authentication login

- Use to set AAA authentication at login. This command creates a list that specifies the methods of authentication.
- After you have specified **aaa new-model** as the authentication method for vty lines, an authentication list called "default" is automatically assigned to the vty lines. To allow users to access the vty lines, you must create an authentication list and either:
  - Name the list "default."
  - Assign a different name to the authentication list, and assign the new list to the vty line using the **login authentication** command.
- The authentication methods that you can use in a list include these options: **radius**, **line**, **tacacs+**, **none**, and **enable**.
- The system traverses the list of authentication methods to determine whether a user is allowed to start a Telnet session. If a specific method is available but the user information is not valid (such as an incorrect password), the system does not continue to traverse the list and denies the user a session.
- If a specific method is unavailable, the system continues to traverse the list. For example, if **tacacs+** is the first authentication type element on the list and the TACACS+ server is unreachable, the system attempts to authenticate with the next authentication type on the list, such as **radius**.
- The system assumes an implicit denial of service if it reaches the end of the authentication list without finding an available method.
- Example

  host1(config)#**aaa authentication login my_auth_list tacacs+ radius line none**

- Use the **no** version to remove the authentication list from your configuration.

aaa authorization

- Use to set the parameters that restrict access to a network.
- Use the keyword **exec** to determine if the user is allowed to run Exec mode commands. The commands that you can execute from Exec mode provide only user-level access.
- Use the keyword **commands** to run authorization for all commands at the specified privilege level (0–15). See Table 51 on page 445 for a description of privilege levels.
- You can enter up to three authorization types to use in an authorization method list. Options include: **if-authenticated, none**, and **tacacs+**.

NOTE: For information about TACACS+, see *JUNOSe Broadband Access Configuration Guide, Chapter 9, Configuring TACACS+*.

- Authorization method lists define the way authorization is performed and the sequence in which the methods are performed. You can designate one or more security protocols in the method list to be used for authorization. If the initial method fails, the next method in the list is used. The process continues until either there is successful communication with a listed authorization method or all methods defined are exhausted.
- Example

  host1(config)#**aaa authorization exec**

- Use the **no** version to delete the method list.

aaa authorization config-commands

- Use to reestablish the default created when the **aaa authorization commands** command was issued.
- After the **aaa authorization commands** command has been issued, **aaa authorization config-commands** is enabled by default, which means that all configuration commands are authorized.
- Example

  host1(config)#**aaa new-model**
  host1(config)#**aaa authorization command 15 parks tacacs+ none**
  host1(config)#**no aaa authorization config-commands**

- Use the **no** version to disable AAA configuration command authorization.

aaa new-model

- Use to specify AAA new model as the authentication method for the vty lines on your router.
- If you specify AAA new model and you do not create an authentication list, users will not be able to access the router through a vty line.
- Example

  host1(config)#**aaa new-model**

- Use the **no** version to restore simple authentication.

authorization

- Use to apply AAA authorization to a specific vty line or group of lines.
- Use the **exec** keyword to apply this authorization to CLI access in general.
- Use the **commands** keyword to apply this authorization to user commands of the privilege level you specify.
- You can specify the name of an authorization method list; if no method list is specified, the default is used.
- After you enable the **aaa authorization** command and define a named authorization method list (or use the default method list) for a particular type of authorization, you must apply the defined list to the appropriate lines for authorization to take place.
- Example

  host1(config)#**line vty 6**
  host1(line-config)#**authorization commands 15 sonny**

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

line

- Use to specify the virtual terminal lines.
- You can set a single line or a range of lines. The range is 0–29.
- Example

  host1(config)#**line vty 6 10**

- Use the **no** version to remove a vty line or a range of lines from your configuration; users will not be able to run Telnet, SSH, or FTP to lines that you remove. When you remove a vty line, the system removes all lines above that line. For example, **no line vty 6** causes the system to remove lines 6 through 29. You cannot remove lines 0 through 4.

login authentication

- Use to apply an authentication list to the vty lines you specified on your router.
- Example

  host1(config-line)#**login authentication my_auth_list**

- Use the **no** version to specify that the system should use the default authentication list.

password

- Use to specify a password on a line or a range of lines if you specified the line option with the **aaa authentication login** command.
- If you enable password checking but do not configure a password, the system will not allow you to access virtual terminals.

- Use the following keywords to specify the type of password you will enter:
  - **0** (zero)—Unencrypted password
  - **5**—Secret
  - **7**—Encrypted password

NOTE: To use an encrypted password or a secret, you must follow the procedure in *Setting Basic Password Parameters* on page 442 to obtain the encrypted password or secret. You cannot create your own encrypted password or secret; you must use a system-generated password or secret.

- Example 1 (unencrypted password)

  host1(config-line)#**password 0 mypassword**

- Example 2 (secret)

  host1(config-line)#**password 5 bcA";+1aeJD8)/[1ZDP6**

- Example 3 (encrypted password)

  host1(config-line)#**password 7 dq]XG`,%N"SS7d}o)_?Y**

- Use the **no** version to remove the password. By default, no password is specified.

Virtual Terminal Access Lists

You can provide additional security for your router by using access lists to restrict access to vty lines.

When the router attempts to authenticate a user, it always selects the first vty line that has an access class that permits that user's host. The vty line's configuration must authenticate the user to allow access. Otherwise, the user can never gain access. Consequently, we recommend that you use identical authentication configurations for all vtys that have the same access class list.

To set up access lists:

- Associate the access list with inbound Telnet sessions.

  host1(config)#**line vty 12 15**
  host1(config-line)#**access-class boston in**

- Configure an access list.

  host1(config)#**access-list boston permit any**

access-class in

- Use to associate the access list with vty lines.
- Example—This example sets the virtual terminal lines to which you want to restrict access and specifies an access class to grant access to incoming requests.

  host1(config)#**line vty 12 15**
  host1(config-line)#**access-class boston in**

- Use the **no** version to remove access restrictions.

access-list

- Use to configure an access list.
- Example

  host1(config)#**access-list boston permit any**

- Use the **no** version to remove the access list.

Secure System Administration with SSH

The system supports the SSH protocol version 2 as a secure alternative to Telnet for system administration.

NOTE: Versions earlier than 2.0.12 of the SSH protocol client are not supported. The SSH server embedded within the router recognizes SSH clients that report an SSH protocol version of 1.99, with the expectation that such clients are compatible with SSH protocol version 2.0. Clients that report an SSH protocol version of 1.99 apparently do so to determine the protocol version supported by the server.

SSH provides the following major features:

- Server authentication through a Diffie-Hellman key exchange—Protects against hackers interjecting mimics to obtain your password. You can be confident that you are connected to your own router.
- User authentication—Ensures that the router is allowing connection from a permitted host and remote user.

NOTE: Digital Signature Standard (DSS) public key user authentication for SSH is not supported. RADIUS password authentication is the only method of user authentication currently supported. It is enabled by default. If RADIUS authentication is disabled, then all SSH clients that pass protocol negotiation are accepted.

- Data encryption and key-protected hashing—Provides a secure, trustable session to the upper-layer user interface. Encryption provides confidentiality by preventing unauthorized persons from listening in on management traffic. Encryption and hashing ensure data integrity to obstruct man-in-the-middle attacks, in which unauthorized persons access messages and modify them without detection.

Transport

The SSH transport layer handles algorithm negotiation between the server and client over TCP/IP. Negotiation begins when the SSH client and server send each other textual information that identifies their SSH version. If they both agree that the versions are compatible, the client and server exchange lists that specify the algorithms that they support for key exchange, encryption, data integrity through a message authentication code (MAC), and compression. Each party sends two lists. One list has the algorithms supported for transmission; the other has the algorithms supported for receipt. The algorithms are specified in order of preference in each list. The client and server use the algorithm for each process that matches the client's highest preference and is supported by the server. If no intersection is found, the negotiation attempt fails and the connection is terminated.

If algorithm negotiation is successful, the server sends its public host key to the client for authentication so the client can be certain that it is connected to the intended host rather than to an imposter. The client compares the key to its host key database. The client authenticates the server if the key is found in the database. If the key is not present, then the client can accept or reject this new, unknown key depending on how you have configured the client. For more information, see *Host Key Management* on page 461.

When the client authenticates the server's host key, it begins the transport key exchange process by sending the key data required by the negotiated set of algorithms. The server responds by sending its own key data set. If both sides agree that the keys are consistent and authentic, the keys are applied so that all subsequent messages between client and server are encrypted, authenticated, and compressed according to the negotiated algorithms.

User Authentication

User authentication begins after the transport keys are applied. The client typically asks the server which authentication methods it supports. The server responds with a list of supported methods with no preference.

The client specifies a user authentication method. If the chosen method is supported by the server, the client then challenges the user—that is, the client prompts the user for a password or public-key pass phrase. The client sends the challenge response from the user and the username to the server. The server authenticates the user based on this response.

The system software currently supports only RADIUS password authentication, which is enabled by default. The RADIUS server validates the username and password from its database. If user authentication is disabled, then all SSH clients that pass protocol negotiation are accepted.

Connection

The SSH connection layer creates the user session when the user is authenticated. The server waits for a connection request. The router currently supports only shell requests, which the server interprets as a request for entry into a CLI session. The server ignores any other requests, such as X11 or TCP/IP tunneling.

Key Management

The E-series router implementation of SSH provides for management of user keys and host keys.

User Key Management

Key administration is still under development for the server environment.

Host Key Management

You create a host key for the SSH server with the **crypto key generate dss** command. If a host key already exists, this command replaces it with a new key and terminates all ongoing SSH sessions. Any SSH clients that previously accepted the old host key reject the new key the next time the client and server connect. The client then typically instructs the end user to delete the locally cached host key and to try to connect again.

CAUTION: Use caution issuing the **crypto key generate dss** command from an SSH client. Issuing this command will terminate that SSH session; it will be the last command you send from that session.

The public half of the host key is sent from the server to the client as part of the transport layer negotiation. The client attempts to find a match for this key with one stored locally and assigned to the server. If the client does not find a match, it can accept or reject the key sent from the server. Refer to your client documentation for detailed information. You typically configure the client to do one of the following:

- Never accept an unknown key.
- Always accept an unknown key.
- Query the administrator before accepting an unknown key.

If you do not want the client ever to trust the server when it sends an unknown key, you must manually copy—using the **copy** command—the host key from each server to each intended client. This is the only way to be certain that each client has a local copy of the necessary keys for matching during negotiation.

If you configure the client to accept unknown keys—either automatically or with administrator approval—this acceptance policy applies only to the first time the client receives a key from a particular server. When the SSH client accepts a host key, it stores the key locally and uses it for all future comparisons with keys received from that host. If the client subsequently receives a different key—a new unknown—from that server, it is rejected.

You cannot configure an SSH client to accept a new key after it has accepted a key from an SSH server. You must delete the old key before a new key can be accepted.

Performance

Generating a host key is computationally intensive and can take up to several minutes depending on the load of the system. The system cannot accept any CLI inputs from that session while it is generating the key.

Encryption, data integrity validation, and compression are all computationally intensive. These features can affect router performance in the following ways:

- Reduce the effective baud rate compared with Telnet or the local CLI. Users are unlikely to notice this performance degradation because user interaction is inherently slow compared with other system operations.
- Increase the general load on the system CPU.

Security Concerns

You might be concerned about security with the current support of SSH for the following reasons:

- Only RADIUS user authentication is supported. If you disable user authentication, all users are accepted if the client and server successfully complete negotiation.
- Because the load on the system CPU increases with use of SSH, you might be concerned about denial-of-service attacks. However, the forwarding engine takes care of this issue, because it limits the rate at which it sends packets to the system controller. A flood of packets from a packet generator does not cause problems regardless of whether SSH is enabled.

Before You Configure SSH

You must obtain and install a commercial SSH client on the host from which you want to administer the system. Versions earlier than 2.0.12 of the SSH client are not supported.

Determine your Telnet policy before you configure SSH on your system. Effective use of SSH implies that you should severely limit Telnet access to the system. To limit Telnet access, create access control lists that prevent almost all Telnet usage, permitting only trusted administrators to access the system through Telnet. For example, you might limit access to administrators who need to Telnet to the system from a remote host that does not have the SSH client installed.

You must install and configure a RADIUS server on a host machine before you configure SSH on your router. Refer to your RADIUS server documentation for information about choosing a host machine and installing the server software. You must also configure the RADIUS client on your router. See *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access* for more information.

SSH Configuration Tasks

You configure SSH on individual virtual routers, rather than on the global system. To configure SSH:

1. Access the context of the virtual router.
2. Configure encryption.(Optional)
3. Configure user authentication, including connection parameters.
4. Configure message authentication.(Optional)
5. Enable SSH.
6. Display SSH to verify configuration.

Configuring Encryption

The embedded SSH server and external SSH client maintain separate lists of the encryption algorithms that each supports. Lists are kept for inbound and outbound algorithms. For the server:

- Inbound means the algorithms that the server supports for information coming in from a client.
- Outbound means the algorithms that the server supports for information it sends out to a client.

You must configure each list separately. By default, all of the supported encryption algorithms are available. You need to configure encryption only if you need to specifically remove or add any supported algorithm from the list. Refer to your SSH client documentation for details on configuring encryption on your client. The system supports the following SSH algorithms for encryption:

- 3des-cbc—A triple DES block cipher with 8-byte blocks and 24 bytes of key data. The first 8 bytes of the key data are used for the first encryption, the next 8 bytes for the decryption, and the following 8 bytes for the final encryption.
- blowfish-cbc—A block cipher with 8-byte blocks and 128-bit keys that provides strong encryption and is faster than DES.
- twofish-cbc—A block cipher with 16-byte blocks and 256-bit keys that is stronger and faster than Blowfish encryption.

Although it is not recommended, you can also specify **none**. In this case, the system does not perform encryption.

ip ssh crypto

- Use to add an encryption algorithm to the specified support list for the SSH server.

  Example 1—This example adds the blowfish-cbc algorithm to the list of supported inbound algorithms.

  host1(config)#**ip ssh crypto client-to-server blowfish-cbc**

  Example 2—This example removes the 3des-cbc algorithm from the list of supported outbound algorithms.

  host1(config)#**ip ssh crypto server-to-client no 3des-cbc**

- The **default** version restores the specified list to the factory default, which includes all supported algorithms (3des-cbc, twofish-cbc, and blowfish-cbc). The default list does not include the **none** option.

  Example

  host1(config)#**ip ssh crypto server-to-client default 3des-cbc**

- If you do not specify a direction (client-to-server or server-to-client), the command applies the algorithm to both inbound and outbound lists.
- Use the **no** version to remove or exclude an algorithm from the specified list.

Configuring User Authentication

The router supports RADIUS for user authentication. RADIUS authentication is enabled by default. You must have previously configured a RADIUS server on a host machine and the RADIUS client on your system.

You can specify timeout and retry limits to control the SSH connection process. The limits apply only from the time the user first tries to connect until the user has been successfully authenticated. The timeout limits are independent of any limits configured for virtual terminals (vtys). The following limits are supported:

- SSH timeout—Maximum time allowed for a user to be authenticated, starting from the receipt of the first SSH protocol packet.
- Authentication retry—Number of times a user can try to correct incorrect information—such as a bad password—in a given connection attempt.
- Sleep—Prevents a user that has exceeded the authentication retry limit from connecting from the same host within the specified period.

ip ssh authentication-retries

- Use to set the number of times that a user can retry a failed authentication, such as trying to correct a wrong password. The SSH server terminates the connection when the limit is exceeded.
- Specify an integer from 0–20.
- Example

  host1(config)#**ip ssh authentication-retries 3**

- Use the **no** version to restore the default value, 20 retry attempts.

ip ssh disable-user-authentication

- Use to disable RADIUS password authentication. If you disable RADIUS authentication, all SSH clients that pass protocol negotiation are accepted.
- RADIUS authentication is enabled by default.
- Example

  host1(config)#**ip ssh disable-user-authentication**

- Use the **no** version to restore RADIUS authentication.

ip ssh sleep

- Use to set a sleep period in seconds for users that have exceeded the authentication retry limit. Connection attempts from the user at the same host are denied until this period expires.
- Specify any nonnegative integer.
- Example

  host1(config)#**ip ssh sleep 300**

- Use the **no** version to restore the default value, 600 seconds.

ip ssh timeout

- Use to set a timeout period in seconds. The SSH server terminates the connection if protocol negotiation—including user authentication—is not completed within this timeout.
- Specify an integer from 10–600.
- Example

  host1(config)#**ip ssh timeout 480**

- Use the **no** version to restore the default value, 600 seconds.

Configuring Message Authentication

The SSH server and SSH client maintain separate lists of the message authentication algorithms that each supports. Lists are kept for *inbound* and *outbound* algorithms. For the server, *inbound* means the algorithms that the server supports for information coming in from a client. For the server, *outbound* means the algorithms that the server supports for information it sends out to a client. You must configure each list separately. By default, all of the supported encryption algorithms are available. You need to configure encryption only if you need to specifically remove or add any supported algorithm from the list. The system supports the following SSH algorithms for hash function-based message authentication:

- hmac-sha1—Uses Secure Hash Algorithm 1 (SHA-1) to create a 160-bit message digest from which it generates the MAC.
- hmac-sha1-96—Uses the first 96 bits of the SHA-1 message digest to generate the MAC.
- hmac-md5—Uses MD5 hashing to create a 128-bit message digest from which it generates the MAC.

Although it is not recommended, you can also specify **none**. In this case, the system does not verify the integrity of the data.

ip ssh mac

- Use to add a message authentication algorithm to the specified support list for the SSH server.

  Example 1—This example adds the hmac-md5 algorithm to the list of supported outbound algorithms.

  host1(config)#**ip ssh mac server-to-client hmac-md5**

- If you to not specify a direction (client-to-server or server-to-client), the command applies the algorithm to both inbound and outbound lists.
- The **default** version restores the specified list to the factory default, which includes all supported algorithms (hmac-md5, hmac-sha1, and hmac-sha1-96). The default list does not include the *none* option.
- Example 2—This example restores the hmac-sha1 algorithm to the list of supported inbound algorithms.

  host1(config)#**ip ssh mac client-to-server default hmac-sha1**

- Use the **no** version to remove or exclude an algorithm from the specified list.

  Example 3—This example removes the hmac-sha1 algorithm from the list of supported inbound algorithms.

  host1(config)#**ip ssh mac client-to-server no hmac-sha1**

Enabling and Disabling SSH

The SSH server daemon starts only if the server host key exists when the router boots. The host key resides in NVS and is persistent across system reboots. After it has started, the daemon listens for traffic on TCP port 22. The server daemon is disabled by default.

crypto key dss

- Use the **generate** keyword to create the SSH server host key and enable the daemon.
- Example

  host1(config)#**crypto key generate dss**

- Use the **zeroize** keyword to remove the SSH server host key and stop the SSH daemon if it is running. Issuing this command terminates any active client sessions. The next time the router boots after this command is issued, the SSH server daemon is not started.
- The command is not displayed by the **show configuration** command.

NOTE: SSH can be enabled or disabled regardless of the state of the Telnet daemon. If SSH is enabled, use access control lists to limit access through Telnet. See *Virtual Terminal Access Lists* on page 458 for information about using access control lists.

- Example

  host1(config)#**crypto key zeroize dss**

- There is no **no** version.

Displaying SSH Status

You can monitor the current state of the SSH server with the **show ip ssh** command.

show ip ssh

- Use to display the current state of the SSH server.
- Use the **detail** keyword to display the encryption and MAC algorithm lists for the client and server. For each active session, **detail** shows the version of SSH running on the client and the algorithms in use for encryption and message authentication.
- Field descriptions
  - daemon status—Indicates whether the SSH server is enabled; if so, how long it has been up
  - supported encryption, inbound—Encryption algorithms supported inbound from the client
  - supported encryption, outbound—Encryption algorithms supported outbound to the client
  - supported MAC, inbound—Message authentication code algorithms supported inbound from the client

- supported MAC outbound—Message authentication code algorithms supported outbound to the client
- connections since last system reset—Number of connections made through SSH since the last time the system was reset
- connections since daemon startup—Number of connections made since the SSH server was enabled
- active sessions—Number of SSH sessions currently active
  - id—Session ID number
  - username—Username for the remote user that initiated the session
  - host—IP address of the remote client
  - uptime (d:h:m:s)—Duration of the session
  - client version—Version of the SSH software run by the remote client
  - ciphers inbound/outbound—Encryption algorithms used by the client and the system for this session
  - MAC inbound/outbound—Message authentication code algorithms used by the client and the system for this session

- Example

```
host1#show ip ssh detail

SSH Server version: SSH-2.0-2.0.12

daemon status: enabled, up since MON NOV 08 1999 14:38:19 UTC

supported encryption, inbound: 3des-cbc,blowfish-cbc,twofish-cbc
supported encryption, outbound: 3des-cbc,blowfish-cbc,twofish-cbc
supported MAC, inbound: hmac-sha1,hmac-sha1-96,hmac-md5
supported MAC, outbound: hmac-sha1,hmac-sha1-96,hmac-md5

connections since last system reset: 4 out of 4 attempts
connections since daemon startup:    4 out of 4 attempts

active sessions: 1
```

id	username	host	uptime (d:h:m:s)	client version	ciphers inbound/outbound	MAC inbound/outbound
3	mcarr	10.0.0.145	0:00:00:19	SSH-2.0-2.0.12 F-SECURE SSH	3des-cbc/3des-cbc	hmac-md5/hmac-md5

- To view failed connection attempts and other protocol errors logged at the error severity level, use the **show log data** command:

  host1#**show log data category ssh severity error**

Terminating an SSH Session

You can use the session identifier to terminate an SSH session.

disconnect ssh

- Use to terminate an active SSH session.
- Use the **show ip ssh** command to determine the session identifier for the session to terminate.
- Example

  host1(config)#**disconnect ssh 12**

NOTE: You can also use the **clear line vty** terminal command to terminate SSH sessions. In that case, use the **show users** command to determine the virtual terminal number to specify with the **clear line vty** terminal command.

- There is no **no** version.

Restricting User Access

Users who are authenticated through RADIUS or TACACS+ can be restricted to certain sets of commands and virtual routers (VRs). The levels of access are shown in Table 52. For information about TACACS+, see *JUNOSe Broadband Access Configuration Guide, Chapter 9, Configuring TACACS+*.

Table 52: CLI User Access Levels

Access Level	Commands Available
0	**disable**, **enable**, **exit**, and **help** commands
1	Level 0 commands and all other commands available in User Exec mode
5	Level 1 commands and all Privileged **show** commands
10	All commands except support and privilege change commands
15	Commands that Juniper Networks Technical Support may provide and all other commands

Restricting Access to Commands with RADIUS

You can use RADIUS authentication to specify a level of commands that a user is allowed. If you do not configure RADIUS authentication for the console or virtual terminals, all users who successfully log in are automatically granted Level 1 access.

The vendor-specific attribute (VSA) Admin-Auth-Level supports the levels of access shown in Table 52. In addition to VSA access level support, the software provides access to levels 1 and 10 through the Initial-Auth-Level in the standard RADIUS Service-Type attribute. If the RADIUS Service-Type attribute is included in the RADIUS Access-Accept message, the standard attribute overrides any VSA setting.

If you are using the RADIUS Service-Type attribute to assign access levels, the system sets the Initial-Auth-Level as follows:

- If the Service-Type attribute is set to “administrative,” then the Initial-Auth-Level is set to 10.
- If the Service-Type attribute is set to “nas prompt” or “login,” the Initial-Auth-Level is set to 1.

Per-User Enable Authentication

After a user has been authenticated through RADIUS, the RADIUS server provides the E-series router with the names of the privilege levels (for example, “10”) that the user has **enable** access to. When the user attempts to access a privilege level through the **enable** command, the system either denies or approves the user’s request.

The decision to deny or approve the user’s request is based on the list the system received through RADIUS. See Table 53.

Table 53: Juniper Networks–Specific CLI Access VSA Descriptions

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Initial-CLI- Access-Level	Specifies the initial level of access to CLI commands.	26	len	18	sublen	Single attribute; enter only: 0, 1, 5, 10, or 15
Alt-CLI- Access-Level	Specifies level of access to CLI commands.	26	len	20	sublen	Single attribute; enter only: 0, 1, 5, 10, or 15

NOTE: All levels to which a user can have access must explicitly be specified in the Admin-Auth-Set VSA.

The user is not prompted for a password, because the system knows whether or not the user should have access to the requested level. If the user is not authenticated through RADIUS, the router uses the system-wide **enable** passwords instead.

Restricting Access to Virtual Routers

You can use RADIUS authentication to specify whether users can access all virtual routers (VRs), one specific VR, or a set of specific VRs.

NOTE: This classification is independent of the command access levels configurable through the Initial-CLI-Access-Level VSA.

The VSA Allow-All-VR-Access controls access; the VSA Virtual-Router controls the VR to which the user logs in, and the VSA Alt-CLI-Virtual-Router-Name specifies which VRs other than the VR specified by the VSA virtual-router are accessible to restricted users. See Table 54.

Table 54: Juniper Networks–Specific Virtual Router Access VSA Descriptions

VSA	Description	Type	Length	Subtype	Subtype Length	Value
Allow-All-VR-Access	Specifies user access to all virtual routers.	26	len	19	sublen	Integer: 0 – disable, 1 – enable
Virtual-Router	Specifies the VR to which the user logs in or the only VR to which a user has access. The default setting is the default VR.	26	len	1	sublen	String: *virtual-router -name*
Alt-CLI-Virtual-Router-Name	Specifies a VR, other than the VR specified by the Virtual-Router VSA, to which the user has access. You can define this VSA multiple times to define a set of VRs to which a user has access.	26	len	21	sublen	String: *virtual-router -name*

VSA Configuration Examples

Consider a router on which five VRs have been configured. The VRs are called Boston, Chicago, Detroit, Los Angeles, and San Francisco. The following examples illustrate how to use the VSAs to control a user's access to these VRs.

Example 1 In this example, you want the user to have access to all VRs and to log in to the default VR. Accept the default setting or set the following VSA:

- Allow-All-VR-Access—1

Example 2 In this example, you want the user to have access to all VRs and to log in to the VR Boston. Set the VSAs as follows:

- Allow-All-VR-Access—1
- Virtual-Router—Boston

Example 3 In this example, you want the user to have access only to the VR Boston. Set the VSAs as follows:

- Allow-All-VR-Access—0
- Virtual-Router—Boston

Example 4 In this example, you want the user to log in to VR Boston, and to have access to VRs Chicago, Los Angeles, and San Francisco. Set the VSAs as follows:

- Allow-All-VR-Access—0
- Virtual-Router—Boston
- Alt-CLI-Virtual-Router-Name—Chicago

- Alt-CLI-Virtual-Router-Name—Los Angeles
- Alt-CLI-Virtual-Router-Name—San Francisco

Commands Available to Users

If you do not configure RADIUS authentication for the console or virtual terminals, there are no restrictions on VR access for any user who successfully logs in to the router. For example, nonrestricted users can:

- Issue the **virtual-router** command in Privileged Exec mode, to switch to another previously created virtual router.
- Issue the **virtual-router** command in Global Configuration mode to create a new virtual router and switch to its context.
- Access Global Configuration mode to configure the router and virtual routers.
- View all settings for the router and all virtual routers.

User restricted to one or a set of specific VRs can see and use only a limited set of commands to monitor the status of those VRs and view some configuration settings on those VRs. More specifically, such users:

- Can issue the **virtual-router** command in Privileged Exec mode to switch to another previously configured VR to which they have access.
- Cannot create new VRs or access VRs other than those to which they have access.
- Cannot access Global Configuration mode and cannot configure VRs to which they have access.
- Cannot see or use any commands associated with the file system, boot settings, or system configuration.

The following table lists some, but not all, commands accessed from Exec mode that are available only to users with no VR restriction:

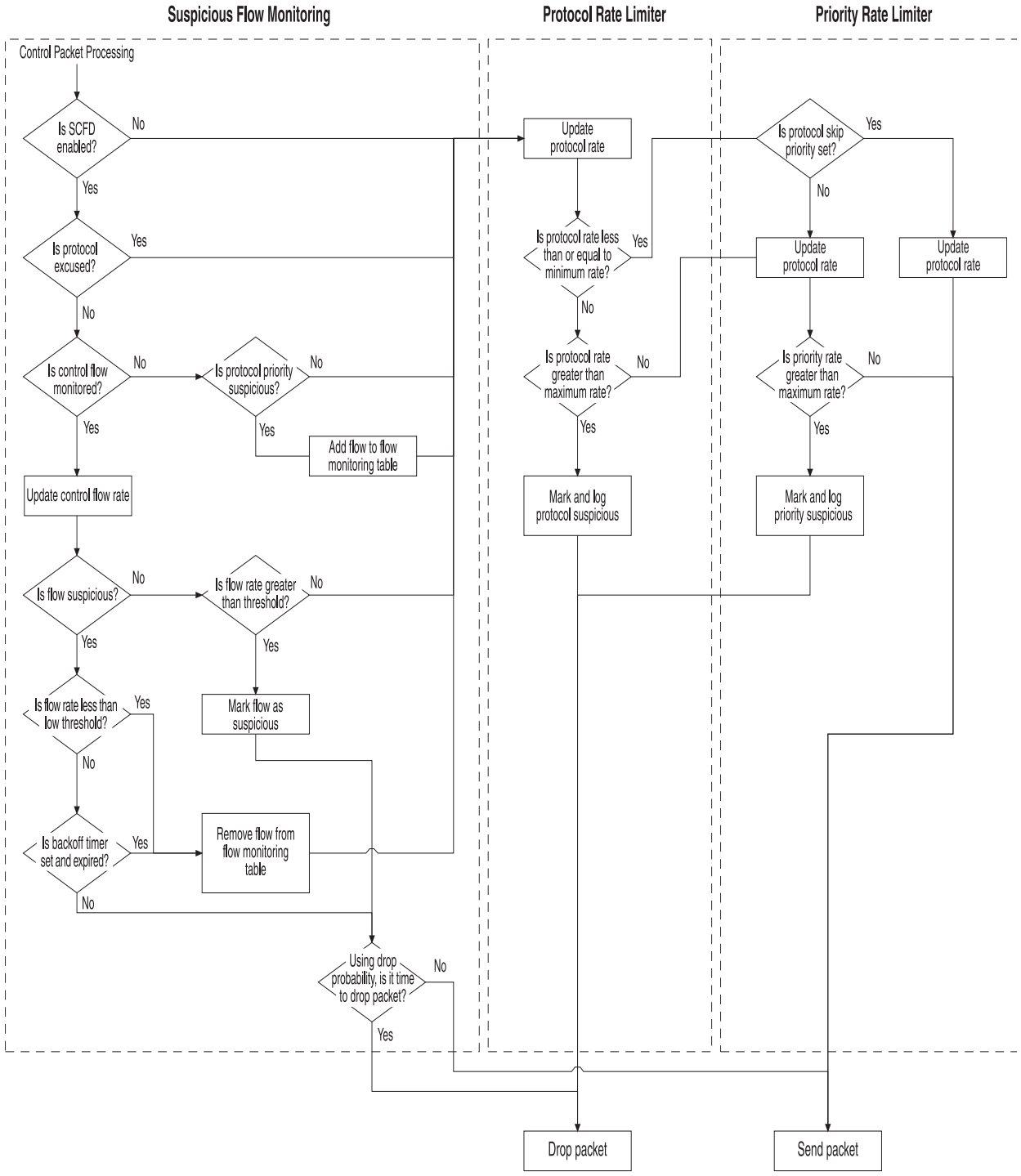
clear line	reload	show redundancy
clock set	reload slot	show secrets
copy	rename	show subsystems
copy running-configuration	redundancy force-switchover	show timing
delete	redundancy revert	show users
dir	show boot	show utilization
disconnect ssh	show config	srp switch
configure	show exception dump	synchronize
erase secrets	show ip ssh	–
halt	show line	–

Denial of Service (DoS) Protection

A denial-of-service (DoS) attack is any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Denial of service protection provides reactive prevention from attack and determines whether the source of traffic is valid or invalid. DoS protection includes diagnostic tools and configuration options. DoS protection groups provide a simple policy that can be applied to interfaces, which can specify a set of parameters to tune behavior.

Figure 29 shows an example of the state of a flow with DoS protection using suspicious control flow detection (SCFD).

Figure 29: Typical Control Packet Processing



Suspicious Control Flow Detection

To reduce the chance of a successful denial of service (DoS) attack and to provide diagnostic abilities while undergoing an attack, the system can detect suspicious control flows and keep state on those flows. A flow is a specific control protocol on a specific interface from a particular source. When the system determines that a control flow is suspicious, it can take corrective action on that control flow.

Keeping full state on each control flow can use a large number of resources. Instead, the system detects which flows have suspicious traffic. If a control flow is marked as suspicious, every packet associated with the flow is considered suspicious. When a packet is marked as suspicious, it is dropped based on drop probability before being delivered to the control processor.

When a distributed DoS attack occurs on a line module, suspicious flow control resources can be exhausted. To provide further counter measures, you can enable the group feature, where flows are grouped together and treated as a whole. If you do not use the group feature, suspicious flows can fill up the suspicious flow table and prevent detection of additional attacking flows.

Suspicious Control Flow Monitoring

Each protocol has a per-protocol rate limit. The rate limiter is used to limit the rate of packets that proceed to the control processor for the specific protocol. Per-protocol rate limiting is also used to begin the process by which flows of the specific protocol are monitored.

Each priority has a per-priority rate limit. The rate limiter limits the rate of packets that proceed to the control processor for the specific priority. It also begins the process by which flows of the specific priority are monitored.

All protocols on each line module have a rate limit. Each protocol is associated with a given priority, which is also provided with a rate limit. When a slot comes under attack, the first lines of defense are the protocol and priority rate limiters. If the line module determines that a specific protocol or priority is under attack (because the rate has been exceeded), it proceeds to monitor all flows from the problem protocol or priority. Initially, a control flow is marked as nonsuspicious.

After a control flow is placed in the suspicious flow table, the system inspects all packets that belong to the flow. The interface controller (IC) and forwarding controller (FC) monitor the table to determine whether the suspicious flow has a packet rate above the suspicious level. If the packet rate is above this level, the flow is marked as suspicious. Marking a control flow as suspicious affects only a particular protocol on a particular interface. When a flow is marked as suspicious, all packets belonging to that flow are marked as suspicious and trapped at the forwarding controller.

Suspicious control flows are continually monitored. The flow can be restored if the flow goes below the low threshold level. The flow can also be restored based on a backoff timer. The flow is removed from the suspicious flow table if the related interface is removed.

Approximately 2000 flows can be monitored as suspicious at any time for each line module. When the suspicious flow table on a particular line module reaches its maximum and the system is not set to group flows, flows that should be marked as suspicious proceed as nonsuspicious. When you return a suspicious flow to a nonsuspicious state or delete it, the flows that did not fit into the table are added to the table.

By default, the system groups flows when the suspicious flow table size is exceeded on a line module. When the flow table is full, instead of marking a specific flow in that group as suspicious and providing information on each flow on that line module, the system groups flows based on group membership and provides information on the group instead of each flow. This flow information is useful under severe distributed DoS attacks. Group membership is based on physical port and control protocol; all flows in that group are considered suspicious.

Configurable Options

You can configure the following options for suspicious flow detection:

- Global on or off. When the option is set to off, flows or packets are not marked as suspicious. The default is on.
- Actions a line module takes when the suspicious flow table on the line module overflows:
  - Overflow—Stop recognizing new suspicious flows
  - Group—Group flows into logical groupings where some individual flows are monitored as a group
- Suspicious threshold for each protocol. The threshold is the rate in packets per second at which a flow becomes suspicious. A zero setting disables suspicious flow detection for the protocol. Flows are subject to protocol and priority rate limits, but not to suspicious flow detection.
- Low threshold for each protocol. The threshold rate determines whether an interface transitions from suspicious back to nonsuspicious. A zero setting means that the flow does not transition back to nonsuspicious based on packet rate.
- Backoff time in seconds for each protocol. After this period expires, the flow transitions to nonsuspicious regardless of the current rate. When set to zero, an interface does not return to the nonsuspicious state using a time mechanism.

You can also clear the following:

- All suspicious flows from the suspicious flow table for a specific slot.
- Suspicious flows from the suspicious flow table for the entire system.
- A single suspicious flow; returns the flow to the nonsuspicious state.

Display Options

For monitoring purposes, you can:

- Display all suspicious control flows when the system has recognized an attack.
- Display the current state and the number of transitions into suspicious state for the protocol and priority.
- Display historical counts about the number of flows made suspicious.
- View a trap or log generated when a control flow is considered suspicious.
- View a trap or log generated when a control flow is no longer suspicious.

Traps and Logs

The system generates a trap and a log message under the following conditions:

- A control flow transitions into a suspicious state; another trap and log message is generated on removal from a suspicious state.
- A protocol transitions to or from the suspicious state.
- A priority transitions to or from the suspicious state.
- The suspicious flow control system is overflowing or grouping flows on a line module.

You can control trap and log messages using CLI or SNMP commands.

Suspicious Control Flow Commands

Use the commands described in this section to regulate suspicious control flows.

baseline suspicious-control-flow-detection counts

- Use to set a baseline for statistics for suspicious control flow detection.
- Example

  host1#**baseline suspicious-control-flow-detection counts**

- There is no **no** version.

clear suspicious-control-flow-detection

- Use to clear the active state for suspicious control detection.
- If you do not specify a slot or interface, clears all suspicious flows.
- If you specify a slot, clears all specified suspicious flows on that slot.
- If you specify an interface and protocol, and source mac-address. clears that specific flow.

- Example

  host1#**clear suspicious-control-flow-detection interface atm 1/0.1 ppp Control address 0000.0001.0002**

- There is no **no** version.

suspicious-control-flow-detection grouping-off

- Use to turn off overflow protection for suspicious control flow detection, enabling flows to be grouped into larger entities when the line module flow table overflows.
- Example

  host1(config)#**suspicious-control-flow-detection grouping-off**

- Use the **no** version to turn on overflow protection.

suspicious-control-flow-detection off

- Use to turn off the suspicious control flow detection.
- Example

  host1(config)#**suspicious-control-flow-detection off**

- Use the **no** version to turn on suspicious control flow detection, which is the default.

suspicious-control-flow-detection protocol backoff-time

- Use to set the backoff time in seconds for a specific protocol that triggers the suspicious flow to return to a nonsuspicious state.
- When set to zero, a suspicious control flow for a protocol does not return to a nonsuspicious state using a time mechanism.
- Example

  host1(config)#**suspicious-control-flow-detection protocol iposi backoff-time 300**

- Use the **no** version to restore the defaults for the protocol, 300 seconds.

suspicious-control-flow-detection protocol low-threshold

- Use to set a threshold for a specific protocol; if the flow rate falls below this rate, a suspicious flow changes to the nonsuspicious state.
- Low threshold is the rate in packets per second at which a suspicious flow becomes no longer suspicious.
- When set to zero, a suspicious flow cannot change to the nonsuspicious state by means of a low threshold rate. To clear this flow, you must use the **clear suspicious-control-flow-detection** command.
- Example

  host1(config)#**suspicious-control-flow-detection protocol iposi low-threshold 512**

- Use the **no** version to restore the defaults for the protocol.

suspicious-control-flow-detection protocol threshold

- Use to set the threshold in packets per second for a specific protocol, which triggers the flow to become a suspicious flow.
- When set to zero, a suspicious flow cannot change to the nonsuspicious state via a threshold rate.
- Example

  host1(config)#**suspicious-control-flow-detection protocol iposi threshold 1024**

- Use the **no** version to restore the defaults for the protocol.

Monitoring Suspicious Control Flow

Use the commands described in this section to monitor suspicious control flows.

show suspicious-control-flow-detection counts

- Use to display statistics for suspicious control flow detection. When a slot is specified, displays only information for the specific slot. If no slot is specified, displays information for all slots.
- The **delta** keyword displays statistics for the current baseline.
- Field descriptions
  - Number of suspicious flows total—Total number of suspicious flows, current and past
  - Number of suspicious flows current—Number of suspicious flows currently detected and monitored
  - Number of groups total—Total number of groups, current and past
  - Number of groups current—Number of groups currently detected and monitored
  - Number of false negatives total—Total number of flows monitored that have not become suspicious (exceeded their threshold)
  - Number of false negatives current—Current number of flows monitored that have not become suspicious (exceeded their threshold)
  - Number of table overflows—Number of times a flow table overflows
- Example

```
host1(config)#show suspicious-control-flow-detection counts
Suspicious Flow Detection System Counts
        Number of suspicious flows total: 0
        Number of suspicious flows current: 0
        Number of groups total: 0
        Number of groups current: 0
        Number of false negatives total: 0
        Number of false negatives current: 0
        Number of table overflows: 0
```

show suspicious-control-flow-detection flows

- Use to display suspicious flows.
- Field descriptions
  - Interface—Interface for the flow
  - Protocol—Control protocol of the flow
  - MAC address—Source MAC address of the flow
  - InSlot—For certain flows detected on egress, the possible ingress slot of the flow
  - Rate (pps)—Rate of the flow
  - Peak Rate (pps)—Peak rate of the flow
  - Time Since Created—Time since the flow was determined to be suspicious, in hh:mm:sec format
- Example

```
host1(config)#show suspicious-control-flow-detection flows
Suspicious Flow Detection System Flows
                                                    Peak            Time
                                              In    Rate    Rate    since
Interface             Protocol       MAC address  Slot  (pps)   (pps)   Create
-----------------     -------        ------------ ----- ---    -------  -------
GigabitEthernet 1/0/7 Ethernet ARP   0000.0100.0002 ---  1000030 1000050 00:00:32

*group 3 slot 1       EthernetArpMiss 0000.0100.0003 ---  1000    3000    00:10:10
```

show suspicious-control-flow-detection info

- Use to display information about suspicious flows.
- You can specify the following keywords:
  - **delta**—Displays statistics for the current baseline
  - **brief**—Displays only suspicious information
  - **slot**—Displays information for the specific slot
- Field descriptions
  - Protocol Information
    - Protocol—Control protocol of the flow
    - State
      - OK—Protocol is currently not receiving an excess amount of traffic.
      - Suspicious—Protocol detected as receiving an excess amount of traffic within the last backoff time in number of seconds.
    - Transitions—Number of times this protocol or priority has transitioned to the suspicious state
  - Priority Information
    - Priority—Priorities map to a specific queue and color; priority groups are Hi-Green, Hi-Yellow, Lo-Green and Lo-Yellow.

- State:
  - OK—Protocol is currently not receiving an excess amount of traffic
  - Suspicious—Protocol detected as receiving an excess amount of traffic within the last backoff time in number of seconds.
- Transitions—Number of times this protocol or priority has transitioned to the suspicious state

- Example

```
host1(config)#show suspicious-control-flow-detection info slot 2
Suspicious Flow Detection System Information
        Suspicious Flow Detection System is enabled

        Using Groups

The suspicious control flow system is not in overflow state or using groups
Protocol Information
Protocol                                State      Transitions
--------------------------------------- ---------- -----------
Ppp Echo Request                        OK         0
Ppp Echo Reply                          OK         0
Ppp Echo Reply Fastpath                 OK         0
Ppp Control                             OK         0
Atm Control (ILMI)                      OK         0
Atm OAM                                 OK         0
Atm Dynamic Interface Column Creation   OK         0
Atm Inverse ARP                         OK         0
Frame Relay LMI Control                 OK         0
Frame Relay Inverse Arp                 OK         0
Pppoe Control                           OK         0
Pppoe Config Dynamic Interface Column   OK         0
 Creation
Ethernet ARP Miss                       OK         0
Ethernet ARP                            OK         0
Ethernet LACP packet                    OK         0
Ethernet Dynamic Interface Column       OK         0
 Creation
Slep SLARP                              OK         0
MPLS TTL Exceeded On Receive            OK         0
MPLS TTL Exceeded On Transmit           OK         0
MPLS MTU Exceeded                       OK         0
Ipsec Transport Mode L2tp Control       OK         0
NAT/Firewall Payload                    OK         0
NAT/Firewall Update Table               OK         0
DHCP External                           OK         0
IP OSI                                  OK         0
IP TTL Expired                          OK         0
IP Options Other                        OK         0
IP Options Router Alert                 OK         0
IP Multicast/Broadcast Other            OK         0
IP Multicast DHCP (SC)                  OK         0
IP Multicast Control (SC)               OK         0
IP Multicast Control (IC)               OK         0
IP Multicast VRRP                       OK         0
IP Mulitcast Cache Miss                 OK         0
IP Multicast Cache Miss Auto Reply      OK         0
IP Multicast Wrong Interface            OK         0
IP Local DHCP (SC)                      OK         0
IP Local Dhcp (IC)                      OK         0
IP Local Icmp Echo                      OK         0
```

```
IP Local Icmp Other                     OK         0
IP Local LDP                            OK         0
IP Local BGP                            OK         0
IP Local OSPF                           OK         0
IP Local RSVP                           OK         0
IP Local PIM                            OK         0
IP Local COPS                           OK         0
IP Local L2tp Control (SC)              OK         0
IP Local L2tp Control (IC)              OK         0
IP Local Other                          OK         0
IP Local Subscriber Interface Miss      OK         0
IP Route To SRP Ethernet                OK         0
IP Route No Route Exists                OK         0
IP Normal Path MTU                      OK         0
IP Neighbor Discovery                   OK         0
IP Neighbor Discovery Miss              OK         0
IP Search Error                         OK         0
IP MLD                                  OK         0
IP Local PIM Assert                     OK         0
IP Local BFD                            OK         0
IP IKE                                  OK         0
IP Reassembly                           OK         0
IP Local Icmp Frag                      OK         0
IP Local Frag                           OK         0
IP Application Classifier HTTP Redirect OK         0

Priority Information
Priority     State    Transitions
------------ ---------- -----------
Hi-Green-IC  OK         0
Hi-Yellow-IC OK         0
Lo-Green-IC  OK         0
Lo-Yellow-IC OK         1
Hi-Green-SC  OK         0
Hi-Yellow-SC OK         0
Lo-Green-SC  OK         0
Lo-Yellow-SC OK         0
```

show suspicious-control-flow-detection protocol

- Use to display protocol information for suspicious control flows.
- Field descriptions
  - Protocol—Control protocol
  - Threshold—Threshold in packets per second
  - Lo-Threshold—Low threshold in packets per second
  - Backoff-Time—Backoff time in seconds
- Example

```
host1(config)#show suspicious-control-flow-detection protocol
Protocol                        Threshold Lo-Threshold Backoff-Time
------------------------------ --------- ------------ ------------
Ppp Echo Request                       10            5          300
Ppp Echo Reply                         10            5          300
Ppp Echo Reply Fastpath                10            5          300
Ppp Control                            10            5          300
Atm Control (ILMI)                     10            5          300
Atm OAM                                10            5          300
Atm Dynamic Interface Column           10            5          300
 Creation
```

Atm Inverse ARP	10	5	300
Frame Relay LMI Control	10	5	300
Frame Relay Inverse Arp	10	5	300
Pppoe Control	512	256	300
Pppoe Config Dynamic Interface Column Creation	10	5	300
Ethernet ARP Miss	128	64	300
Ethernet ARP	128	64	300
Ethernet LACP packet	10	5	300
Ethernet Dynamic Interface Column Creation	512	256	300
Slep SLARP	128	64	300
MPLS TTL Exceeded On Receive	10	5	300
MPLS TTL Exceeded On Transmit	10	5	300
MPLS MTU Exceeded	10	5	300
Ipsec Transport Mode L2tp Control	2048	1024	300
NAT/Firewall Payload	512	256	300
NAT/Firewall Update Table	512	256	300
DHCP External	1024	512	300
IP OSI	2048	1024	300
IP TTL Expired	10	5	300
IP Options Other	512	256	300
IP Options Router Alert	2048	1024	300
IP Multicast/Broadcast Other	512	256	300
IP Multicast DHCP (SC)	512	256	300
IP Multicast Control (SC)	2048	1024	300
IP Multicast Control (IC)	512	256	300
IP Multicast VRRP	512	256	300
IP Mulitcast Cache Miss	128	64	300
IP Multicast Cache Miss Auto Reply	128	64	300
IP Multicast Wrong Interface	10	5	300
IP Local DHCP (SC)	512	256	300
IP Local Dhcp (IC)	512	256	300
IP Local Icmp Echo	512	256	300
IP Local Icmp Other	128	64	300
IP Local LDP	2048	1024	300
IP Local BGP	2048	1024	300
IP Local OSPF	64	32	300
IP Local RSVP	2048	1024	300
IP Local PIM	2048	1024	300
IP Local COPS	2048	1024	300
IP Local L2tp Control (SC)	2048	1024	300
IP Local L2tp Control (IC)	512	256	300
IP Local Other	512	256	300
IP Local Subscriber Interface Miss	512	256	300
IP Route To SRP Ethernet	512	256	300
IP Route No Route Exists	10	5	300
IP Normal Path MTU	10	5	300
IP Neighbor Discovery	128	64	300
IP Neighbor Discovery Miss	128	64	300
IP Search Error	10	5	300
IP MLD	512	256	300
IP Local PIM Assert	512	256	300
IP Local BFD	1024	512	300
IP IKE	512	256	300
IP Reassembly	2048	1024	300
IP Local Icmp Frag	512	256	300
IP Local Frag	512	256	300
IP Application Classifier HTTP Redirect	128	64	300

show snmp interfaces

- Use to display a list of interface types that are compressed in the interface tables and the interface numbering method configured on the router.
- Field descriptions
  - Compressed(Removed) Interface Types—List of interface types that are removed from the ifTable and ifStackTable
  - Armed Interface Numbering Mode—Interface numbering method configured on the router: RFC1213, RFC2863
  - maxIfIndex—Maximum value that the system will allocate to the ifIndex field
  - maxIfNumber—Maximum number of interfaces allowed in the ifTable
  - Interface Description Setting—Method used to encode the ifDescr and ifName objects: common, legacy, proprietary
- Example

```
host1#show snmp interfaces
Compressed(Removed) Interface Types:
HDLC, FT1, ATM, ATM1483
Armed Interface Numbering Mode:
RFC1213, maxIfIndex=65535, maxIfNumber=65535
Interface Description Setting: proprietary
```

Denial-of-Service Protection Groups

A DoS protection group provides a simple policy that can be applied to interfaces. This policy can specify a complete set of parameters to tune the behavior of the DoS protection groups. The system uses these parameters to determine the priority and rates for various control protocols. The rate of traffic for a particular protocol is unlikely to be the same on all ports in the system. A configuration can have several types of interfaces, such as DHCP access clients, PPPoE access clients, and uplink interfaces. Each of these interfaces requires a different DoS configuration. All interfaces are associated with a default DoS protection group, which has standard system defaults. The maximum rates are per line module, and the drop probability is 100 percent (all suspicious packets are dropped).

Group Parameters

DoS protection groups support the following set of parameters:

- Protocol-to-priority mapping enables you to map a protocol to one of four priorities.
- Protocol burst enables you to configure the burst level for the protocol. The burst is configurable in packets, and defaults to a value in packets that is one half of the maximum rate.

- Protocol maximum rate limit (per line module) enables you to map a protocol to a maximum rate limit. This rate limit applies to all packets for a particular protocol for interfaces belonging to this particular DoS protection group on a line module. By having a DoS protection group on a single line module, the total maximum rate for a protocol can be up to the sum of the four rates configured, depending on the DoS group attached to an interface. You can set a maximum rate of zero for protocols that are not used. The actual rate never exceeds the maximum rate, but the actual rate allowed can be less than the configured maximum rate because of the weighting of protocols within a DoS protection group and the use of multiple DoS protection groups.

- Protocol weight with respect to other protocols in the DoS protection group enables you to balance the priority of the protocols. For each priority grouping, weight determines the effective minimum rate that each protocol receives. Within each priority, the sum of the minimum rates for all protocols using that priority is equal to or less than the priority rate times the over-subscription value. Each priority has a separate rate for each DoS protection group.

- Protocol drop probability for suspicious packets enables you to map a protocol to a specific drop probability. The drop probability is the percentage probability that a suspicious packet is dropped.

- Protocol skip priority rate limiter enables you to configure the system so that the specified protocol is not subject to the priority rate limiter for the priority and DoS protection group selected. The default is off—the protocol is subject to priority rate limiting.

- Priority rate sets the rate of the priority in packets per second for the line module. If this rate is exceeded, it triggers DoS suspicious control flow detection.

- Priority burst enables you to set the number of packets allowed to exceed the maximum rate before packets are dropped and DoS suspicious control flow detection is triggered.

- Priority oversubscription enables you to set an oversubscription factor for the priority rate limiter. In addition to the priority rate, it calculates the minimum rate limits for protocols with a priority grouping and allows for oversubscription of the priority rate. The value indicates a percentage that the priority rate limiter is allowed to be oversubscribed, in the range 100–1000.

Attaching Groups

By default, each interface belongs to the default DoS protection group. The name is the only non-configurable aspect of the default DoS protection group.

The DoS protection group is a configurable parameter for all Layer 2 and IP interfaces. Similar to other configurable interface parameters, the DoS protection group can be set using profiles.

Because all newly created interfaces default to using the default DoS protection group, they do not inherit any DoS protection group association from a higher or lower interface binding. The DoS group applies to all types of control flows for the specific interface. For example, an IP interface supports a variety of control protocols, each of which can be separately mapped to a priority and drop probability, but to a single DoS protection group.

Protocol Mapping

Table 55 and Table 56 list the protocols mapped within DoS protection groups.

Table 55: Layer 2-Related Protocols

CLI Name	Description of Flow
atmControl	ATM ILMI packets
atmOAM	ATM OAM packets
atmDynamicIf	ATM dynamic interface column creation
atmInverseArp	ATM inverse ARP packets
dhcpExternal	DHCP external packets
ethernetArpMiss	Ethernet/Bridged Ethernet request to send ARP
ethernetArp	Ethernet/Bridged Ethernet reception of ARP packet
ethernetLacp	Ethernet LACP packet
ethernetDynamicIf	Ethernet/Bridged Ethernet dynamic VLAN interface creation
flisInPayload	Firewall/NAT payload
flisInPayloadUpdateTbl	Firewall/NAT payload and update table
frameRelayControl	Frame Relay LMI packets
frameRelayArp	Frame Relay inverse ARP packets
itmL2tpControl	IPSec transport mode L2TP control packets
mplsTtlOnRx	MPLS TTL expired on ingress
mplsTtlOnTx	MPLS TTL expired on egress
mplsMtu	MPLS MTU exceeded
pppEchoRequest	PPP echo request packets destined for the IC
pppEchoReply	PPP echo reply packets destined for the IC
pppEchoReplyFast	PPP echo request packets generating an FC-based reply
pppControl	other PPP control packets
pppoeControl	PPPoE PADx packets

Table 55: Layer 2-Related Protocols (continued)

CLI Name	Description of Flow
pppoePppConfig	PPPoE handling of PPP LCP packets for dynamic interface creation
slepSlarp	Serial Line Interface SLARP packets

Table 56: IP-Related Protocols

CLI Name	Description of Flow
ipAppClassifierHttpRedirect	IP Application Classifier (HTTP redirect) packets
ipIke	IP IKE packet
ipLocalBfd	IP BFD packets
ipLocalBgp	IP BGP packets
ipLocalCops	IP COPS packets
ipLocalDemuxMiss	IP Subscriber Interface Miss packets
ipLocalDhcpIc	IP DHCP packets destined for the IC (not broadcast)
ipLocalDhcpSc	IP DHCP packets destined for the SC (broadcast and IC not enabled)
ipLocalFrag	IP fragments not classifiable
ipLocalIcmpEcho	IP ICMP echo request and reply
ipLocalIcmpFrag	IP ICMP packets that are not further classifiable (most likely large ping packets)
ipLocalIcmpOther	IP ICMP except echo request and reply
ipLocalL2tpControlIC	IP L2TP control packets for IC
ipLocalL2tpControlSC	IP L2TP control packets for SC
ipLocalLDP	IP LDP packets
ipLocalOspf	IP OSPF packets
ipLocalOther	IP Local packets not otherwise classified
ipLocalPim	IP PIM packets (except typeAssert)
ipLocalPimAssert	IP PIM assert type packets
ipLocalRsvp	IP RSVP packets
ipMld	IP Multicast listener packet
ipMulticastBroadcastOther	Ip Multicast/Broadcast not otherwise classified
ipMulticastCacheMiss	IP Multicast route table misses
ipMulticastCacheMissAutoRp	IP Multicast route table Auto-RP misses
ipMulticastControlIc	IP IGMP packets for the IC
ipMulticastControlSc	IP Multicast control packet not otherwise classified
ipMulticastDhcpSc	IP Multicast DHCP destined for SC
ipMulticastVrrp	IP VRRP packets
ipMulticastWrongIf	IP Multicast on wrong interface
ipNeighborDiscovery	IPv6 Neighbor Discovery

Table 56: IP-Related Protocols (continued)

CLI Name	Description of Flow
ipNeighborDiscoveryMiss	IPv6 Neighbor Discovery miss
ipNormalPathMtu	IP Path MTU request
ipOptionsOther	IP options not otherwise classified
ipOptionsRouterAlert	IP Router Alert
ipOsi	OSI packets
ipReassembly	IP packets that have been reassembled on a server card
ipRouteNoRoute	IP packets with no route indication
ipRouteToSrpEthernet	Packets routed to the SRP Ethernet
ipTtlExpired	IP TTL expired

DoS Protection Group Configuration Example

NOTE: To configure a DoS protection group for an interface, you must configure the settings under the default group, which is the only group that is currently supported.

To configure a DoS protection group for an interface:

```
host1(config)#dos-protection-group default
host1(config-dos-protection)#protocol AtmOam rate 512
host1(config-dos-protection)#protocol PppoeControl rate 512
host1(config-dos-protection)#protocol IpLocalOther rate 512
```

To display the configuration:

```
host1#show dos-protection-group default
           default (canned-group: defaultCanned)  *modified -- no references

      Protocol       Dest Mod Rate  Burst Weight DropProb Priority  Skip
-------------------- ---- --- ----- ----- ------ -------- --------- ----
Ppp Echo Request     IC     -  2048  1024    100      100 HI green  Y
Ppp Echo Reply       IC     -  2048  1024    100      100 HI green  Y
Ppp Echo Reply Fastp FC     -     0     0    100      100 Data path Y
path
Ppp Control          IC     -  2048  1024    100      100 HI green  N
Atm Control (ILMI)   IC     -  2048  1024    100      100 HI green  Y
Atm OAM              IC     *   512   512    100      100 LO green  N
Atm Dynamic Interfac IC     -  1024   512    100      100 HI yellow N
e Column Creation
Atm Inverse ARP      IC     -   256   128    100      100 LO yellow N
Frame Relay Control  IC     -  2048  1024    100      100 HI green  Y
(LMI)
Frame Relay Inverse  IC     -   256   128    100      100 LO yellow N
Arp
Pppoe Control        IC     *   512   512    100      100 HI yellow N
Pppoe Ppp Config Dyn IC     -  1024   512    100      100 HI yellow N
amic Interface Colum
n Creation
Ethernet ARP Miss    IC     -   256   128    100      100 LO yellow N
Ethernet ARP         IC     -   256   128    100      100 LO yellow N
```

DoS Protection Group Commands

Use the commands described in this section to create DoS protection groups and attach them to different types of interfacesatm dos-protection-group

- Use to attach an ATM DoS protection group to an interface.
- Example

  host1(config-if)#**atm dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

bridge1483 dos-protection-group

- Use to attach a bridge 1483 DoS protection group to an interface.
- Example

  host1(config-if)#**bridge1483 dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

dos-protection-group

- Use to create a DoS protection group and enter DoS Protection Group Configuration mode.
- A group named default always exists.
- Example

  host1(coonfig)#**dos-protection-group default**

- Use the **no** version to remove the DoS protection group.

ethernet dos-protection-group

- Use to attach an Ethernet DoS protection group to an interface.
- Example

  host1(config-if)#**ethernet dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

frame-relay dos-protection-group

- Use to attach a Frame Relay DoS protection group to an interface.
- Example

  host1(config-if)#**frame-relay dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

hdlc dos-protection-group

- Use to attach an HDLC DoS protection group to an interface.
- Example

  host1(config-if)#**hdlc dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

ip dos-protection-group

- Use to attach an IP DoS protection group to an interface.
- Example 1

  host1(config-if)#**ip dos-protection-group group1**

- Example 2

  host1(config)#**dos-protection-group default**
  host1(config-dos-protection)#**protocol Atm0am rate 512**
  host1(config-dos-protection)#**protocol PppoeControl rate 512**
  host1(config-dos-protection)#**protocol IpLocalOther rate 512**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

ipv6 dos-protection-group

- Use to attach an IPv6 DoS protection group to an interface.
- Example

  host1(config-if)#**ipv6 dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

lag dos-protection-group

- Use to attach a LAG DoS protection group to an interface.
- Example

  host1(config-if)#**lag dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

ppp dos-protection-group

- Use to attach a PPP DoS protection group to an interface.
- Example

  host1(config-if)#**ppp dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

pppoe dos-protection-group

- Use to attach a PPPoE DoS protection group to an interface.
- Example

  host1(config-if)#**pppoe dos-protection-group group1**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

priority burst

- Use to set the burst size in packets for the priority.
- Example

  host1(config-dos-protection)#**priority Hi-Green-IC burst 32**

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

priority over-subscription-factor

- Use to set the oversubscription value for the priority rate limiter.
- The oversubscription value and the priority rate are used to calculate the minimum rate limits for port compression.
- Allows an oversubscription of the priority rate because all protocols within a priority are not generally used simultaneously.
- Example

  host1(config-dos-protection)#**priority Hi-Green-IC over-subscription-factor 100**

- Use the **no** version to return no oversubscription value.

priority rate

- Use to set the rate in packets-per-second for the priority.
- Example

  host1(config-dos-protection)#**priority Hi-Green-IC rate 6000**

- Use the **no** version to return to the default value of 0.

protocol burst

- Use to set the burst size in packets-per-second for the protocol.
- The default value is one half the maximum rate in packets.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc burst 65535**

- Use the **no** version to set the default value, which is equal to half of the configured maximum rate.

protocol drop-probability

- Use to map a protocol to a specific drop probability, which is the percentage probability of an exceeded packet being dropped.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc drop-probability 100**

- Use the **no** version to set the drop probability to the value specified in the associated default group.

protocol priority

- Use to set the priority for the protocol.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc priority hiGreen**

- Use the **no** version to set the priority to the value specified in the associated default group.

protocol rate

- Use to map a protocol to a maximum rate limit.
- The rate limit applies to all packets of the protocol for interfaces belonging to the DoS protection group.
- A particular protocol can be up to the sum of the four rates configured, depending on the DoS group attached to an interface.
- Use a maximum rate of 0 for protocols that are not used.
- The actual rate never exceeds the maximum rate, but can be less than the configured maximum rate due to the weighting of the protocols within a DoS protection group and the use of multiple DoS protection groups.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc rate 100**

- Use the **no** version to set the value to the value specified in the associated default group.

protocol skip-priority-rate-limiter

- Use to set the skip priority rate limiter for the protocol.
- The specified protocol is not subject to the priority rate limiter for the priority and DoS protection group selected.
- The default sets the protocol such that it is subject to priority rate limiting.
- Example

  host1(config-dos-protection)#**protocol IpLocalDhcpIc skip-priority-rate-limiter**

- Use the **no** version to set the value to the default, which is not to use skip-priority-rate-limiter.

protocol weight

- Use to set the weight for the protocol.
- For each port compression, weight determines the effective minimum rate that each protocol receives.
- Within each port compression, the sum of the minimum rates for all protocols is equal to or less than the priority rate.
- For each priority, there is a separate rate for each DoS protection group.
- Example

  host1(config-dos-protection)#**protocol lpLocalDhcpIc weight 100**

- Use the **no** version to set the weight to the value specified in the associated default group.

use canned-group

- Use to create a DoS protection group that uses a pre-programmed set of parameters.
- Use the **revert** keyword to return the values to the canned group values
- Example

  host1#**use canned-group group1**

- Use the **no** version to associate the group with the default canned group settings.

vlan dos-protection-group

- Use to attach a VLAN DoS protection group to an interface.
- Example

  host1(config-if)#**vlan dos-protection-group**

- Use the **no** version to remove the attachment of the DoS protection group from the interface.

Monitoring DoS Protection Groups

Use the commands described in this section to monitor DoS protection groups.

show dos-protection-group

- Use to display DoS protection groups.
- If you do not specify a group, displays the names of the currently configured DoS protection groups.
- If you specify a group, displays information about the specified group.
- If you do not specify the **brief** keyword, displays a list of references (interfaces and templates) to the DoS protection group,
- When *modified* appears next to the name of the DoS protection group. the group or protocol within the group has changed from the preprogrammed value of the associated group.

- Example

```
host1(config)#show dos-protection-group
DOS Protection Groups:
        Default (canned-group: “default”)  *modified*
        Uplink  (canned-group: “link” }
        ATM     (canned-group: “pppoe” )   *modified*
        VLAN    (canned-group: “mixed-access”)
```

Chapter 10

Writing CLI Macros

An E-series router has an embedded macro language that enables you to define and run macros that can generate and execute CLI commands. Macro files—identified by the *.mac* extension—can be used to store more than one macro. Depending on your needs, you might want to store all of your macros in one file, group macros by function, or store only one macro per file.

This chapter contains the following sections:

- Platform Considerations on page 495
- Writing Macros on page 495
- Detecting and Recording Macro Errors on page 509
- Running Macros on page 514
- Practical Examples on page 516

Platform Considerations

Macros are supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Writing Macros

You must write macros on your computer, not on the E-series router. The macros can contain loops, variables, string and numeric values, and conditional statements. Macros can invoke other macros (as long as they are contained within the same macro file), including themselves, but infinite recursion is not permitted. Macros are case-insensitive.

Macros consist of *control expressions* and *noncontrol expressions*. Control expressions are enclosed by *control brackets*, which are angle-bracket and number sign pairs, like this: **<#** *controlExpression* **#>**. Examples of control expressions include the macro name and macro end statements, and *while* loops. A control expression can include multiple operation statements if you separate the statements with semicolons (;). For example:

```
<# i:=0; while i++ < 3 #>
```

All macros must have names consisting only of letters, numbers, and the underline character (_). The first character of a macro name cannot be a number. If you include more than one macro within a macro file, each macro must have a unique name. The first line of a macro defines the macro's name:

```
<# macroName #>
```

Noncontrol expressions are not enclosed by control brackets and simply become part of the generated CLI command text.

You must end all macros with the following control expression:

```
<# endtmpl #>
```

You can add comments to your control expressions to clarify the code by prefacing the comment with forward slashes (//) inside the control brackets:

```
<# endtmpl //A comment in the macro end expression #>
```

Text after the // is ignored when the macro is run and is not displayed by the CLI.

You can also add comments outside the control expressions by prefacing the comment with an exclamation point (!). The CLI displays these comments if you use the **test** or **verbose** keywords with the **macro** command; the CLI never interprets these comments as commands.

```
!This is a comment outside any control expression
```

You can improve the readability of a macro by using tabs to indent expressions. Leading and trailing tabs have no effect on the macro output, because they are removed when the macro is run.

Example The following is a simple macro that you can use to configure the IP interface on the Fast Ethernet port of the SRP module after you have restored the factory defaults:

```
<# ipInit #>
<# ipAddress := env.getline ("IP Address of System?") #>
ena
conf t
int f0/0
ip addr <# ipAddress; '\n' #>
ip route 10.0.0.0 255.0.0.0 192.168.1.1
host pk 10.10.0.166 ftp
<# endtmpl #>
```

Environment Commands

Macros use environment commands to write data to the macro output, to determine a value, or to call other commands. Table 57 describes the environment commands that are currently supported.

Table 57: Environment Commands

Command	Description
env.delay(int *delay*)	Causes the macro to delay further execution for the number of seconds specified by *delay*
env.getLine	Prompts the user with a question mark (?) and waits for a response
env.getLine(string *prompt-string*)	Prompts the user with the value of *prompt-string* and waits for a response
env.getLineMasked	Prompts the user with a question mark (?), waits for a response, and echoes the response with an asterisk (*) for each character entered by the user
env.getLineMasked(string *prompt-string*)	Prompts the user with the value of *prompt-string*, waits for a response, and echoes the response with an asterisk (*) for each character entered by the user
env.argc	Returns the number of arguments passed to the macro
env.argv(n)	Returns the value of the nth argument, such that 1 < = n < = env.argc The returned value is a string, not a number; if you want to use this value for a subsequent numeric operation, you must first convert it to a number with the env.atoi(*string*) command
env.argv(0)	Returns the name of the macro
env.atoi(*string*)	Converts the specified string to a numeric value
env.atoi(env.argv(n))	Converts input values to integers
env.setResult	Sets parameters within a macro for display through the macroData log at the NOTICE severity level following the completion of the macro
env.getErrorCommand	Returns the command string that triggered a macro error
env.getErrorStatus	Returns the reason for a triggered error

Variables

A local variable enables you to store a value used by the macro while it executes. The macro can modify the value during execution. Local variables can be integers, real numbers, or strings. The initial value of local variables is zero.

Like macros, local variables must have a name consisting only of letters, numbers, or the underline character (_). The variable name must not begin with a number. You must not use a reserved keyword as a variable name. A line that ends with a variable needs a new line character at the end of the line.

Literals

A literal is an exact representation of numeric or string values. Every number is a literal. Place single or double quotation marks around a string to identify it as a string literal. You can specify special characters within a literal string by prefacing them with a backslash as follows:

quotation mark	\’
double quotation mark	\”
tab	\t
carriage return	\r
new line	\n
string end	\0
backslash	\\

Examples

```
42
98.6
‘string literal’
“count”
“\t this string starts with a tab and ends with a tab \t”
```

Operators

You can use operators to perform specific actions on local variables or literals, resulting in some string or numeric value. Table 58 lists the available macro operators in order of precedence by operation type. Operators within a given row are equal in precedence.

Table 58: Macro Operators

Operation Type	Operators						
Extraction	substr()	rand()	round()	truncate()			
String	$						
Multiplicative	*	/	%				
Arithmetic	+	–	+ +	– –			
Relational	<	>	< =	> =	=	! =	
Logical	||	&&	!				
Assignment	: =						
Miscellaneous	[ ]	,	( )	.	;	< #	# >

Table 59 briefly describes the action performed by each operator.

Table 59: Operator Actions

Operation	Operator	Action
Arithmetic (binary)	+	Adds the right and left sides together
Arithmetic (binary)	–	Subtracts the element to the right of the operator from the element to the left of the operator
Assignment	: =	Evaluates the elements to the right of the operator, then assigns that value to the local variable to the left of the operator
Combine	$	Creates a new string by joining the values of the right and left sides; converts any numeric values to strings before joining
Less than	<	Evaluates as true (returns a 1) if the element to the left of the operator is *less than* the expression to the right of the operator; otherwise the result is false (0)
Greater than	>	Evaluates as true (returns a 1) if the element to the left of the operator is *greater than* the expression to the right of the operator; otherwise the result is false (0)
Less than or equal to	< =	Evaluates as true (returns a 1) if the element to the left of the operator is *less than or equal to* the expression to the right of the operator; otherwise the result is false (0)
Greater than or equal to	> =	Evaluates as true (returns a 1) if the element to the left of the operator is *greater than or equal to* the expression to the right of the operator; otherwise the result is false (0)
Equal to	=	Evaluates as true (returns a 1) if the element to the left of the operator is equivalent to the expression to the right of the operator; otherwise the result is false (0)
Not equal to (logical NOT)	! =	Evaluates as true (returns a 1) if the element to the left of the operator is not equal to the expression to the right of the operator; otherwise the result is false (0)
Logical OR	||	Evaluates as true (returns a 1) if the values of either the left or right sides is nonzero; evaluation halts at the first true (1) expression
Logical AND	&&	Evaluates as true (returns a 1) if the values of the left and right sides are both nonzero; evaluation halts at the first false (0) expression
Miscellaneous	[ ]	See *Invoking Other Macros* on page 507 for usage.
Miscellaneous	,	See *While Constructs* on page 505 for usage.
Miscellaneous	( )	Groups operands and operators to achieve results different from simple precedence; effectively has the highest precedence
Miscellaneous	.	Provides access to environment commands; see Table 57. Provides access to macros; see *Invoking Other Macros*
Miscellaneous	;	Separates operation statements within a control expression
Miscellaneous	< # # >	Encloses control expressions
Multiplication	*	Multiplies the expression to the left of the operator by the expression to the right

Table 59: Operator Actions (continued)

Operation	Operator	Action
Division	/	Divides the expression to the left of the operator by the expression to the right
Modulo	%	Divides the expression to the left of the operator by the expression to the right and returns the integer remainder. If the expression to the left of the operator is less than the expression to the right, then the result is the expression to the left of the operator.
Postincrement	+ +	Increments the variable after the expression is evaluated
Postdecrement	– –	Decrements the variable after the expression is evaluated
Preincrement	+ +	Increments the variable before the expression is evaluated
Predecrement	– –	Decrements the variable before the expression is evaluated
Negation	!	Reverses the logical state of its operand. 0 is returned for nonzero operands. 1 is returned for operands that evaluate to zero.
Arithmetic (unary)	+	Provides the absolute value of the value
Arithmetic (unary)	–	Provides the inverse of the value
Substring	substr()	Extracts a portion of a string
Randomize	rand()	Generates a random integer between the provided endpoints, inclusive
Round	round()	Rounds the value to the nearest integer
Truncate	truncate()	Truncates a noninteger value to the value left of the decimal point

Assignment

Use the assignment operator (: =) to set the value of a local variable. The expression to the right of the operator is evaluated, and then the result is assigned to the local variable to the left of the operator. The expression to the right of the operator can include the local variable if you want to modify its current value.

Example

```
<# i := i + 1 #>
<# count := count - 2 #>
```

Increment and Decrement

You can use the increment operator (+ +) to increase the value of a local variable by one. You specify when the value is incremented by the placement of the operator. Incrementing occurs after the expression is evaluated if you place the operator to the right of the operand. Incrementing occurs before the expression is evaluated if you place the operator to the left of the operand.

Example 1

```
<# i := 0; j := 10 #>
<# j := j - i++ #>
```

In Example 1, the result is that *i* equals 1 and *j* equals 10, because the expression is evaluated (10 – 0 = 10) before *i* is incremented.

Example 2

```
<# i := 0; j := 10 #>
<# j := j - ++i #>
```

In Example 2, the result is still that *i* equals 1, but now *j* equals 9, because *i* is incremented to 1 before the expression is evaluated (10 – 1 = 9).

Similarly, you can use the decrement operator (– –) to decrement local variables. Placement of the operator has the same effect as for the increment operator.

When a local variable with a string value is used with the increment or decrement operators, the value is permanently converted to an integer equal to the length in characters of the string value.

String Operations

The combine operator ($) concatenates two strings into one longer string. Numeric expressions are converted to strings before the operation proceeds. The variable *local* evaluates to "want a big":

Example

```
\<# local := "want a " $ "big" #>
```

Extraction Operations

The extraction operations are substring (substr), randomize (rand), round, and truncate. These operators are equal in precedence, and all take precedence over the string operator.

You can use the substring operator (substr) to extract a shorter string from a longer string. To use the substring operator, you must specify the source string, an offset value, and a count value. You can specify the string directly, or you can specify a local variable that contains the string. The offset value indicates the place of the first character of the substring to be extracted; "0" indicates the first character in the source string. The count value indicates the length of the substring. If the source string has fewer characters than the sum of the offset and count values, then the resulting substring has fewer characters than indicated by the count value.

Example

```
<# local := "want a " $ "big" $ " string" #>
<# substr(local, 5, 12) #>The result is "a big string"
<# substr(local, 0, 10) #>The result is "want a big"
<# substr("ready", 0, 4) #>The result is "read"
```

The random operator produces a random integer value from the specified inclusive range; in the following example, the result is between 1 and 10:

```
<# number:= rand(1,10) #>
```

The round operator rounds off the number to the nearest integer:

```
<# decimal:= 4.7 #>
<# round(decimal) #>The result is decimal is now 5
```

The truncate operator truncates noninteger numbers to the value left of the decimal point:

```
<# decimal:= 4.7 #>
<# truncate(decimal) #>The result is decimal is now 4
```

Arithmetic Operations

The arithmetic operations are multiply (*), divide (/), modulo (%), add (+), and subtract (-). Multiply, divide, and modulo are equal in precedence, but each has a higher precedence relative to add and subtract. Add and subtract are equal in precedence.

Example

```
<# 4 % 3 + 12 - 6 #>The result is 7
```

When a local variable with a string value is used with arithmetic operators, the value is temporarily converted to an integer equal to the length in characters of the string value. You can use the env.atoi commands to avoid this situation.

Relational Operations

The relational operations compare the value of the expression to the left of the operator with the value of the expression to the right. The result of the comparison is 1 if the comparison is true and 0 if the comparison is false.

If the expressions on both sides of the operator are strings, they are compared alphabetically. If only one expression is a string, the numeric value is used for comparison. Arithmetic operators have a higher precedence.

Example

```
<# i := 9; i++ < 10 #>The result is 1
<# i := 9; ++i < 10 #>The result is 0
```

Logical Operations

You can use the logical operators AND (&&), OR (||), and NOT (!) to evaluate expressions. The result of the operation is a 1 if the operation is true and 0 if the operation is false.

For the logical AND, the result of the operation is true (1) if the values of the expressions to the left and right of the operator are both nonzero. The result of the operation is false (0) if either value is zero. The evaluation halts when an expression is evaluated as zero.

For the logical OR, the result of the operation is true (1) if the values of the expression on either the left or right of the operator is nonzero. The result of the operation is false (0) if both values are zero. The evaluation halts when an expression is evaluated as nonzero.

The NOT operator must precede the operand. The operation inverts the value of the operand; that is, a nonzero expression becomes 0, and a zero expression becomes 1. For the logical NOT, the result of the operation is true (1) if it evaluates to zero, or false if it evaluates to nonzero.

Example

```
<# i := 6; i >= 3 && i <= 10 #>The result is 1
<# i := 1; i >= 3 && i <= 10 #>The result is 0
<# i := 6; i >= 3 || i <= 10 #>The result is 1
<# i := 1; i >= 3 && i <= 10 #>The result is 0
<# i := 5; !i #> The result is 0
<# i := 5; j := 0; !i && !j #>The result is 0
<# i := 5; j := 0; !i || !j #>The result is 1
```

Relational operators have a higher precedence than logical AND and OR. The NOT operator is equal in precedence to the increment and decrement operators.

Miscellaneous Operations

The positive (+) and negative (-) operations must precede the operand. The result of a positive operation is the absolute value of the operand. The result of a negative operation is the negative value of the operand; that is, a + (-5) becomes 5 and a -(-2) becomes 2. These operators have the same precedence as the increment and decrement operators. If there is an operand on both sides of these operators, they are interpreted as the add and subtract operators.

Example

```
<# local_abs := +local #>
<# local_neg := -local #>
```

All operations are performed in the order implied by the precedence of the operators. However, you can modify this order by using parentheses (**( )**) to group operands and operators. Operations within parentheses are performed first. The result is that of the operations within the parentheses.

Example

```
<# 4 % (3 + 12) - 6 #>The result is -6
<# 5 && 2 > 1 #>The result is 1
<# (5 && 2) > 1 #>The result is 0
```

Results of control expressions are written to the output stream when the expression consists of the following:

- A single local variable
- A single literal element
- An operation whose result is not used by one of the following operations:

assignment	predecrement	postdecrement	while
if	preincrement	postincrement	

Example

```
<# localvar #>value of localvar is written
<# " any string" #>“ any string” written
<# 4 % 3 + 12 - 6 #>“7” is written
<# 4 % (3 + 12) - 6 #>“-6” is written
<# i := i + 1 #>nothing is written
<# count := (count - 2) #>nothing is written
```

Conditional Execution

You can use *if* or *while* constructs in macros to enable conditional execution of commands.

If Constructs

If constructs provide a means to execute portions of the macro based on conditions that you specify. An *if* construct consists of the following components:

- An opening *if* expression
- A group of any number of additional expressions
- (Optional) Any number of *elseif* expressions and groups of associated expressions

- (Optional) An *else* expression and any associated group of expressions
- An *endif* expression to indicate the end of the *if* structure

The *if* expression and any optional *elseif* expressions must include a lone environment value command, a local variable, a literal, or some operation using one or more operators.

Only one of the groups of expressions within the *if* construct is executed, according to the following scheme:

1. The *if* expression is evaluated. If the result is true (nonzero), the associated expression group is executed.
2. If the result is false (zero), then the first *elseif* expression, if present, is evaluated. If the result is true (nonzero), the associated expression group is executed.
3. If the result of evaluating the first *elseif* expression is false (zero), the next *elseif* expression is evaluated, if present. If the result is true (nonzero), the associated expression group is executed.

   If all *elseif* expressions evaluate to false (zero) or if no *elseif* expressions are present, then the *else* expression group—if present—is executed.
4. This evaluation process continues until an expression evaluates to nonzero. If there is no nonzero evaluation, then no expression group is executed.

You can write an empty expression group so that no action is performed if this group is selected for execution. You can nest *if* structures within other *if* structures or *while* structures.

The following sample macro demonstrates various *if* structures:

```
<#            if_examples                      #>
<# //---------------------------------------- #>

<# if 1 #>
! This is always output because any nonzero value is “true.”
<# endif #>

<# if 0 #>
! This is never output because a value of zero is “false.”
<# endif #>

<# // Here’s an example with elseif and else. #>
<# color := env.getline("What is your favorite color? ") #>
<# if color = "red" #>
    ! Red is my favorite color, too.
<# elseif color = "pink" #>
    ! Pink is a lot like red.
<# elseif color = "black" #>
    ! Black is just a very, very, very dark shade of red.
<# else #>
    ! Oh.  That’s nice.
<# endif #>

<# // Here’s a nested if example. #>
```

```
<# sure := env.getline("Are you sure that " $ color $ " is your favorite
color? ") #>
<# if substr(sure, 0, 1) = 'y' || substr(sure, 0, 1) = 'Y' #>
    <# if color != "black" && color != "white";
        shade := env.getline("Do you prefer dark " $ color $
                                " or light " $ color $ "? ") #>
        <# if shade = "dark" #>
            ! I like dark colors, too.
        <# elseif shade = "light" #>
            ! I prefer dark colors myself.
        <# else #>
            ! Hmmm, that's neither dark nor light.
        <# endif #>
    <# else #>
        ! Oh.  That's nice.
    <# endif #>
<# else #>
! I didn't think so!
<# endif #>
<# endtmpl #>
```

While Constructs

While constructs provide a means to repeatedly execute one or more portions of the macro based on a condition that changes during the execution. A *while* construct consists of the following components:

- An opening *while* expression
- A group of any number of additional expressions
- An *endwhile* expression to indicate the end of the *while* structure

The *while* expression must include a lone environment value command, a local variable, a literal, or some operation using one or more operators. Each time that this expression evaluates to nonzero, the associated expression group is executed.

You can place an iteration expression after the *while* expression. This optional expression is evaluated after each execution of the *while* expression group.

You can include *if* structures within a *while* structure. You can also include special control expressions indicated by the *break* or *continue* expressions. The *break* expression breaks out of the *while* structure by halting execution of the expression group and executing the first expression after the *endwhile* statement. The *continue* expression skips over the rest of the expression group, evaluates any iteration expression, then continues with the execution of the *while* structure. The *while* structure is limited to 100,000 repetitions by default. You can nest up to 10 *while* structures.

Example The following sample macro demonstrates various *while* structures:

```
<#               while_examples               #>
<# //---------------------------------------- #>
<# // Remember that variables are automatically initialized to 0. #>
! Table of squares of the first 10 integers:
<# while ++i <= 10 #>
!<#i;"  ";i*i;"\n"#>
<# endwhile #>
```

```
<# // Remember that the value of a string used as an integer is the number. #>
<# // of characters in the string.                                          #>
<# stars := "*" #>
<# while stars < 10, stars := stars $ "*"#>
!<# stars;"\n" #>
<# endwhile #>
<# while stars > 0, stars := substr(stars, 0, stars-1)#>
!<# stars;"\n" #>
<# endwhile #>

<# // An example of the continue and break statements. #>
<# // Also note that many statements can be grouped. #>
! All the positive even numbers less than 11
<# i:=0; while ++i < 100 #>
    <#if i%2; continue; endif; if i > 10; break; endif; "!" $ i $ "\n"; #>
<# endwhile #>

<# // While constructs will NOT iterate forever. #>
<# while 100 > 0 // This is always true, but the macro will eventually stop #>
<# ++iterations; endwhile #>
! The while loop iterated <#iterations#> times.
<# endtmpl #>
```

Passing Parameters in Macros

You can pass parameters to an entry macro. The system translates these parameters to the correct data type.

NOTE: The env.argv array is separate from this feature and still functions as designed. In other words, the env.argv array continues to pass parameters as text strings. To use env.argv array values for subsequent numeric operations, you must first convert the values to a number by using the env.atoi(string) command.

Example The following macro (saved as *m.mac*) uses values specified in a CLI command to compute the final result:

```
<# m(left,right,third) #>
<# multi := left * right #>
<# multiFinal := multi * third #>
<# setoutput console #>
<# “The result is: multiFinal; “\n” #>
<# endsetoutput #>
<# endtmpl #>
```

The following example provides the output from using this macro:

```
host1#macro m.mac m 5 6 7
host1#The result is: 210
```

Generating Macro Output

You may want a macro to provide output while it is operating. In simple cases, you can use the **verbose** keyword to echo commands to the display and display comments as the macro executes. For more information about the **verbose** keyword, see Example 2 in *Invoking Other Macros* on page 507.

When running more complex macros or macros that contain a lot of commands or comments, you may want to output only certain information (that is, not all commands and comments). In this case, you can use < # setoutput console # > to send the information directly to the console display when it executes.

Example 1 The following example shows how you can send output directly to the console:

```
<# setoutput console #>
This message appears in the console window (whether or not you use verbose mode).
<#endsetoutput #>
```

Example 2 The following example shows how you can send a single argument to the console:

```
<# puts (msg) #>
!====================================================================
!====================================================================
! output "msg" to console
!====================================================================
!====================================================================
<# setoutput console #>
<# msg; "\n"#>
<#endsetoutput #>
<# endtmpl #>
!====================================================================
!====================================================================
<# tmpl.puts("Hello World")
```

Invoking Other Macros

Macros can invoke other macros within the same macro file; a macro can also invoke a macro from another macro file if the invocation takes place in literal text, that is, not within a control expression. A macro can invoke itself directly or indirectly (an invoked macro can invoke the macro that invoked it); the number of nested invocations is limited to 10 to prevent infinite recursion.

Within each macro, you can specify parameters that *must* be passed to the macro when it is invoked by another. You must specify named variables enclosed in parentheses after the macro name in the first line of the macro, as shown in this example:

```
<# macroName (count, total) #>
```

Additional parameters can be passed as well. Parameters can be local variables, environmental variables, literals, or operations. The invoking macro passes local variables by reference to the invoked macro. Passing parameters has no effect on the invoking macro unless the parameter is a local variable that is changed by the invoked macro. When the invoked macro completes execution, the local variable assumes the new value for the invoking macro.

The invoked macro can use the **param[***n***]** expression to access parameters passed to it, where *n* is the number of the parameter passed. This is useful if optional parameters can be passed to a macro or if the same iterative algorithm needs to process the parameters.

Use the expression **param[0]** to return the total number of parameters passed to the macro. Use the **return** keyword to halt execution of the invoked macro and resume execution of the invoking macro. Use the **exit** keyword to halt execution of all macros.

Example 1 The following sample macro demonstrates macro invocation:

```
<#            invoking_examples               #>
<# //------------------------------------- #>
<# name := env.getline("What is your first name? ") #>
! First, <#name#>, we will invoke the if_examples and
! the while_examples macros...
<# tmpl.if_examples; tmpl.while_examples #>
! Hey <#name#>, have you noticed that your name backwards is:
!<# eman:= ""; tmpl.reversestring(name, eman); eman; "\n"#>
<#  tmpl.argumentlist("a", "b", "c")#>
<# endtmpl #>

<# argumentlist #>
<# if param[0] = 0; return; endif #>
! argumentList() was called with the following arguments:
<# while ++i <= param[0]#>
    ! <#param[i];"\n"#>
<# endwhile #>
<# endtmpl #>

<# reversestring (string, gnirts) #>
<# i := 0 + string; // i is now equal to the number of characters in string. #>
<# while --i >= 0; gnirts := gnirts $ substr(string, i, 1); endwhile #>
<# endtmpl #>
```

Example 2 The following macro in file macro1.mac invokes a macro from within another file, macro2.mac:

```
<# callAnotherMacro #>
   <# localVar := 5 #>
   macro macro2.mac macroName2 <# localVar #> string1
<# endtmpl #>
```

This macro passes the value of localVar to macroName2. The value of localVar remains at 5 for callAnotherMacro, regardless of any operations upon that variable in the second macro. In other words, an invoked macro in another file cannot return any values to the invoking macro.

The output of callAnotherMacro looks like this:

```
host1#macro verbose macro1.mac callAnotherMacro
host1#!Macro 'callAnotherMacro' in the file 'macro1.mac' starting execution (Id: 55)
macro macro2.mac macroName2 5 string1
!Macro 'macroName2' in the file 'macro2.mac' starting execution
!Macro 'macroName2' in the file 'macro2.mac' ending execution
host1#!Macro 'callAnotherMacro' in the file 'macro1.mac' ending execution (Id: 55)
```

The invoked macro cannot invoke a third macro from another file. Only a single level of invocation is supported.

Detecting and Recording Macro Errors

You can control how a macro responds when an error occurs during execution. By creating and adding an onError macro to your macro file, you can specify that, on the occurrence of an error, macro execution within the current macro stops and the onError macro is invoked. An onError macro can call other macros. If another error occurs after the onError macro is invoked, macro execution stops again and the onError macro is invoked again. This process continues either until the onError macro completes or until reaching the recursion limit of 10.

Detectable Macro Errors

CLI macros detect various errors when a macro is executed. Some of these errors are detected without the use of an onError macro; they include the following:

- Macro file not found
- Macro not found
- Macro compilation error
- Macro does not complete error due to excessive looping or recursion

The following errors are detected only when a CLI macro file contains an onError macro:

- Syntactic error in executed CLI command
- Runtime error in executed CLI command

In addition to these detectable errors, you can use the following environment commands to return textual error information to the macroData log file:

- env.getErrorCommand
- env.getErrorStatus

CAUTION: Though you can use the **env.getErrorCommand** and **env.getErrorStatus** commands in any macro, the only appropriate place from which to execute these commands is from an onError macro.

Logging Macro Results

You can use the **env.setResult** command to set parameters within a macro to display information through the macroData log file. When defined, parameter information appears in the macroData log file at the NOTICE severity level following the completion of the macro.

The following example defines several results (1 through 5):

```
<# numberMacro #>
<# env.setResult("A", ""$1 ) #>
<# env.setResult("A", ""$2 ) #>
<# env.setResult("A", ""$3 ) #>
```

```
<# env.setResult("A", ""$4 ) #>
<# env.setResult("A", ""$5 ) #>
<#endtmpl#>
```

Each value is sent to the macroData log file, starting with 1 and ending with 5. Each successive value overwrites the previous value in the log file. In other words, if the macro ends after setting the third result (that is, 3) the log file displays the following:

A is 3

If the macro finishes completely, the log file displays the following:

A is 5

Viewing Macro Errors

You can view macro error information in the macroData log file using the **show log data** command and specifying the **macroData** keyword for the category.

NOTE: Each execution of a macro, by any user and by any name, obtains a unique ID. This ID appears in the starting and ending message of the macro output and for each log message in the macroData log.

show log data

- Use to display log event data using the **category** keyword and the macroData category.
- **delta**—Limits the display to events that occurred after the time set with the log baseline command.
- **severity**—Displays events that have a specific severity level.
- Example

```
host1(config)#show log data category macroData severity debug
NOTICE 01/07/2006 09:46:57 macroData: Macro 'badInterfaceCommandMacro' in file
'testInterfaceCommand.mac' starting execution (Id: 402) on vty, 0
ERROR 01/07/2006 09:46:57 macroData: (Id: 402) Command error:  interface fastEthernet 500, Command
execution error
NOTICE 01/07/2006 09:46:57 macroData: (Id: 402) commandError is interface fastEthernet 500
NOTICE 01/07/2006 09:46:57 macroData: (Id: 402) commandErrorStatus is Command execution error
NOTICE 01/07/2006 09:46:57 macroData: (Id: 402) runStatus is Loop:500
NOTICE 01/07/2006 09:46:57 macroData: Macro 'badInterfaceCommandMacro' in file
'testInterfaceCommand.mac' ending execution (Id: 402) on vty, 0
```

onError Macro Examples

The following examples provide an indication of how the onError macro can assist in using and troubleshooting macro files. The examples purposely contain errors and show the result when using the onError macro.

Detecting Invalid Command Formats

In this example, the following macro file (*badInterfaceCommand.mac*) performs a loop. Within each loop, the CLI executes the **interface fastEthernet** command using an invalid interface format:

```
<# badInterfaceCommandMacro #>
<# env.setResult("runStatus","start" ) #>
<# theLoopCount := 500 #>
conf t
  <# while theLoopCount > 0 #>
  <# env.setResult("runStatus", "Loop:" $ theLoopCount ) #>
  interface fastEthernet <# theLoopCount; '\n' #>
  <# –theLoopCount #>
  <# endwhile #>
<# env.setResult("runStatus","complete" ) #>
<#endtmpl#>

<# onError #>
<# env.setResult("commandError", env.getErrorCommand) #>
<# env.setResult("commandErrorStatus", env.getErrorStatus) #>
<#endtmpl#>
```

If the macro were to run to completion, the CLI would execute the commands as follows:

```
interface fastEthernet 500
interface fastEthernet 499
.
.
.
interface fastEthernet 1
```

Because the macro uses invalid interface formats, executing the macro without the embedded onError macro would result in error output for each loop. However, the onError macro detects the error and stops the macro. Using the onError macro, the output appears as follows:

```
host1(config)#macro testInterfaceCommand.mac badInterfaceCommandMacro

Macro 'badInterfaceCommandMacro' in file 'testInterfaceCommand.mac' starting execution (Id: 402)
Enter configuration commands, one per line.  End with ^Z.
ERX-40-94-fb(config)#interface fastEthernet 500
                                            ^
% invalid interface format
Macro 'badInterfaceCommandMacro' in file 'testInterfaceCommand.mac' ending execution (Id: 402)
```

You can determine the execution progress through the runStatus result entry in the macroData log file. For this example, the runStatus value of 500 indicates that the macro ended early.

```
host1(config)#show log data category macroData severity debug
NOTICE 01/07/2006 09:46:57 macroData: Macro 'badInterfaceCommandMacro' in file
'testInterfaceCommand.mac' starting execution (Id: 402) on vty, 0
ERROR 01/07/2006 09:46:57 macroData: (Id: 402) Command error:  interface fastEthernet 500, Command
execution error
NOTICE 01/07/2006 09:46:57 macroData: (Id: 402) commandError is interface fastEthernet 500
```

```
NOTICE 01/07/2006 09:46:57 macroData: (Id: 402) commandErrorStatus is Command execution error
NOTICE 01/07/2006 09:46:57 macroData: (Id: 402) runStatus is Loop:500
NOTICE 01/07/2006 09:46:57 macroData: Macro 'badInterfaceCommandMacro' in file
'testInterfaceCommand.mac' ending execution (Id: 402) on vty, 0
```

Detecting Invalid Commands

In this example, the following macro file (*badExecCommand.mac*) is programmed to executes four exec mode commands. However, the second command in the sequence is invalid.

```
<# badExecCommandMacro #>
<# env.setResult("runStatus","start" ) #>
show clock
<# env.setResult("runStatus","after first show clock" ) #>
foo
<# env.setResult("runStatus","after foo" ) #>
show privilege
<# env.setResult("runStatus","after show privilege" ) #>
show clock
<# env.setResult("runStatus","complete" ) #>
<#endtmpl#>

<# onerror #>
<# errCmd := env.getErrorCommand #>
<# errStatus := env.getErrorStatus #>
<# env.setResult("commandError", errCmd) #>
<# env.setResult("commandErrorStatus", errStatus) #>
<#endtmpl#>
```

If the macro were to run to completion, the following commands would be executed:

```
show clock
foo
show privilege
show clock
```

Without the onError macro, the macro would indicate the invalid command, but it would also continue with the rest of the configuration. When using the onError macro, the macro stops when it encounters the invalid command.

Executing the macro that contains the onError macro, the output appears as follows:

```
host1#macro badExecCommandTest.mac badExecCommandMacro

Macro 'badExecCommandMacro' in file 'badExecCommandTest.mac' starting execution (Id: 101)
SUN JAN 08 2005 07:21:50 UTC
ERX-40-94-fb#foo
             ^
% Invalid input detected at '^' marker.
Privilege level is 15
Macro 'badExecCommandMacro' in file 'badExecCommandTest.mac' ending execution (Id: 101)
```

You can determine the execution progress through the runStatus result entry in the macroData log file. For this example, the log output indicates the command error and displays the following to indicate that the macro ended early:

runStatus is after foo

```
host1#show log data category macroData severity debug
NOTICE 01/08/2006 07:14:13 macroData: Macro 'startmin' in file 'master.mac' starting execution (Id: 1)
on vty, 0
NOTICE 01/08/2006 07:14:18 macroData: Macro 'startmin' in file 'master.mac' ending execution (Id: 1) on
vty, 0
NOTICE 01/08/2006 07:21:50 macroData: Macro 'badExecCommandMacro' in file 'badExecCommandTest.mac'
starting execution (Id: 101) on vty, 0
ERROR 01/08/2006 07:21:50 macroData: (Id: 101) Command error: foo, Command syntax error
NOTICE 01/08/2006 07:21:50 macroData: (Id: 101) commandError is foo
NOTICE 01/08/2006 07:21:50 macroData: (Id: 101) commandErrorStatus is Command syntax error
NOTICE 01/08/2006 07:21:50 macroData: (Id: 101) runStatus is after foo
NOTICE 01/08/2006 07:21:50 macroData: Macro 'badExecCommandMacro' in file 'badExecCommandTest.mac'
ending execution (Id: 101) on vty, 0
```

Detecting Missing Macros

In this example, the following macro file (*badMacroInvocation.mac*) is programmed to invoke a missing or nonexistent macro (*tmpl.foo*).

```
<# badMacroInvocation #>
<# env.setResult("runStatus","start" ) #>
<# tmpl.foo #>
<# env.setResult("runStatus","complete" ) #>
<#endtmpl#>

<# onerror #>
<# errCmd := env.getErrorCommand #>
<# errStatus := env.getErrorStatus #>
<# env.setResult("commandError", errCmd) #>
<# env.setResult("commandErrorStatus", errStatus) #>
<#endtmpl#>
```

When using the onError macro, the macro stops when it encounters the missing macro. The output appears as follows:

```
host1#macro badMacroInvocation.mac badMacroInvocation
Macro 'badMacroInvocation' in file 'badMacroInvocation.mac' starting execution (Id: 407)

% can't find macro foo
Macro 'badMacroInvocation' in file 'badMacroInvocation.mac' ending execution (Id: 407)
```

You can determine the execution progress through the runStatus result entry in the macroData log file. For this example, the log output indicates the macro error and displays the following to indicate that the macro ended prior to invoking the macro:

start

```
host1#show log data category macrodata severity debug

NOTICE 05/27/2005 12:39:10 macroData: Macro 'badMacroInvocation' in file 'badMacroInvocation.mac'
starting execution (Id: 407) on vty, 0
ERROR 05/27/2005 12:39:10 macroData: (Id: 407) Command error: foo, macro not found
NOTICE 05/27/2005 12:39:10 macroData: (Id: 407) commandError is foo
```

```
NOTICE 05/27/2005 12:39:10 macroData: (Id: 407) commandErrorStatus is macro not found
NOTICE 05/27/2005 12:39:10 macroData: (Id: 407) runStatus is start
NOTICE 05/27/2005 12:39:10 macroData: Macro 'badMacroInvocation' in file 'badMacroInvocation.mac'
ending execution (Id: 407) on vty, 0
```

Running Macros

Although you must write macros on a computer, you can copy them to the system. Issue the **macro** command from the CLI to execute both local macros and macros stored remotely.

You can display the commands that are generated by the macro file without executing the commands by using the **test** keyword. We recommend you confirm that the test display matches your expectations before you execute the macro to run the commands.

You can terminate a macro while it is running by pressing Ctrl + c. You can close Telnet and SSH windows while a macro is running, but the macro does not terminate until it completes the current command.

macro

- Use to execute a macro that generates—and can execute—CLI commands. This command is available in all command modes.
- This command invokes a hidden FTP client and takes place in the context of the current virtual router (VR) rather than the default VR. You must configure the FTP server so that any traffic destined for the VR can reach the VR; typically, you configure the FTP server to reach the default address of the system, which will always be able to reach the VR.
- You can specify both a macro filename and a macro contained within that file. For example, the following command looks for the file *confatm.mac* and runs the macro named *atm0verDs3* contained within the file:

  host1(config)#**macro confatm.mac atm0verDs3**

- You can specify only a macro filename. The command searches in the specified file for a macro named *start*. The command fails if the *start* macro does not exist. For example, the following command looks for the file *confatm.mac* and runs the macro named *start* contained within the file:

  host1(config)#**macro confatm.mac**

- You can specify only the macro name, using the **name** keyword, if the macro file is stored locally in NVS and has the same name as the included macro you want to invoke. For example, the following command looks for the file *confatm.mac* and runs the macro named *confatm* contained within the file:

  host1(config)#**macro name confatm**

- You must specify a macro filename for remotely stored macro files, as in the following example:

  host1(config)#**macro pc:/macros.mac atm0verDs3**

- You can pass arguments to the macro; if the argument contains a space or other special character, you must enclose the argument within double quotation marks.
- Use the **test** keyword to specify that the macro generate, but not execute, the commands. You can look at the output to verify that it is what you want. The test mode is verbose and displays comments.
- Use the **verbose** keyword to echo commands to the display and display comments as the macro executes. By default the command executes in nonverbose mode.
- There is no **no** version.

Example A typical macro application is to iteratively generate a series of commands, as shown in the following macro, *atm0verDs3*:

```
<# atmOverDs3 #>
<# i:=0; while i++ < 3 #>
    controller t3 9/<#i;'\n'#>
    no shut
    clock source internal module
    framing cbitadm
    ds3-scramble
!
    interface atm 9/<#i;'\n'#>
    atm vc-per-vp 256
!
<# endwhile #>
!
interface atm 9/1.1
encap pppoe
!
<# i:=1; while i < 100 #>
    interface atm 9/1.1.<#i;'\n'#>
        encap ppp
        no ppp shut
        no ppp keep
        atm pvc <# i #> 1 <# i #> aal5mux ip
        ip addr 10.1.<#i#>.1 255.255.255.0
!
<# i++ #>
<# endwhile #>
!
<# endtmpl #>
```

If you stored this macro remotely in the macro file, *pc:/macros.mac*, you issue the following commands to execute the macro:

```
host1>enable
host1#conf t
host1(config)#macro pc:/macros.mac atm0verDs3
```

Alternatively, if you stored this macro locally in the macro file *atm0verDs3.mac*, you issue the following commands to execute the macro:

```
host1>enable
host1#conf t
host1(config)#macro verbose atm0verDs3
```

The following example shows a portion of the output resulting from executing the *atm0verDs3* macro from a local file (the starting and ending comments vary for a remote macro):

```
host1(config)#!Macro 'atmOverDs3' in the file 'atmOverDs3.mac' starting
execution (Id: 103)
host1(config)#controller t3 9/1
host1(config)#no shut
host1(config)#clock source internal module
host1(config)#framing cbitadm
host1(config)#ds3-scramble
host1(config)#interface atm 9/1
host1(config)#atm vc-per-vp 256
host1(config)#controller t3 9/2
host1(config)#no shut
host1(config)#clock source internal module
host1(config)#framing cbitadm
host1(config)#ds3-scramble
host1(config)#interface atm 9/2
host1(config)#atm vc-per-vp 256
host1(config)#controller t3 9/3
host1(config)#no shut
host1(config)#clock source internal module
host1(config)#framing cbitadm
host1(config)#ds3-scramble
host1(config)#interface atm 9/3
host1(config)#atm vc-per-vp 256

host1(config)#interface atm 9/1.1
host1(config)#encap pppoe

host1(config)#interface atm 9/1.1.1
host1(config)#encap ppp
host1(config)#no ppp shut
host1(config)#no ppp keep
host1(config)#atm pvc 1 1 1 aal5mux ip
host1(config)#ip addr 10.1.1.1 255.255.255.0
```

[display omitted]

```
host1(config)#interface atm 9/1.1.99
host1(config)#encap ppp
host1(config)#no ppp shut
host1(config)#no ppp keep
host1(config)#atm pvc 99 1 99 aal5mux ip
host1(config)#ip addr 10.1.99.1 255.255.255.0
host1(config)#!Macro 'atmOverDs3' in the file 'atmOverDs3.mac' ending
execution (Id: 103)
```

Practical Examples

You can use the macros in this section for configuring your router or as examples of useful macros you can build yourself.

Configuring Frame Relay

You can organize your macros in many different ways to suit your needs. The first sample macro in this section, *ds1mac.mac*, shows a typical method of organization. It consists of a number of related macros for configuring interfaces on CT1 and CE1 modules, as described in Table 60.

Some of the macros provide a single configuration function, like configuring the controller. These are invoked by other macros that are executable from the command line. A high-level macro invokes several of the executables, acting much like a script to provide greater functionality.

Table 60: Contents of ds1mac.mac

Macro Name	Description
Help	Lists the executable macros in ds1mac.mac
controllerDs1	Executable macro that configures C*x*1 ports; calls macro cntrDs1
ds1Encap	Executable macro that configures Frame Relay encapsulation on C*x*1 serial interfaces; calls macro cx1Encap
ds1FrCir	Executable macro that configures Frame Relay circuits on C*x*1 subinterfaces; calls macro cx1FRCir
configCx1	Executable macro that configures C*x*1 serial Frame Relay interfaces; calls macros cntrDs1, cx1Encap, and cx1FrCir
cntrDs1	Configures the C*x*1 controller; called by other macros
cx1Encap	Configures Frame Relay encapsulation on serial interfaces; called by other macros
cx1FrCir	Configures Frame Relay circuits on the subinterfaces; called by other macros

The following examples list the complete set of macros contained in ds1mac.mac. You can run the Help macro to list the other executable macros contained in ds1mac.mac. To configure Frame Relay on your router with ds1mac.mac, you can do one of the following:

- Run the controllerDS1, ds1Encap, and ds1FrCir macros in that order
- Run the configCx1 macro

In either case, to run the macros you must provide the required values described in the macros.

```
<# Help #>
! This file contains the following executable macros:
!  controllerDs1
!  ds1Encap
!  ds1FrCir
!  configCx1
<# endtmpl #>

<# controllerDs1 #>
<# if env.argc = 0 #>
! This macro configures your Cx1 controller.
! This macro will configure e1 ports as unframed.
! This macro should be called with 4 arguments.
! The argument list should be as follows:
```

```
! type; number of numPorts; slot; port; clock; framing; lineCoding
<# return #>
<# endif #>
<# type := env.argv(1) #>
<# ifCount := env.argv(2) #>
<# slot := env.argv(3) #>
<# port := env.argv(4)#>
<# clock := env.argv(5) #>
<# framing := env.argv(6) #>
<# coding := env.argv(7) #>

<# if clock = 'internal' #>
<# clock := 'internal mod' #>
<# endif #>

<# tmpl.cntrDs1(type, ifCount, slot, port, clock, framing, coding) #>
<# endtmpl #>

<# ds1Encap #>
<# if env.argc = 0 #>
! This macro configures Frame Relay encapsulation on Cx1 serial
! interfaces.
! This macro must be called with 4 arguments.
! If the protocol is Frame Relay (fr), then specify the type (DTE
! or DCE) and the lmi type.
! The argument list should be as follows:
! number of numPorts; slot; port; proto; frType; frLmi
<# return #>
<# endif #>
<# ifCount := env.argv(1) #>
<# slot := env.argv(2) #>
<# port := env.argv(3) #>
<# proto := env.argv(4) #>
<# if proto = 'fr' #>
<# proto := 'frame-relay ietf' #>
<# endif #>
<# tmpl.cx1Encap(ifCount, slot, port, proto) #>
<# endtmpl #>

<# ds1FrCir #>
<# if env.argc = 0 #>
! This macro configures Frame Relay circuits on Cx1
! subinterfaces.
! This macro must be called with 4 arguments.
! The argument list should be as follows:
! number of numPorts; slot; port; numCirs; dlci
<# return #>
<# endif #>
<# ifCount := env.argv(1) #>
<# slot := env.argv(2) #>
<# port := env.argv(3) #>
<# numCirs := env.argv(4) #>
<# dlci := env.argv(5) #>
<# tmpl.cx1FrCir(ifCount, slot, port, numCirs, dlci) #>
<# endtmpl #>

<# configCx1 #>
<# if env.argc = 0 #>
! This macro configures Cx1 serial Frame Relay interfaces.
! This macro must be called with 4 arguments.
! The argument list should be as follows:
! type; number of numPorts; slot; port; clock; framing; coding; proto; frType;
frLmi; numCirs; dlci
```

```
<# return #>
<# endif #>
<# type := env.argv(1) #>
<# ifCount := env.argv(2) #>
<# slot := env.argv(3) #>
<# port := env.argv(4) #>
<# clock := env.argv(5) #>
<# framing := env.argv(6) #>
<# coding := env.argv(7) #>
<# proto := env.argv(8) #>
<# tmpl.cntrDs1(type, ifCount, slot, port, clock, framing, coding) #>
<# if proto = 'fr' #>
<# frType := env.argv(9) #>
<# frLmi := env.argv(10) #>
<# numCirs := env.argv(11) #>
<# dlci := env.argv(12) #>
<# tmpl.cx1Encap(ifCount, slot, port, proto, frType, frLmi) #>
<# tmpl.cx1FrCir(ifCount, slot, port, numCirs, dlci) #>
<# else #>
<# tmpl.cx1Encap(ifCount, slot, port, proto, type, type) #>
<# endif #>
<# endtmpl #>

<# cntrDs1 #>
<# //This macro is called by other macros to configure DS1 ports #>
<# //Parameters in order are interface Type; numPorts; slot; port; clock;
framing; lineCoding #>
!
! Configure Cx1 Controller
!
<# type := param[1] #>
<# ifCount := env.atoi(param[2]) #>
<# slot := param[3] #>
<# port := env.atoi(param[4]) #>
<# clock := param[5] #>
<# framing := param[6] #>
<# coding := param[7] #>
<# while ifCount-- > 0 #>
controller <# type;' '; slot;'/';port;'\n' #>
<# if framing = 'unframed' #>
unframed
<# else #>
framing <# framing;'\n' #>
linecoding <# coding;'\n' #>
<# endif #>
clock source <# clock;'\n' #>
no shutdown

<# port++ #>
<# endwhile #>
<# endtmpl #>

<# cx1Encap #>
<# //This macro is called by other macros to configure Frame Relay encapsulation
on serial interfaces. #>
<# //Parameters in order are interface Type; numPorts; slot; port; clock;
framing; lineCoding #>
!
! Configure Encapsulation
!
<# ifCount := env.atoi(param[1]) #>
<# slot := param[2] #>
<# port := env.atoi(param[3]) #>
```

```
<# proto := param[4] #>
<# if proto = 'fr' #>
<# proto := 'frame-relay ietf' #>
<# endif #>
<# while ifCount-- > 0 #>
interface serial <# slot;'/';port;':1';'\n' #>
encapsulation <# proto;'\n' #>
<# if proto = 'frame-relay ietf' #>
frame-relay intf-type <# param[5];'\n'#>
frame-relay lmi-type <# param[6];'\n'#>
<# endif #>

<# port++ #>
<# endwhile #>
<# endtmpl #>

<# cx1FrCir #>
<# //This macro is called by other macros to configure Frame Relay circuits on
subinterfaces. #>
<# //Parameters in order are interface numPorts; slot; port; numCirs; dlci #>
!
! Configure Frame Relay Circuits
!
<# ifCount := env.atoi(param[1]) #>
<# slot := param[2] #>
<# port := env.atoi(param[3]) #>
<# numCirs := env.atoi(param[4]) #>
<# startDlci := env.atoi(param[5]) #>
<# id := env.atoi('1') #>
<# while ifCount-- > 0 #>
<# cirs := numCirs #>
<# id := env.atoi('1') #>
<# dlci := startDlci #>
<# while cirs-- > 0 #>
interface serial <# slot;'/';port;':1.';id;'\n' #>
frame-relay interface-dlci <# dlci #> ietf

<# id++; dlci++ #>
<# endwhile #>
<# port++ #>
<# endwhile #>
<# endtmpl #>
```

Configuring ATM Interfaces

This sample macro configures ATM interfaces based on the inputs you provide when prompted by the macro.

```
<# atmIf #>
<# slotPort:=env.getline("slot/port?") #>
<# while (vcType != 1 && vcType != 2);
vcTypeStr :=env.getline("VC type (1 = AAL5MUX IP, 2 = AAL5SNAP)?");
vcType := env.atoi(vcTypeStr);
endwhile #>
<# if vcType = 1; vcTypeStr := "aal5mux ip"; else; vcTypeStr := "aal5snap";
endif
#>
<# encapRouted:=1; encapBridged:=2; encapPPP:=3 #>
<# while (encapType < encapRouted || encapType > encapPPP );
encapTypeStr :=env.getline("encapsulation (1 = routed, 2 = bridged, 3 =
ppp)?");
encapType := env.atoi(encapTypeStr);
```

```
endwhile #>
<# if encapType = encapPPP #>
<# authNone:=1; authPap:=2; authChap:=3; authPapChap:=4; authChapPap:=5 #>
<# while (authType < authNone || authType > authChapPap );
authTypeStr :=env.getline("authentication (1 = None, 2 = PAP, 3 = CHAP, 4 =
PAP/CHAP; 5 = CHAP/PAP)?");
authType := env.atoi(authTypeStr);
endwhile #>
<# endif #>
<# vpStartStr := env.getline("Starting VP number?");
vpStart:=env.atoi(vpStartStr)#>
<# vpEndStr := env.getline("Ending VP number?"); vpEnd
:=env.atoi(vpEndStr)#>
<# vcStartStr := env.getline("Starting VC number?");
vcStart:=env.atoi(vcStartStr)#>
<# vcEndStr := env.getline("Ending VC number?"); vcEnd
:=env.atoi(vcEndStr)#>

<# loopbackStr := env.getline("Loopback interface number or <cr>?") #>
<# vp := vpStart; while vp <= vpEnd, ++vp #>
<# vc := vcStart; while vc <= vcEnd, ++vc #>
interface atm <#slotPort $ '.' $ ++i;'\n'#>
atm pvc <# i; ' '; vp; ' '; vc; ' '; vcTypeStr;'\n'#>
<# if encapType = encapPpp #>
encap ppp
<# if authType = authPap#>
ppp authentication pap
<# elseif authType = authPapChap#>
ppp authentication pap chap
<# elseif authType = authChapPap#>
ppp authentication chap pap
<# elseif authType = authChap#>
ppp authentication chap
<# endif #>
<# elseif encapType = encapBridged #>
encap bridged1483
<# endif #>
<# if loopbackStr != "" #>
ip unnumbered loopback <# loopbackStr;"\n" #>
<# endif #>
!
<# endwhile #>
!
<# endwhile #>

<# if encapType = encapPPP #>
<# authNone:=1; authPap:=2; authChap:=3; authPapChap:=4; authChapPap:=5 #>
<# while (authType < authNone || authType > authChapPap );
authTypeStr :=env.getline("authentication (1 = None, 2 = PAP, 3 = CHAP, 4 =
PAP/CHAP; 5 = CHAP/PAP)?");
authType := env.atoi(authTypeStr);
endwhile #>
<# endif #>
<# vpStartStr := env.getline("Starting VP number?");
vpStart:=env.atoi(vpStartStr)#>
<# vpEndStr := env.getline("Ending VP number?"); vpEnd
:=env.atoi(vpEndStr)#>
<# vcStartStr := env.getline("Starting VC number?");
vcStart:=env.atoi(vcStartStr)#>
<# vcEndStr := env.getline("Ending VC number?"); vcEnd
:=env.atoi(vcEndStr)#>
<# loopbackStr := env.getline("Loopback interface number or <cr>?") #>
<# vp := vpStart; while vp <= vpEnd, ++vp #>
```

```
<# vc := vcStart; while vc <= vcEnd, ++vc #>
interface atm <#slotPort $ '.' $ ++i;'\n'#>
atm pvc <# i; ' '; vp; ' '; vc; ' '; vcTypeStr;'\n'#>
<# if encapType = encapPpp #>
encap ppp
<# if authType = authPap#>
ppp authentication pap
<# elseif authType = authPapChap#>
ppp authentication pap chap
<# elseif authType = authChapPap#>
ppp authentication chap pap
<# elseif authType = authChap#>
ppp authentication chap
<# endif #>
<# elseif encapType = encapBridged #>
encap bridged1483
<# endif #>
<# if loopbackStr != “” #>
ip unnumbered loopback <# loopbackStr;”\n” #>
<# endif #>
!
<# endwhile #>
!
<# endwhile #>
<# endtmpl #>
```

Chapter 11

Booting the System

This chapter provides information about booting your E-series router.

NOTE: The type of file you must always use for booting your system is a software release file with the extension .rel.

This chapter contains the following sections:

- Platform Considerations on page 523
- Configuring Your System for Booting on page 523
- Rebooting Your System on page 528
- Operations in Boot Mode on page 531
- Displaying Boot Information on page 531

Platform Considerations

System booting is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

Configuring Your System for Booting

Juniper Networks delivers your E-series router already set up with a factory default configuration and a software release (.rel) file. You can, however, create a new configuration file (.cnf) and select a different software release file to use in future reboots of your router. When you reboot your router, you can use:

- An existing configuration file to be used each time the system reboots
- An existing configuration file limited to a single reboot

- An existing script file to be used on only the next reboot
- An existing script file to be used on the next and every subsequent reboot using backup mode
- The configuration that is already running on the system
- The factory default configuration

In addition, you can configure the system to load a different software release file on its next reboot. Use the **boot system** command to do this. If you do not configure your system with a backup release, it reverts to the release and configuration it had before the crash.

You can use the **boot backup** command to specify a software release and configuration for the system to use in case the system resets too many times in a given period.

The **boot subsystem** command enables you to override the system release setting for a given subsystem—for example, OC3.

Booting the GE-2 Line Module

The GE-2 line module can now detect whether it supports the software release installed on the primary SRP module in an E-series router. When the GE-2 line module is booting and it detects that it supports the software release on the SRP module, the line module boots successfully with that software release. However, if the GE-2 line module detects that it does not support the software release on the SRP module, the module does not boot successfully and the following messages appear in the system log:

```
ERROR 05/04/2005 06:09:05 system (slot 13): Line card failed diags in slot 13
with status: Autoboot disabled
ERROR 05/04/2005 06:09:05 system (slot 13): board failed diagnostics
```

boot backup

- Use to set the release version and the configuration to be used when the boot logic chooses backup mode.
- This command does not reboot the system; it configures the system for rebooting.
- You can require the system to reboot from an existing configuration file, from an existing local script file, or with the factory default configuration.
- Example

  host1(config)#**boot backup rel_1_1_0.rel newfile.cnf**

- Use the **no** version of this command to remove the backup setting.

boot config

- Use to specify the configuration with which the system is rebooted.

CAUTION: All versions of this command except those using the **running-configuration** or **startup-configuration** keywords erase the current system running configuration. Before issuing one of those versions, you might want to save the running configuration to a .cnf file by issuing the **copy running-configuration** command.

- You can require the system to reboot from a configuration file.

  To specify an existing system configuration (.cnf) file that the system uses for the next reboot and all subsequent reboots:

  host1(config)#**boot config newconffile.cnf**

  To specify an existing system configuration (.cnf) file that the system uses only on the next reboot. On subsequent reboots, the system will use the running configuration current at the time of that reboot:

  host1(config)#**boot config newconffile.cnf once**

- You can require the system to reboot from an existing local script (.scr) file that the system uses only on the next reboot. On subsequent reboots, the system will use the running configuration current at the time of that reboot:

  host1(config)#**boot config scriptfile.scr**

  Configuring this option causes the system to ignore—only at the next reboot—an autocfg.scr file that you may also have configured.

- If you specify a .cnf file, upon the next reboot the system resets to the factory defaults; it then opens the .cnf file and begins applying it immediately. If you specify a .scr file, upon the next reboot the system resets to the factory defaults; it then waits for a 600-second countdown timer to expire before applying the script. This period gives the line modules an opportunity to fully initialize before configuration begins. Upon timer expiration or system initialization (whichever occurs first), the script executes regardless of the state of the line modules. You can escape from the countdown by pressing Ctrl + c; the system prompts you to execute the script immediately or return to the system console.
- You can require the system to reboot from the configuration running on the system at the time of the reboot.

  If the system is in Automatic Commit mode:

  host1(config)#**boot config running-configuration**

  If the system is in Manual Commit mode:

  host1(config)#**boot config startup-configuration**

  See *Saving the Current Configuration* in *Chapter 5, Managing the System*, for information about Automatic and Manual Commit modes.

- You can require the system to reboot from the factory default configuration. On subsequent reboots, the system will use the running configuration current at the time of that reboot:

  host1(config)#**boot config factory-defaults**

- This command does not reboot the system.
- Use the **no** version to clear a previous request to reboot in a specified manner.

boot force-backup

- Use to force the system to use the backup release/configuration on the next boot.
- This command does not reboot the system.
- Example

  host1(config)#**boot force-backup mysafe.rel mysafe.cnf**

NOTE: Even if you request the normal release/configuration, the boot logic still checks the reboot history file. It may force the backup mode regardless of your request. To guarantee that the boot logic does not override your request to use the normal release/configuration, do either of the following:

- Delete the reboot history file after issuing the **no boot force-backup** command.
- Do not configure a backup release or configuration file.

- Use the **no** version to set the system to return to its normal release/configuration on the next boot.

boot revert-tolerance

- Use to set the reversion tolerances that the boot logic uses to determine whether to use normal or backup settings.
- The default settings tolerate up to three resets in 30 minutes.
- This command does not reboot the system when high availability is not enabled.
- Issuing this command when high availability is enabled results in the system cold-restarting the router and using the backup settings if the tolerance settings are met.
- Example

  host1(config)#**boot revert-tolerance 2 60**

- Use the **no** version to restore the default values, 3 and 1800.

boot revert-tolerance never

- Use to set the boot logic to never revert to the backup image/configuration.
- This command does not reboot the system.
- Example

  host1(config)#**boot revert-tolerance never**

NOTE: This command is functionally equivalent to specifying no backup image/configuration, but it allows you to leave the backup settings alone and to toggle autoreversion on and off. This command is undone by using the **no boot revert-tolerance** command, which restores the default settings, or the **boot revert-tolerance** command. The default settings are count = 3 (crashes) and time = 1800 (seconds); that is, 3 crashes in 30 minutes.

- There is no **no** version.

boot subsystem

- Use to configure the software release the selected subsystem will use the next time it reboots.
- This command does not reboot the subsystem.
- Example 1

  host1(config)#**boot subsystem ct3 rel_1_0_1.rel**

- The **boot backup subsystem** version of this command enables you to configure a backup subsystem for booting.
- Example 2

  host1(config)#**boot backup subsystem ct3 rel_1_0_1.rel**

- Use the **no** version to remove the configuration setting.

boot system

CAUTION: This command attempts to reprogram the SRP boot PROMs, if necessary. The SRP has a primary and, typically, a backup boot PROM. If the **boot system** command is executed on an SRP with no backup boot PROM, the following message is displayed: "Write to Backup Boot ROM failed." In this instance, this message is correct, and you can ignore it.

- Use to specify the software release (.rel) file that your system will use when rebooting.
- This command does not reboot the system.
- In a dual SRP configuration, when this information is synchronized to the standby SRP, the standby SRP is reloaded to boot the specified release. The high availability feature requires the release to be the same on the active and the standby SRP. This means that arming the system to boot with a different release causes the standby to reload and prevent high availability from becoming active or disable high availability it if it is active or pending.

- Example

  host1(config)#**boot system release1.rel**

- There is no **no** version.

Rebooting Your System

You can reboot your system as a whole or select a single slot in the system to be rebooted. You can reboot your system immediately or in a designated interval of time, and can configure the system to prompt you if the modules are in a state that could lead to a loss of configuration data or an NVS corruption.

If you reboot the system before it has completely written configuration updates to NVS, the system will start with the last saved configuration. If you reboot the system after it has written the configuration updates to NVS, but before it has applied those updates to actual configuration data, the configuration update process resumes immediately following the reboot and completes before any application accesses its configuration data.

reload

- Use to reload the software on the system immediately.
- Reloads the system software (.rel) file and the configuration (.cnf) file on the system.
- When you issue this command, the system prompts you for a confirmation before the procedure starts.
- If you specify the **force** keyword, the procedure will fail if the system is updating the boot prom. In this case, the system will display a message that indicates that the procedure cannot currently be performed and the cause. However, if the system is in a state that could lead to a loss of configuration data or an NVS corruption, such as during the synchronization of SRP modules, the system displays a message that describes the state, and asks you to confirm (enter y for yes, n for no) whether you want to proceed.
- If you do not specify the **force** keyword, the procedure will fail if the system is in a state that could lead to a loss of configuration data or an NVS corruption, and the system will display a message that explains why the procedure failed.
- Use the **standby-srp** keyword to reload the system software (.rel) file and the configuration (.cnf) file on the standby SRP module without having to look up its slot number to use with the **reload slot** command.
- When you issue this command, the system prompts you for a confirmation before the procedure starts.
- If you remove a standby SRP module without issuing the **slot erase** command to delete the configuration, the E-series router cannot guarantee that the SRP modules were synchronized. In this situation, you must do either of the following to reload the router:
  - Issue the **reload** command with the **force** keyword.
  - Issue the **slot erase** command followed by the **reload** command.

- Example

  host1#**reload**
  host1#**reload force**

- There is no **no** version.

reload at

- Use to reload the software on the system at an absolute time.
- This command halts the system.
- Reloads the system software (.rel) file and the configuration (.cnf) file on the system.If the system is in a state that could lead to a loss of configuration data or an NVS corruption, it will delay the procedure for one minute. Each time the system delays the procedure, it adds a message to the os log that explains why the procedure was delayed. If the system cannot reload on its sixth attempt, the reboot procedure will fail, and the system will add an explanation to the os log.
- Example

  host1#**reload at 10:10 May 5**

  This command reloads the software 10 minutes after 10 on May 5th.

- There is no **no** version.

reload in

- Use to reload the software on the system in a relative period of time.
- This command halts the system.
- Reloads the system software (.rel) file and the configuration (.cnf) file on the system.
- If the system is in a state that could lead to a loss of configuration data or an NVS corruption, it will delay the procedure for one minute. Each time the system delays the procedure, it adds a message to the os log that explains why the procedure was delayed. If the system cannot reload on its sixth attempt, the reboot procedure will fail, and the system will add an explanation to the os log.
- Example

  host1#**reload in 00:10**

  This command reloads the software in 10 minutes.

- There is no **no** version.

reload slot

- Use to reboot a selected slot on the router.
- Reloads the system software (.rel) file and the configuration (.cnf) file on the module in the selected slot.
- When you issue this command, the system prompts you for a confirmation before the procedure starts.

- If you specify the **force** keyword and the slot number of the primary SRP module, the procedure will fail if the system is updating the boot prom. In this case, the system will display a message that indicates that the procedure cannot currently be performed and the cause. However, if the system is in a state that could lead to a loss of configuration data or an NVS corruption, such as using the synchronization of SRP modules, it displays a message that describes the state, and asks you to confirm (enter yes or no) whether you want to proceed.
- If you do not specify the **force** keyword, the procedure will fail if the system is in a state that could lead to a loss of configuration data or an NVS corruption, and the system will display a message that explains why the procedure failed.
- Example

  host1#**reload slot 3**

- There is no **no** version.

Rebooting When a Command Takes a Prolonged Time to Execute

Although some commands might take a relatively long time to execute, most do not. If the CLI displays no output other than "Please wait..." for a prolonged period, you can press Ctrl + x to reset the system. Use Ctrl + x only as a last resort; if at all possible, wait until the command is completed, or attempt to connect to the system through a Telnet or SSH client through which you can use the **reload** command.

service ctrl-x-reboot

- Use to enable the Ctrl + x key combination to reset the system from any location.
- Issuing the Ctrl + x command has no effect if you are accessing the system through Telnet.
- This feature is disabled by default.
- Loading the factory default configuration does not override this feature.
- Example

  host1(config)#**service ctrl-x-reboot**

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

Configuration Caching

Configuration caching prevents the system from being partially configured with changes in the event of a reset. When a script or macro begins execution, the resulting configuration changes are automatically cached in system RAM rather than being committed to nonvolatile storage (NVS). When the script or macro completes execution, the cache is flushed as a background operation, saving the configuration changes to NVS.

If the SRP module resets during the script or macro execution, the system boots as though the script were never started because no NVS files have changed. If the SRP module resets during the flush operation, the system boots with factory defaults.

If you start another script or macro in the middle of an ongoing flush operation, the current flush is halted; now if the SRP module resets during the script, the system boots with factory defaults.

If you issue the **reload** command to manually reset the system, the system checks for an ongoing cache flush and warns you if a flush operation is discovered.

Operations in Boot Mode

To access Boot mode:

1. Reload the system from Privileged Exec mode:

   ```
   host1#reload
   WARNING: Execution of this command will cause the system to reboot.
   Proceed with reload? [confirm]
   Reload operation commencing, please wait...
   7
   ```

2. Press the < mb > key sequence (case-insensitive) during the countdown that is displayed immediately after the BPOST tests are bypassed. This puts the CLI in Boot mode.

   ```
   :boot##
   ```

   If you do not press the < mb > key sequence before the countdown timer expires, the reloading process continues and returns the CLI to the normal User Exec mode.

Displaying Boot Information

You can display information about the system's booting configuration, installed hardware versions, and installed software versions.

show boot

- Use to show the current boot settings.
- Example

  ```
  host1#show boot
  System Release:         release.rel
  System Configuration:   running-configuration
  ```

  Note: This system is not configured with backup settings.

show hardware

- Use to display detailed information about the system hardware.
- Field descriptions
  - slot—Physical slot that contains the module
  - type—Type of module
  - serial number—Serial number of the module

- assembly number—Part number of the module
- assembly rev—Hardware revision of the module
- ram (MB)—Memory capacity of the host processor
- number of MAC addresses—Total number of Ethernet addresses on an I/O module
- base MAC address—Lowest Ethernet address on an I/O module

- Example

```
host1#show hardware
                              serial      assembly    assembly   ram
slot        type              number       number      rev.     (MB)
----   ----------------   ----------   ----------   --------   ----
0      SRP-10Ge           4305358981   3500005472     A06      2048
1      SRP-10Ge           4305359020   3500005472     A06      2048
2           ---             ---          ---          ---      ---
3           ---             ---          ---          ---      ---
4      CT3-12             4305337201   3500010901     A07      128
5      OC3/OC12/DS3-ATM   4605300290   3500103958     A06      256
6      GE/FE              4605340294   3500104554     A08      256

                                                                number
                                                                  of
                            serial      assembly    assembly      MAC
slot       type             number       number       rev.     addresses
----   -------------   ----------   ----------   --------   ---------
0           ---            ---          ---          ---        ---
1      SRP-10Ge I/O    4605250426   3500003302     A02          1
2           ---            ---          ---          ---        ---
3           ---            ---          ---          ---        ---
4      CT3/T3-12 I/O   4305316605   3500010801     A02
5      OC3(8)-MM I/O   4304443600   4500001501     A03          4
6      GE-SFP I/O      4605310064   4500002001     A05          1
            base
slot    MAC address
----   --------------
0           ---
1      0090.1aa0.577a
2           ---
3           ---
4
5      0090.1a41.7c68
6      0090.1aa0.6216
```

show last-reset

- Use to display the reason for the system's last user-directed reload or error-caused reset.
- Example

```
host1#show last-reset
last reset: power cycle
```

show reload

- Use to display the system's reload status.
- Example

```
host1#show reload
reload scheduled for TUE OCT 2 2001 10:10:00 UTC
```

show version

- Use to display the configuration of the system hardware and the software version.
- Example

```
host1#show version
Juniper Edge Routing Switch ERX-700
Copyright (c) 1999-2005 Juniper Networks, Inc.  All rights reserved.
System Release: erx_7-1-0.rel Partial
        Version: 7.1.0 [BuildId 4518]   (December 21, 2005  11:23)
System running for: 25 days, 3 hours, 31 minutes, 5 seconds
        (since THU DEC 22 2005 11:36:41 UTC)

slot  state     type     admin  spare  running release    slot uptime
---- ------- ---------- ------- ----- ------------------ --------------
0    standby SRP-10Ge   enabled  ---  erx_7-1-0.rel           ---
1    online  SRP-10Ge   enabled  ---  erx_7-1-0.rel      25d03h:28m:49s
2      ---      ---       ---    ---         ---              ---
3      ---      ---       ---    ---         ---              ---
4    online  CT3-12     enabled  ---  erx_7-1-0.rel      25d03h:24m:46s
5    online  OC3-4A-APS enabled  ---  erx_7-1-0.rel      25d03h:24m:22s
6    online  GE         enabled  ---  erx_7-1-0.rel      25d03h:24m:44s
```

Output Filtering

The output filtering feature of the **show** command is not available in Boot mode.

Chapter 12

Configuring the System Clock

Use the procedures described in this chapter to configure the E-series router clock.

This chapter contains the following sections:

- Overview on page 535
- Platform Considerations on page 538
- References on page 539
- Setting the System Clock Manually on page 539
- Before You Configure NTP on page 541
- NTP Configuration Tasks on page 541
- Monitoring NTP on page 547

Overview

You can use the **clock** commands to set the time and date on your system manually. These commands allow you to specify settings such as the source of the time, the time zone, and dates for seasonal time changes.

You can configure your router to update its clock automatically by configuring it as a Network Time Protocol (NTP) client. NTP provides a method of synchronizing the system clocks of hosts on the Internet to Universal Coordinated Time (UTC). Using NTP allows the system to record accurate times of events. You can view the log file of events to monitor the status of the network.

Since there is only one system clock, you can configure an NTP client on one virtual router only. Other virtual routers obtain clock parameters from the system clock. However, multiple virtual routers can act as NTP servers.

NTP

NTP uses a hierarchical structure of hosts, such as computers and routers, that form client-server and peer *associations*. An NTP client synchronizes with an NTP server, which in turn synchronizes with another time source. If two hosts provide synchronization for each other, they are peers.

Primary or *stratum 1* servers synchronize directly with an accurate time source, such as a radio clock or an atomic clock. *Secondary* or *stratum n* servers synchronize with other servers, and are *n* hops from an accurate time source.

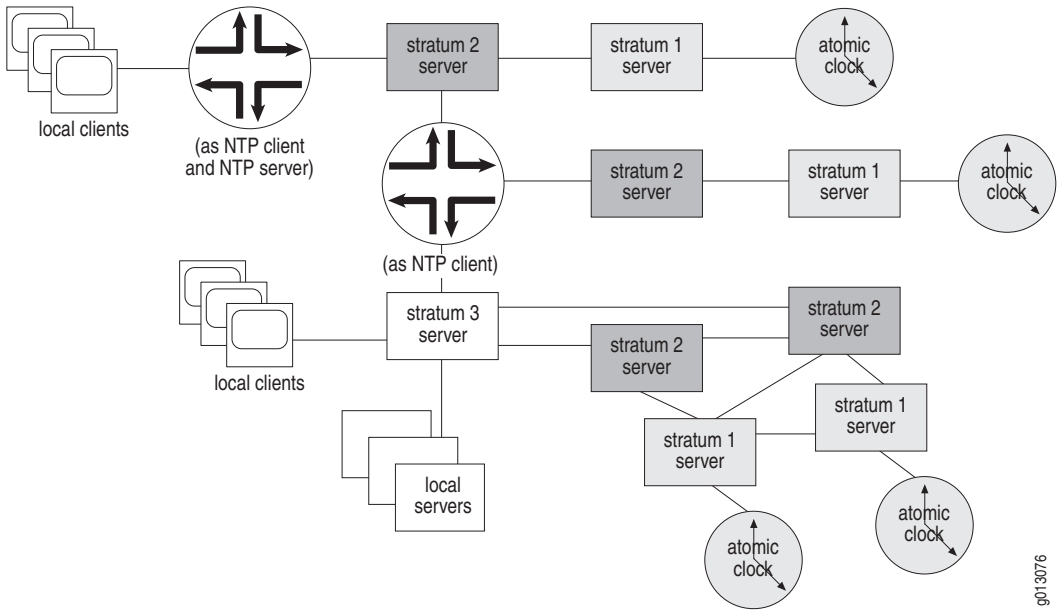
To obtain high precision and reliability with NTP, clients typically synchronize with several NTP servers at different physical locations. Peer associations, especially for stratum 1 and 2 servers, provide redundancy for the network.

Hosts synchronize by exchanging NTP messages through UDP. NTP uses the IP and UDP checksums to confirm data integrity.

By default, the router is an NTP client. You must configure NTP client parameters to start NTP client operation. You can also configure the router as an NTP server, whether or not you configure NTP client parameters.

Figure 30 shows an example of an NTP hierarchy.

Figure 30: Example of an NTP Hierarchy



System Operation as an NTP Client

To synchronize to the clock of a server, the system must receive time information from NTP servers recurrently. The way the system receives such information depends on how you configure it:

- If you configure the system to poll NTP servers, it sends time requests to the servers periodically. NTP servers receive the requests, add time information to the messages, and send replies to the system.
- If you configure the system as a broadcast client, it receives NTP broadcasts from servers periodically. The broadcasts include time information from the servers.

By default, NTP servers respond to the interface from which an NTP request originated. You can direct responses from all NTP servers to one interface on the system, or from a specific NTP server to a specific interface.

NOTE: When the system is not configured as either an NTP client or an NTP server, it responds to NTP requests with an invalid stratum number.

Synchronization

There are three stages to synchronization:

- Preliminary synchronization
- Frequency calibration
- Progressive synchronization

Preliminary Synchronization

Preliminary synchronization is a stage during which the system evaluates the initial time situation and decides how to proceed with longer-term synchronization. This stage involves the following steps:

1. The system obtains several readings of time data from NTP servers.
2. The system analyzes time data in the messages and compares the readings from different servers. Using this information, the system identifies the initial best time source (the *best server*).
3. The system calculates the difference between its own clock and the best server's clock (the *offset*) and proceeds as follows:
   - If the offset is greater than 15 minutes, the system disables NTP and displays a message advising you to check the time zone and clock settings.
   - If the offset is less than 15 minutes, the system sets its clock to that of the best server.
4. Provided the system has not disabled NTP, it proceeds to the next stage:
   - If a frequency calibration is available, the system starts progressive synchronization.
   - If the system has never performed a frequency calibration or the calibration has been deleted, the system starts a frequency calibration.

Frequency Calibration

Frequency calibration takes place the first time you use NTP or when you reboot the system. During this stage, the system evaluates the frequency error of its clock by measuring change in the offset error. A frequency calibration takes 15 minutes.

Progressive Synchronization

After the system has established initial NTP parameters, it continues to synchronize to a server as follows:

1. The system acquires time information from servers periodically.
2. The system evaluates which server is currently the best time source (the *master*) by analyzing time data in the messages and comparing the data from different servers.
3. The system gradually synchronizes its clock to that of the master.

System Operation as an NTP Server

The NTP server supports both unicast (user-to-user addressing protocol) and broadcast modes. Depending on the server configuration you choose, the system functions in different ways:

- When the system is configured as a unicast NTP server, it synchronizes clients to its own clock by responding to NTP requests from clients as follows:
  1. Swaps the destination and source addresses in the request packet.
  2. Sets all timestamps and NTP attributes in the packet.
  3. Returns the packet to the client.
- When the system is configured as a broadcast NTP server, it periodically sends NTP time synchronization messages to the local network broadcast address (255.255.255.255). The broadcast server would also respond to any NTP unicast requests from clients.

If the system is configured both as an NTP client and an NTP server, the system effectively synchronizes its clients to its master's clock. If the system is configured as an NTP server but not an NTP client, the system synchronizes its clients to its own clock, which can be set by the **clock** commands.

NOTE: When the system is not configured as either an NTP client or an NTP server, it responds to NTP requests with an invalid stratum number.

Platform Considerations

The system clock is supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

This implementation of NTP meets the following specifications:

- RFC 1305—Network Time Protocol (version 3) Specification, Implementation and Analysis (March 1992)
- RFC 2030—Simple Network Time Protocol (SNTP) (Version 4) for IPv4, IPv6, and OSI (October 1996)

Setting the System Clock Manually

Before you set the system clock, obtain the following information about your time zone:

- The name of the time zone
- The difference (offset) between the time zone and UTC
- The dates and times of transitions to and from summer time (daylight saving time)
- The difference between the standard time and summer time (daylight saving time)

The international Web site *www.timeanddate.com* contains information about time zones.

NOTE: Be sure to set the time zone (default is UTC) and summer time dates before you set the clock.

You can set the system clock at any time. This process involves the following steps:

1. Set the time zone.
2. Set the summer time dates.
3. Set the time.
4. Check the clock settings.

clock set

- Use to set the time and date on your system manually.
- Use the following syntax for setting the time: HH:MM:SS. This is the current time in 24-hour format—hours:minutes:seconds.
- There are two acceptable date forms for this command. Both produce the same display when you run the **show clock** command.
  - Day:month:year
  - Month:day:year

- Examples

  host1#**clock set 08:12:42 12 March 2000**
  host1#**clock set 11:12:55 March 10 2000**

- There is no **no** version.

clock summer-time date

- Use to set the clock to switch automatically to summer time (daylight saving time).
- Example

  host1(config)#**clock summer-time PDT date 1 April 200X 2:00 31 October 200X 2:00 60**

- Use the **no** version to prevent automatic switching to summer time.

clock summer-time recurring

- Use to set the clock to summer time at the same time each year.
- Example—This overrides the default settings for PDT,

  host1(config)#**clock summer-time PDT recurring first Sunday April 2:00 last Sunday October 2:00**

- Use the **no** version to prevent automatic switching to summer time.

clock timezone

- Use to set the time zone for display.
- Example—This sets the time zone to 5 hours behind UTC.

  host1(config)#**clock timezone EST -5**

- Use the **no** version to set the time zone to UTC, the default setting.

show clock

- Use to display the system time and the date.
- Example 1—Shows time source value when clock is manually configured

```
host1#show clock detail
TUE JAN 23 2007 11:50:47 UTC
time source: manually entered by user
timezone: UTC (0 minutes from UTC)
```

- Example 2—Shows time source value when clock is synchronized with NTP

```
host1#show clock detail
TUE JAN 23 2007 11:50:47 UTC
time source: Configured via NTP
timezone: UTC (0 minutes from UTC)
```

Before You Configure NTP

Before you configure NTP, complete the following procedures:

1. Configure at least one IP address on the router.
2. Check that the system clock reads the correct time to within 15 minutes, and that the time zone and summer time settings are correct.
3. Reset the system clock manually if the time, time zone, or summer time settings are incorrect.
4. If you want to configure the NTP system as an NTP client, choose the NTP servers.

Choosing NTP Servers

For the system, synchronizing to several stratum 2 or higher servers on the Internet provides sufficient accuracy for the timing of event messages. You can find a list of stratum 2 servers at *www.eecis.udel.edu/~mills/ntp.*

If you have access to an NTP server that you know to be reliable and accurate, you can synchronize the system to that server alone. You may prefer this method if you have used Simple Network Time Protocol (SNTP) with other equipment.

If you know that an NTP server broadcasts on a network to which the system has an interface, you do not need to configure NTP servers. Simply enable the system to accept NTP broadcasts on that interface.

NTP Configuration Tasks

By default, the system is an NTP client. You must configure NTP client parameters to start NTP client operation. You can also configure the system as an NTP server, whether or not you configure NTP client parameters.

Enabling NTP Services

Before you can configure NTP client parameters or enable a virtual router to act as an NTP server, you must enable NTP services. When you enable NTP services, the NTP client associates itself with the current virtual router. Because there is only one system clock to update, only the virtual router on which you configure NTP can act as the NTP client. However, any virtual router can act as an NTP server. To enable NTP services:

1. (Optional) Access the virtual router with which you want to associate NTP services.
2. Issue the **ntp enable** command.

ntp enable

- Use to enable NTP services on the system.
- This command associates NTP services and the NTP client with the current virtual router.
- Example

  host1:boston(config)#**ntp enable**

- Use the **no** version to disable NTP polling and clock correction and to remove the association between NTP services and the virtual router.

NTP Client Configuration

To configure the system as an NTP client:

1. Ping the selected NTP servers to ensure that the system can reach them.
2. Configure the system to acquire NTP data by completing one or both of the following actions:
   - Assign the NTP servers.
   - Enable the system to receive broadcasts on an interface.
3. If you enable the system to receive broadcasts on an interface, set the estimated round-trip delay between the system and an NTP broadcast server.
4. Disable NTP on interfaces that you do not want to receive NTP communications for security or other reasons.

ntp broadcast-client

- Use to enable the system to receive NTP broadcasts on an interface.
- Example

  host1(config-if)#**ntp broadcast-client**

- Use the **no** version to prevent the system from receiving NTP broadcasts.

ntp broadcast-delay

- Use to set the estimated round-trip delay in the range 0 to 999,999 microseconds between the system and an NTP broadcast server.
- Example

  host1(config)#**ntp broadcast-delay 2000**

- Use the **no** version to set the estimated round-trip delay to the default, 3000 microseconds.

ntp disable

- Use to disable NTP on an interface.
- Example

  host1(config-if)#**ntp disable**

- Use the **no** version to reenable NTP on an interface.

ntp server

- Use to assign an NTP server to the system and to customize the way the server communicates with the system.
- Specify the **source** option to direct responses from the NTP server to a specific interface on the system and override the **ntp source** command.
- Example

  host1(config)#**ntp server 192.35.42.1 version 3 prefer source atm 3/0.1**

- Use the **no** version to terminate communications between the system and an NTP server.

ping

- Use to check that the system can reach an NTP server.
- Example

  host1(config)#**ping 192.35.42.1**

- There is no **no** version.

Directing Responses from NTP Servers

By default, an NTP server sends a response to the interface from which an NTP request originated. You can now direct responses from all NTP servers to one interface on the system or direct responses from a specific NTP server to a specific interface.

ntp source

- Use to direct responses from all NTP servers to a specific interface. Using the **source** option with the **ntp server** command overrides the **ntp source** command.
- Example

  host1(config)#**ntp source atm 3/1**

- Use the **no** version to direct all servers to reply to the interface from which the NTP request was sent (the default setting).

Refusing Broadcasts from NTP Servers

You can prevent the system from receiving certain types of broadcasts and specify the servers from which the system will accept NTP broadcasts. To do so:

1. Issue the **ntp access-group** command.
2. Configure an access list.

access-list

- Use to configure an access list.
- Example

  host1(config)#**access-list europe permit any**

- Use the **no** version to remove the access list.

ntp access-group

NOTE: The system can accept, but does not use, NTP control queries.

- Use to specify the types of broadcasts that the system will accept and respond to, and to specify an access list of servers from which the system will accept broadcasts.You can enable the system to:
  - Receive time requests, receive NTP control queries, and synchronize itself to the servers specified on the access-list
  - Only receive time requests and NTP control queries from specified servers
  - Only receive time requests from specified servers
  - Only receive NTP control queries from specified servers
- Example

  host1(config-line)#**ntp access-group peer europe**

- Use the **no** version to enable the system to receive all NTP broadcasts on interfaces configured to receive broadcasts.

NTP Server Configuration

To enable a virtual router to act as an NTP server:

1. Access the virtual router context.
2. Specify that the virtual router acts as an NTP server.

CAUTION: Be sure that you do not override a valid time source if you specify the stratum of the NTP server. Issuing the **ntp master** command on multiple systems in the network might lead to unreliable timestamps if those systems do not agree on the time.

3. (Optional) Specify the stratum of this NTP server.

ntp broadcast

- Use to enable broadcast server on an interface to send NTP broadcast messages periodically.
- The server sends the NTP broadcast messages to the local network broadcast address (255.255.255.255).
- Example—In this example, the interface supports NTP software, version 4, and a poll interval of 5 (32 seconds) for broadcasting NTP messages.

  host1:boston(config-if)#**ntp broadcast version 4 5**

- Use the **no** version to prevent the interface from sending NTP broadcast messages.

ntp master

- Use to specify the stratum number of a virtual router you configured as an NTP server
- By default, the stratum number is set to the stratum number of the master plus one.

CAUTION: Although you can specify a stratum number of 1, the system does not support stratum 1 service. The system can synchronize only with an NTP server, and not directly with an atomic clock or radio clock.

- Specify a stratum number for the system in the range 1 – 15. A stratum *n* server is *n* hops from an accurate time source.
- Example

  host1:boston(config)#**ntp master**

- Use the **no** version to restore the default stratum number.

ntp server enable

- Use to enable a virtual router to act as an NTP server.
- Example

  host1:boston(config)#**ntp server enable**

- Use the **no** version to prevent a virtual router from acting as an NTP server.

Configuration Examples

The following examples show how to configure the system as an NTP client and an NTP server.

Example 1 NTP communications are established on the virtual router boston. The system is a client of the NTP server with IP address 172.16.5.1.

```
host1#virtual-router boston
host1:boston#ping 172.16.5.1
Sending 5 ICMP echos to 172.16.5.1, timeout = 2 sec.
.....
Success rate = 100% (0/5), round-trip min/avg/max = 0/0/0 ms
host1:boston#configure terminal
host1:boston(config)#ntp server 172.16.5.1
host1:boston(config)#ntp enable
```

Example 2 NTP communications are established on the virtual router boston. The system is specified as an NTP server.

```
host1#virtual-router boston
host1:boston#configure terminal
host1:boston(config)#ntp server
```

Example 3 NTP communications are established on the virtual router boston. The router is specified as an NTP broadcast server and synchronizes with NTP server 172.16.5.1. The specified interface enabled for NTP broadcasting is configured with version 4 and poll interval 5 for broadcasting NTP messages.

```
host1#virtual-router boston
host1:boston#configure terminal
host1:boston#ntp enable
host1:boston(config)#ntp server 172.16.5.1
host1:boston(config)#interface fastethernet 9/3
host1:boston(config-if)#ntp broadcast 4 5
```

NOTE: In Example 3, the router that acts as the NTP broadcast server must either synchronize to another server or master (specified by the **ntp server** command) or act as master (**ntp master** command).

Monitoring NTP

After you configure the system as an NTP client, you can use **show** commands to view information about the NTP servers you assigned and the status of NTP on the interface.

NOTE: For about 30 minutes after you configure the system as an NTP client, the data varies rapidly, and then starts to stabilize. Wait at least 1 hour before using the data to make decisions about NTP servers.

Many of the fields in the displays of these **show** commands take their values from the NTP messages. The NTP client uses this data to compare the performance of its NTP servers and to choose a master.

show ntp associations

- Use to view the information about the NTP servers you assigned.
- Field descriptions
  - * (Master)—System is synchronizing to this server
  - # (Master - unsynchronized)—System has chosen this server as master, but the master has not yet synchronized to UTC
  - + (Selected)—System will consider this server when it chooses the master
  - - (Candidate)—System may consider this server when it chooses the master
  - x (Unusable)—Server does not meet the initial criteria for master
  - p (Preferred)—Server that you specified as the preferred server
  - ~ (Configured)—Server is a configured server; no tilde indicates a broadcast server
  - Peer Address—IP address of server
  - Stratum—Number of hops between the server and the accurate time source
  - Poll—Time between NTP requests from system to server
  - Reachable—8-bit number that shows whether or not the NTP server responded to the last eight requests from the system; one indicates a response, zero indicates no response. For example, 11111111 indicates that the NTP server responded to the last eight requests. If the system reaches one server less often than it does other servers, that server is not a good choice for the master.
  - Precision—Length of the clock tick (interrupt interval) of server's clock
  - Delay—Round-trip delay, with the lowest dispersion value in the sample buffer, between the system and the server

- Offset—Difference, with the lowest dispersion in the sample buffer, between the system's clock and the server's clock
- Disp.—Lowest measure, in the sample buffer, of the error associated with the peer offset, based on the peer delay

- Example

```
host1#show ntp associations

Peer Address      Stratum   Poll  Reachable  Precision  Delay   Offset  Disp.
- 10.6.129.58        3      512s  01111111   0.000000s  0.000s  0.052s  0.010s
+~152.2.21.1         2      256s  11111111   0.000015s  0.070s  0.039s  0.020s
+~128.182.58.100     2      256s  11011111   0.000004s  0.030s  0.019s  0.074s
*p128.118.25.3       2      256s  10111111   0.000015s  0.020s  0.038s  0.073s
  (* Master, + Selected, - Candidate, x Unusable) (p Preferred, ~ Configured)
```

show ntp associations detail

- Use to view the information about the NTP servers you assigned.
- Field descriptions
  - Peer—IP address of server, status of the server: configured, master, selected, candidate, correct, or unusable
    - configured—Confirmation that you assigned this NTP server to the system
    - master—System has chosen this server as the master
    - selected—System will consider this server when it chooses the master
    - candidate—System may consider this server when it chooses the master
    - correct—System considers the server's clock to be reasonably correct
    - unusable—Server does not meet the initial criteria for the master
    - stratum—Number of hops between the server and its stratum 1 server
    - Peer is a Broadcast/Configured Server—Type of NTP server: one that broadcasts NTP messages or one you have configured for NTP services
    - version—Version of NTP on the server
    - polled every—Time between NTP requests from the system to the server
    - polls every—Time between NTP requests from the server to its NTP servers
    - Root Delay—Round-trip time between the server and its stratum 1 root server
    - Root Dispersion—Measure of all the errors associated with the network hops and servers between the server and its stratum 1 server
    - Sync Dist.—Measure of the total time error since the update in the path to the stratum 1 server
    - Peer Delay—Round-trip delay, with the lowest dispersion value in the sample buffer, between the system and the server
    - Peer Dispersion—Lowest measure, in the sample buffer, of the error associated with the peer offset, based on the peer delay and precision

- Offset—Difference, with the lowest dispersion in the sample buffer, between the system's clock and the server's clock
- Reachability—8-bit number that shows whether or not the NTP server responded to the last eight requests from the system; one indicates a response; zero indicates no response. For example, 11111111 indicates that the NTP server responded to the last eight requests. If the system reaches one server less often than it does other servers, that server is not a good choice for the master.
- Precision—Length of the clock tick (interrupt interval) of the server's clock
- Source—IP address of the interface to which NTP servers should send NTP responses

- Timestamps of latest time samples from this peer; actual timestamps displayed depends on how the server is configured
  - Root reference at—Last time at which the stratum 1 server sent an NTP reply to the server
  - Last request sent—Last time at which the system sent an NTP request to the server
  - Response/Broadcast was sent—Last time at which the server sent an NTP reply or broadcast to the system
  - Response/Broadcast received—Last time at which the system received an NTP reply or broadcast from this server
- Sample buffer for this peer contains the following samples:
  - Delay—Round-trip delay from client to server
  - Offset—Difference between client's and server's clocks
  - Dispersion—Measure of the errors of the offset values, based on the round-trip delay and the precisions of the system and the server

- Example

```
host1#show ntp associations detail

Peer 10.6.129.58 is selected, stratum 3
   Peer is a Broadcast Server, version 3, broadcasts every 64 sec
   Root Delay 0.059052 sec, Dispersion 0.189056 sec, Sync Dist. 0.229679 sec
   Peer Delay -0.000016 sec, Dispersion 0.009665 sec, Offset 0.050714 sec
   Reachability 11111110, Precision 0.000000 sec
   'Source' Interface : default (transmit interface)
 Timestamps of latest time sample from this peer:
   Root reference  at:  Thu, Apr 13 2000 17:27:17.145 from 128.118.25.3
   Broadcast was sent:  Thu, Apr 13 2000 17:42:02.118
   Broadcast received:  Thu, Apr 13 2000 17:42:02.067
 Sample buffer for this peer contains the following samples:
   Delay      (sec):   0.000  0.000  0.000  0.000  0.000  0.000  0.000  0.000
   Offset     (sec):   0.049  0.050  0.050  0.050  0.050  0.050  0.051  0.051
   Dispersion (sec):   0.015  0.015  0.014  0.013  0.012  0.011  0.010  0.009
```

show ntp status

- Use to view the configuration and status of the system.
- Field descriptions
  - NTP Status—State of NTP on the system and the stratum number of the server
  - No. of associations—Number of peer associations for the NTP server
  - Clock Status:
    - Offset Error—Time difference between the system and the master, in seconds
    - Frequency Error—Error in the frequency of the system's clock, in seconds per second
    - Last Update—Last time received from the master
    - Root Dispersion—Measure of all the errors associated with the network hops and servers between the system and its stratum 1 server, in seconds
  - Configuration:
    - Admin. State—Status of NTP on the router (enabled or disabled)
    - Virtual Router Name—Name of the virtual router to which you attached NTP
    - Broadcast Delay—Time for a broadcast message to travel between the server and the client, in microseconds
    - Client Mode—NTP client status (True – system is an NTP client; False – system is not an NTP client)
    - Master Mode—NTP server status (True – system is configured as an NTP server; False – system is not configured as an NTP server)
    - Stratum No.—Stratum number of system if configured as NTP server
    - Summer Time—Status of seasonal time, True or False
    - Summer Timezone Name—Name of summer time zone
    - Timezone Name—Name of time zone
    - Timezone Offset—Time difference between the time zone and UTC, in hours:minutes
    - Access List—Identities of access lists of servers from which the system does not accept broadcasts
    - 'Server Source' Interface—Interface through which responses from the NTP server are directed; configured through the **ntp server source** command, which overrides the interface configured through the **ntp source** command.
    - 'Client Source' Interface—Interface through which all NTP server responses are directed; configured through the **ntp source** command.
    - Source Interface—IP address of the interface to which NTP servers should send NTP responses
    - Address—IP address of interface

- Enable—Status of NTP on the interface, On or Off
- BcastClient—Indication of whether or not this interface accepts broadcasts from NTP servers, On or Off
- BcastServer—Indication of whether or not this interface functions as a broadcast server, On or Off
- Name—Type of interface and its location

- Example

```
host1#show ntp status
Network Time Protocol (NTP v.4)

 NTP Status                   :No valid NTP server available
   No. of associations        : 0
 Clock Status                 :Initializing: frequency to be calibrated
   Offset Error               : 0 sec, amortizing asymptotically
   Frequency Error            : 0 sec/sec, compensating every second
   Last Update                :
   Root Dispersion            : 0 sec
 Configuration:
   Admin. State               : NTP Enabled
   Virtual Router Name        : default
   Broadcast Delay            : 3000 microseconds
   Client Mode                : True
   Master Mode                : False
   Stratum No.                : Unspecified
   Summer Time                : False
   Summer Timezone Name       :
   Timezone Name              : UTC
   Timezone Offset            : 00:0  hours:minutes
   Access List                :
   'Server Source' Interface  :
   'Client Source' Interface  : Default (transmit interface)
 Interface Configuration      :
   Address     Enable    BcastClient  BcastServer   Name
   1.1.1.1      ON          ON           ON        FastEthernet1/0
```

Chapter 13

Configuring Virtual Routers

E-series routers allow you to create multiple logical or *virtual* routers in a single router. Each virtual router has its own separate set of IP interfaces, forwarding table, and instances of routing protocols.

This chapter contains the following sections:

- Overview on page 553
- Platform Considerations on page 555
- References on page 555
- Configuring Virtual Routers on page 555
- Monitoring Virtual Routers on page 560

Overview

Multiple distinct routers are supported within a single router, which allows service providers to configure multiple, separate, secure routers within a single chassis. These routers are identified as *virtual routers (VRs)*. Applications for this function include the creation of individual routers dedicated to wholesale customers, corporate virtual private network (VPN) users, or a specific traffic type.

Default Virtual Router

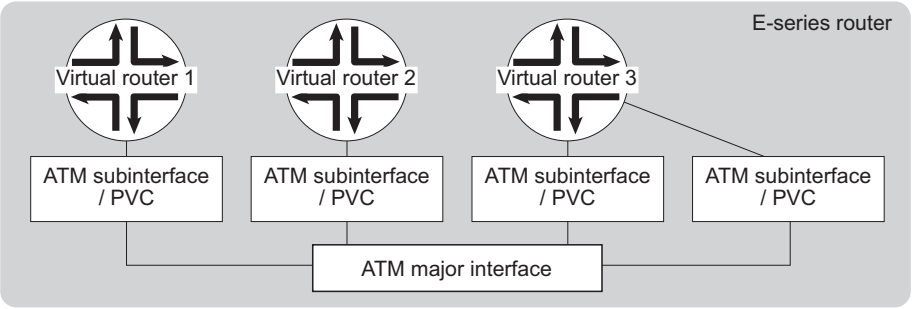
When you first boot your router, it creates a *default* virtual router. The only difference between the default VR and any other router is that you cannot create or delete the default VR. Just like any other router, the default VR gets its IP addresses when you add interfaces to it.

Virtual Router Instances

E-series routers can support up to 1,000 forwarding tables; that is, up to a total of 1,000 VRs and VPN routing and forwarding (VRF) instances. Each VRF has a forwarding table. A network device attaching to a router detects a router interface. The attaching device has no notion of the *virtual* router behind the interface.

For example, a physical ATM link may have circuits that are connected to different VRs. The physical and data link layers are not aware that there are multiple router instances. See Figure 31.

Figure 31: Virtual Routers



VRs and VRFs are tools for implementing VPNs.

Routing Protocols

Your router implements the VRs by maintaining a separate instance of each data structure for each VR and allowing each protocol (for example, TCP/UDP, RIP, OSPF, and IS-IS) to be enabled on a case-by-case basis. A table of router interfaces associates user connections (for example, PPP or ATM) with one or more IP interfaces within a VR.

VPNs and VRFs

Your router supports VPNs and VRFs. For information about VPNs and VRFs, see *Configuring BGP VPN Services* and *Monitoring BGP/MPLS VPNs* in *JUNOSe BGP and MPLS Configuration Guide, Chapter 3, Configuring BGP-MPLS Applications*.

VPNs

A VPN is a set of sites attached to a common network, but whose data is handled separately from that common network.

VPNs enable private IP traffic to travel over a public TCP/IP network by tunneling that traffic between VPN member sites. Different levels of security are available depending on the security of the tunnel used between sites.

Your router supports VPNs consisting of VRs or VRFs. See RFC 2547—BGP/MPLS VPNs (March 1999). Additionally, your router supports tunnels built from GRE, IPSec, L2TP, MPLS, and tunnels built from layer 2 circuits, such as Frame Relay and ATM.

VRFs

A VRF is a virtual routing and forwarding instance that exists within the context of a VR. The VRF provides forwarding information to your router. The system looks up a packet's destination in the VRF associated with the interface on which the packet is received. In general, any application that can be enabled in a VR can be enabled in a VRF. VRFs are generally associated with the VPN behavior described in RFC 2547—BGP/MPLS VPNs (March 1999).

When a VRF receives an update message, it needs to know whether it should add the route to its routing table. Similarly, when a VRF sends update messages, it needs to identify the VPNs that it wants to receive the updates. See *JUNOSe BGP and MPLS Configuration Guide, Chapter 3, Configuring BGP-MPLS Applications*.

Platform Considerations

Virtual routers are supported on all E-series routers.

For information about the modules supported on E-series routers:

- See the *ERX Module Guide* for modules supported on ERX-7xx models, ERX-14xx models, and the ERX-310 router.
- See the *E120 and E320 Module Guide* for modules supported on the E120 router and the E320 router.

References

For more information about virtual routers, VPNs, or VRFs, consult the following resources:

- *JUNOSe Release Notes*, *Appendix A*, *System Maximums*—Refer to the Release Notes corresponding to your software release for information about maximum values.
- *JUNOSe BGP and MPLS Configuration Guide, Chapter 3, Configuring BGP-MPLS Applications*
- RFC 2547—BGP/MPLS VPNs (March 1999)
- RFC 2917—A Core MPLS IP Architecture (September 2000)

Configuring Virtual Routers

This section provides examples of some of the more common virtual router tasks.

There are different uses of the **virtual-router** command. You can create or access VRs and VRFs in Global Configuration mode or map a VR to a domain map in Domain Map Configuration mode. After you have created a VR, you can continue to work in different command modes and configure the same user interface parameters as before the virtual router was created.

For information about the many VR tasks you can configure, see the related chapter; for example, *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP* or *JUNOSe BGP and MPLS Configuration Guide, Chapter 1, Configuring BGP Routing*.

To configure a virtual router:

- Create and name a VR in Configuration mode.

  ```
  host1(config)#virtual-router western
  host1:western(config)#
  ```

- Create a VRF to provide forwarding information to your router. In this example, the VRF created is in context with the VR created above.

  ```
  host1:western(config)#ip vrf eastern
  Proceed with new VRF creation? [confirm]
  host1:western(config-vrf)#virtual-router:eastern
  host1:western:eastern(config)#
  ```

- Access a VRF from the context of a different VR.

  ```
  host1(config)#virtual-router western:eastern
  host1:western:eastern(config)#
  ```

- View your configuration choices from a VR or VRF context.

```
host1:western:eastern(config)#?
aaa                     Configure authentication, authorization,
                          and accounting characteristics
  access-list           Configure an access list entry
  arp                   Configure a static ARP entry
  bandwidth             Configure slot-group bandwidth control
  banner                Define a banner line
  baseline              Configure baseline operations
  boot                  Configure boot time behavior
  bulkstats             Configure bulkstats parameters
  classifier-list       Configure a classifier list entry
  clns                  Configure CLNS characteristics
  clock                 Set the system's clock
  controller            Configure controller parameters
  crypto                Configure cryptographic parameters
  disable-autosync      Disable automatic synchronization of
                        redundant system controller file system
  disable-switch-on-error  Disable automatic switch to redundant system
                        controller upon software/hardware error
  enable                Configure security related options
  end                   Exit Global Configuration mode
  exception             Configure core dump
  exclude-subsystem     Exclude copying a subsystem from the release
  exit                  Exit from the current command mode
  ftp-server            Configure FTP Server characteristics
  help                  Describe the interactive help system
  host                  Add/modify an entry to the host table
  hostname              Set the host (system) name
  interface             Enter Interface Configuration mode
  ip                    Configure IP characteristics
  l2tp                  Configure L2TP parameters
  license               Configure licenses
```

```
  line                    Enter Line Configuration mode
  log                     Configure logging settings
  macro                   Run a CLI macro
  map-list                Create an NBMA static map
  memory                  Configure and administer memory operations
  mpls                    Configure MPLS global parameters
  no                      Negate a command or set its default(s)
  ntp                     Configure the Network Time Protocol
  policy-list             Enter Policy Configuration mode
  pppoe                   Configure PPPoE
  profile                 Specify a profile
  radius                  Configure RADIUS server
  rate-limit-profile      Enter rate limit profile configuration mode
  redundancy              Perform a redundancy configuration
  route-map               Configure a route map
  router                  Configure a routing protocol
  rtr                     Configure rtr parameters
  service                 Configure system-level services
  set                     Configure
  sleep                   Make the Command Interface pause for a
                          specified duration
  slot                    Configure and administer slot operation
  snmp-server             Configure SNMP parameters
  sscc                    The SSC Client
  telnet                  telnet daemon configuration
  timing                  Configure network timing
  traffic-shape-profile   Enter traffic shape profile configuration mode
  virtual-router          Specify a virtual router
host1:western:eastern(config)#
```

- View the VRF configuration choices from VRF Configuration mode.

```
host1:western(config-vrf)#?
  exit          Exit from the current command mode
  export        Specify VRF export characteristics
  help          Describe the interactive help system
  import        Specify VRF import characteristics
  log           Configure logging settings
  macro         Run a CLI macro
  no            Negate a command or set its default(s)
  rd            Specify route distinguisher
  route-target  Specify VPN extended community Target
  sleep         Make the Command Interface pause for a
                 specified duration
host1:western(config-vrf)#
```

- Access a VR to configure it with an interior gateway protocol (IGP) or exterior gateway protocol (EGP) to learn routes from a customer edge (CE) device. See the related routing protocol chapters for detailed information.

Example 1
VR with an IGP

```
host1(config)#virtual-router miami
host1:miami(config)#router ospf 5
host1:miami(config-router)#
```

Example 2
VR with an EGP

```
host1(config)#virtual-router western
host1:western(config)#router bgp 359
host1:western(config-router)#
```

- Configure a Telnet daemon to listen in VRs other than the default VR.

  host1(config)#**virtual-router boston**
  host1:boston(config)#**telnet listen port 23**

- List all VRs and VRFs on the router.

```
host1#show virtual-router
Virtual Router : default
Virtual Router : thursday
Virtual Router : western
                 VRF : eastern
Virtual Router : boston
Virtual Router : miami
Virtual Router : northern
                 VRF : southern
host1#
```

- Map a VR to a user domain name in Domain Map Configuration mode. The VR must already exist.

  host1(config)#**aaa domain-map jacksonville**
  host1(config-domain-map)#**virtual-router western**
  host1(config-domain-map)#

aaa domain-map

- Use to map a user domain name to a virtual router.
- Examples

  host1-0-1-90(config)#**aaa domain-map juniper.net vrouter_1**
  host1-0-1-90(config)#**aaa domain-map none vrouter__all_purpose**
  host1-0-1-90(config)#**aaa domain-map DEFAULT vrouter_all_purpose**

- Use the **no** version to delete the domain map.

ip vrf

- Use to create a VRF or access VRF Configuration mode to configure a VRF.
- You must specify a route distinguisher after you create a VRF. Otherwise, the VRF will not operate.
- Example

  host1-00-02-80:boston(config)#**ip vrf vpn-A**

- Use the **no** version to remove a VRF.

telnet listen

- Use to create a Telnet daemon to listen in a virtual router.
- Example

  host1(config)#**virtual-router 3**
  host1:3(config)#**telnet listen port 3223**

- Use the **no** version to delete the daemon.

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.
- From Domain Map Configuration mode, use this command to map the VR to a user domain name. Use the **no** version in this mode to delete the VR parameter and assign the default VR.
- A VR name consists of 1–32 alphanumeric characters.
- After you are in the context of a particular VR or VRF (indicated by the change in the prompt), all subsequent commands you enter apply to that context until you exit the context.
- Use the **no** version of the command only to delete the VR and return the router to the default VR. Issuing the command **no virtual-router** *vrName.vrfName* has no effect.
- Issuing a **no** version of this command (**no virtual-router :***vrfName* or **no virtual-router** *vrName***:***vrfName*) that specifies an existing VRF displays only the error message: "Cannot delete a VRF with this command." You must use the **no ip vrf** command to remove a VRF.

NOTE: See the *JUNOSe Command Reference Guide* for additional information.

- Use the **wait-for-completion** keyword with the **no** version if you require a synchronous deletion of a VR, such as when executing Telnet or console commands through an external script. Alternatively, you might want to use this keyword if the VR being deleted has many configured VRFs and someone might attempt to re-create the VR before all the VRFs have been deleted. If you do not issue the **wait-for-completion** keyword in those circumstances, a **virtual-router** command issued as soon as the prompt appears could fail because the router is still deleting VRFs. You can specify a period during which the CLI waits before it returns a prompt. If you do not specify a wait time, then the CLI does not return a prompt until the operation is complete. You can press Ctrl + c to break out of the wait period early.

Monitoring Virtual Routers

Use the **show virtual-router**, the **show configuration virtual router**, and **show aaa domain-map** commands to display virtual router and user-domain-to-virtual-router mapping information. Use the **show ip forwarding table** command to display information about memory usage by virtual routers.

show aaa domain-map

- Use to display the mapping between user domains and virtual routers.
- The following keywords have significance when used as user domains:
  - **none**—All client requests with no user domain name are associated with the virtual router mapped to the *none* entry
  - **default**—All client requests with a domain present that has no map are associated with the virtual router mapped to the *default* entry
- Example

```
host1#show aaa domain-map
Domain: boston; virtual-router: default

Tunnel Tunnel Tunnel Tunnel Tunnel  Tunnel   Tunnel  Tunnel
 Tag    Peer  Source  Type  Medium Password   Id    Hostname
------ ------ ------ ------ ------ --------  ------ --------
31     <null> <null> l2tp   ipv4   <null>    <null> <null>

         Tunnel
Tunnel   Server     Tunnel
 Tag      Name    Preference
------   ------   ----------
31       <null>   2000
```

show configuration virtual-router

- Use to display configuration information for the virtual routers configured on your router.
- You can create a configuration script from the output by saving it as a file with the .scr extension.
- You can exclude information about a particular type of interface.
- You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string that you specify. See *Chapter 2, Command-Line Interface*, for details.
- Example

```
host1#show configuration virtual-router default
virtual-router default
ip domain-lookup
ip name-server 10.2.0.3
ip domain-name "junipercom.com"
!
host f 10.10.0.129 ftp anonymous null
interface null 0
!
interface fastEthernet 0/0
 ip address 192.168.1.155 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

```
no ip multicast-routing
!
mpls rsvp profile default
mpls ldp profile default
!
rtr 1
 type echo protocol ipIcmpEcho 10.5.0.200 source fastEthernet0/0
 frequency 1
 samples-of-history-kept 5
 timeout 10000
!
```

show ip forwarding-table slot

- Use to display the memory used by each VR configured on a line module and free memory available on the line module.
- Field descriptions
  - Free Memory—Amount of memory free on the line module, in kilobytes
  - Virtual Router—Name of the virtual routers configured on the line module
  - Memory (KB)—Amount of memory consumed by the VR, in kilobytes
  - Load Errors—Counts errors made while loading the routing table on the line module
  - Status—Indicates whether the routing table for the VR is valid
- Example

```
host1#show ip forwarding-table slot 9
Free Memory = 14,328KB
  Virtual Router      Memory       Load Errors     Status
                      (KB)
-----------------     ---------    -------------    --------
   vr1                 4128              0          Valid
   vr2                 3136              0          Valid
   vr3                 2256              0          Valid
   vr4                 1512              0          Valid
 default               1024              0          Valid
------------------------------------------------------------
```

show virtual-router

- Use to display the virtual routers and VRFs configured on your router.
- Use the **summary** keyword to display only the total number of virtual routers and the total number of VRF instances.
- Use the **detail** keyword to display the status of the routing protocols configured for each virtual router.
- Use the **summary** keyword with the **detail** keyword to display the number of VRF instances for each virtual router.
- Use the output filtering feature of the **show** command to include or exclude lines of output based on a text string you specify. See *Chapter 2, Command-Line Interface*, for details.

- Example 1

```
host1#show virtual-router
Virtual Router : default
Virtual Router : vr1
                 VRF : eastern
                 VRF : western
                 VRF : northern
                 VRF : southern
Virtual Router : vr2
                 VRF : eastern
                 VRF : western
                 VRF : northern
                 VRF : southern
Virtual Router : vr3
                 VRF : eastern
                 VRF : western
                 VRF : northern
                 VRF : southern
```

- Example 2

```
host1#show virtual-router detail
Virtual Router : default
                       Ip:     Present
                       Ipv6:   Not Present
                       Mgtm:   Not Present
                       Mgtmv6: Not Present
                       Bgp:    Not Present
                       Isis:   Present
                       Ospf:   Not Present
                       Pim:    Not Present
                       Rip:    Not Present
                       Igmp:   Not Present
                       Mld:    Not Present
                       Dvmrp:  Not Present
Virtual Router : vr1
                       Ip:     Present
                       Ipv6:   Not Present
                       Mgtm:   Present
                       Mgtmv6: Not Present
                       Bgp:    Not Present
                       Isis:   Present
                       Ospf:   Present
                       Pim:    Present
                       Rip:    Not Present
                       Igmp:   Not Present
                       Mld:    Not Present
                       Dvmrp:  Not Present
```

- Example 3

```
host1#show virual-router summary detail
Virtual Router default                          VRF Count: 0
Virtual Router vr1                              VRF Count: 4
Virtual Router vr2                              VRF Count: 4
Virtual Router vr3                              VRF Count: 4

Total VR Count: 4
        VRs with    VRFs Count: 3
        VRs without VRFs Count: 1
Total VRF Count: 12
Total Count    : 16
```

Appendix A
Abbreviations and Acronyms

Abbreviation or Acronym	Term
A	
AAA	authentication, authorization, and accounting
AAAA	authentication, authorization, accounting, and address assignment
AAL	ATM Adaptation Layer
ABR	area border router
AC	alternating current; access concentrator
ACCM	Async Control Character Map
ADSL	asymmetric digital subscriber line
AESA	ATM end system address
AF	assured forwarding
AFI	authority and format identifier
AH	authentication header
AIS	alarm indication signal
AIS-L	alarm indication signal – line
AIS-P	alarm indication signal – path
ALG	application-level gateway
ANSI	American National Standards Institute
API	application programming interface
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	autonomous system; Australia (re standards compliance)
AS boundary router	autonomous system boundary router
ASCII	American Standard Code for Information Interchange
ASIC	application-specific integrated circuit
AS number	autonomous system number
ATM	Asynchronous Transfer Mode
AVP	attribute-value pair

Abbreviation or Acronym	Term
B	
backup DR	backup designated router
BECN	backward explicit congestion notification
BER	bit error rate
BERT	bit error rate test
BFD	Bidirectional Forwarding Detection (protocol)
BGP	Border Gateway Protocol
BMA	broadcast multiaccess
BOOTP	bootstrap protocol
B-RAS	Broadband Remote Access Server
BSD	Berkeley Software Distribution
C	
CA	certificate authority
CAC	call admission control (MPLS); connection admission control (ATM)
CAM	content-addressable memory
CAP	carrierless amplitude phase
CAR	committed access rate
CARS	committed access rate service
CBC	cipher block chaining
CBR	constant bit rate
CC	continuity check
CCITT	International Telegraph and Telephone Consultative Committee
CCP	Compression Control Protocol
CDV	cell delay variation
CDVT	cell delay variation tolerance
CE	customer edge device
CHAP	Challenge Handshake Authentication Protocol
CIDR	classless interdomain routing
CISPR	International Special Committee on Radio Interference
CLACL	classifier control list
CLEC	competitive local exchange carrier
CLI	command-line interface
CLNP	Connectionless Network Protocol
CLNS	Connectionless Network Service
CLP	cell loss priority
CMDA	code division multiple access
CMTS	cable modem termination system
CoA	change of authorization

Abbreviation or Acronym	Term
cOC	channelized optical carrier
COPS	Common Open Policy Service (protocol)
CORBA	Common Object Request Broker Architecture
CoS	class of service
CPE	customer premises equipment
CPU	central processing unit
CRC	cyclic redundancy check
CR-LDP	Constraint-Based Routed Label Distribution Protocol
CR-LSP	constraint-based routed label-switched path
CSNP	complete sequence number PDU (protocol data unit)
CSU	channel service unit
CT1, CT3	channelized T1, T3
CTI	computer telephony integration
CTS	clear to send
CTT	connection traffic table
CUL	agreement between Underwriter Laboratories and Canadian Standards Association for joint product safety approval
D	
DC	direct current
DCC	Data Country Code
DCD	data carrier detect
DCE	data communication equipment
DCM	dynamic configuration manager
DE	discard eligibility
DES; 3DES	Data Encryption Standard; triple DES
DF	don't fragment (bit)
DHCP	Dynamic Host Configuration Protocol
DIS	designated intermediate system
DLCI	data-link connection identifier
DLCMI	data-link connection management interface
DMZ	demilitarized zone
DNIS	dialed number identification service
DNS	Domain Name System
DNS-ALG	Domain Name System – Application Level Gateway
DOCSIS	Data over Cable System Interface Specifications
DoS	denial of service
DPD	dead peer detection
DR	designated router
DS	digital signal; DiffServ

Abbreviation or Acronym	Term
DS-BGP	dual-stack Border Gateway Protocol
DSI	dynamic subscriber interface
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DSP	domain-specific part
DSR	data set ready
DSS	Digital Signature Standard
DST	Daylight Saving Time
DSU	data service unit
DTE	data terminal equipment
DTR	data terminal ready
DU	downstream unsolicited
DVMRP	Distance Vector Multicast Routing Protocol
DXI	data exchange interface (abbreviation pronounced “dixie”)
E	
EAP	Extensible Authentication Protocol
EBGP	external Border Gateway Protocol
ECC	error checking and correction; error-checking code
ECMP	equal-cost multipath
ECP	Encryption Control Protocol
EEPROM	electrically erasable programmable read-only memory
EF	expedited forwarding
EFA	egress forwarding ASIC
EGP	exterior gateway protocol
E-LSP	EXP-inferred-PSC LSP
EN	European Norm
EPD	early packet discard
ES	end system
ESD	electrostatic discharge
ESF	extended superframe
ESI	end system identifier
ESP	Encapsulating Security Payload
EXP	experimental (refers to bits in MPLS shim header)
F	
FAT	file allocation table
FCC	Federal Communications Commission
FCS	frame check sequence
FDL	facilities data link

Abbreviation or Acronym	Term
FE	Fast Ethernet
FE-2	dual-port Fast Ethernet
FEC	forwarding equivalence class (abbreviation pronounced “feck”)
FECN	forward explicit congestion notification
FERF	far-end receive failure
FFA	frame forwarding ASIC
FIB	forwarding information base
FIFO	first-in, first-out
FIN	finish (bit)
FPGA	field programmable gate array
FQDN	fully qualified domain name
FRU	field-replaceable unit
FSM	finite state machine
FTE	forwarding table entry
FTP	File Transfer Protocol
G	
Gbps	gigabits per second
GE	Gigabit Ethernet
giaddr	gateway IP address
GRE	Generic Routing Encapsulation
GRxx	(refers to Bellcore standards)
GUI	graphical user interface
H	
HAR	hierarchical assured rate
HDLC	High-Level Data Link Control; High-Speed Data Link Control
HMAC	Hashed Message Authentication Code
HO-DSP	high-order domain-specific part
HRR	hierarchical round-robin
HSSI	high-speed serial interface (abbreviation pronounced “hissy”)
I	
I/O	input/output
IANA	Internet Assigned Numbers Authority
IAPP	Inter Access Point Protocol
IBGP	internal Border Gateway Protocol
IC CS	Industry Canada Communications Section
ICD	International Code Designator
ICMP	Internet Control Message Protocol
ICRQ	incoming-call request

Abbreviation or Acronym	Term
ID	identification; identifying; identifier
I-DAS	integrated DHCP access server
IDI	initial domain identifier
IDP	initial domain part
IDSL	ISDN digital subscriber line
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	interior gateway protocol
IIF	incoming interface
IKE	Internet Key Exchange
ILEC	incumbent local exchange carrier
ILMI	Integrated Local Management Interface
InARP	Inverse Address Resolution Protocol
IOA	input/output adapter
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPoA	Internet Protocol over Asynchronous Transfer Mode
IPSec	Internet Protocol Security
IRDP	ICMP Router Discovery Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System–to–Intermediate System
ISM	IPSec Service module
ISO	International Organization for Standardization
ISP	Internet service provider
IS Voice	Intelligent Service Voice application
ITU-T	International Telecommunication Union – Telecommunication Standardization
J	
JATE	Japan Approvals Institute for Telecommunications Terminal Equipment
JDBC	Java Database Connectivity
K	
KB	kilobyte(s)
Kbps	kilobits per second
L	
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP access concentrator

Abbreviation or Acronym	Term
LAG	link aggregation group
LAN	local area network
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LDP	Label Distribution Protocol
LED	light-emitting diode
LER	label edge router
LIB	label information base
LIP	Link Integrity Protocol
LLC	logical link control
L-LSP	label-only-inferred-PSC LSP
LMI	local management interface; link management interface
LNS	L2TP network server
LOF	loss of frame
LOP	loss of pointer
LOS	loss of signal
LSA	link-state advertisement
LSDB	link-state database
LSP	label-switched path; link-state PDU; link-state protocol
LSR	label-switching router
M	
MAC	media access control; Message Authentication Code
MAU	medium attachment unit
MB	megabyte(s)
MBGP	multicast Border Gateway Protocol
MBone	multicast backbone
Mbps	megabits per second
MBS	maximum burst size
MD5	Message Digest 5
MDL	maintenance data link
MD*x*	Message Digest *x* (hash algorithm)
MED	multiple exit discriminator
MGTM	multicast group table manager
MIB	Management Information Base
MLFR	Multilink Frame Relay
MLPPP	Multilink Point-to-Point Protocol
motd	message of the day
MOTM	message of the minute

Abbreviation or Acronym	Term
MP-BGP	Border Gateway Protocol multiprotocol extensions (sometimes referred to as multiprotocol Border Gateway Protocol)
MPLS	Multiprotocol Label Switching
mrinfo	multicast router information
MRRU	multilink maximum received reconstructed unit
MRU	maximum receive unit
MSDP	Multicast Source Discovery Protocol
MSO	multiple service operator
MSP	Multiplex Section Protection
MSS	maximum segment size
MTU	maximum transmission unit; multitenant unit
N	
NAK	negative acknowledgment
NAPT	Network Address Port Translation
NAS	network access server
NAT	Network Address Translation
NBMA	nonbroadcast multiaccess
NCP	Network Control Protocol
ND	Neighbor Discovery
NEBS	Network Equipment Building System
NET	network entity title
NLRI	network layer reachability information
NMC	Network Management Center
NMS	network management system
NNI	network-to-network interface
NRZ	nonreturn to zero
NRZI	nonreturn to zero inverted
NSAP	network service access point
NSF	nonstop forwarding
NSSA	not-so-stubby area (refers to OSPF routing)
NTP	Network Time Protocol
NVRAM	nonvolatile random-access memory
NVS	nonvolatile storage
O	
OAM	operations, administration, and management
OC	optical carrier
ODBC	Open Database Connectivity
OID	object identifier
OIF	outgoing interface

Abbreviation or Acronym	Term
ORF	outbound route filter; outbound route filtering
OSI	Open Systems Interconnection
OSINLCP	OSI Internet Link Control Protocol; OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OSS	operations support system
P	
P	provider core router
PADI	PPPoE Active Discovery Initiation
PADM	PPPoE Active Discovery Message
PADN	PPPoE Active Discovery Network
PADO	PPPoE Active Discovery Offer
PADR	PPPoE Active Discovery Request
PADS	PPPoE Active Discovery Session
PADT	PPPoE Active Discovery Termination
PAP	Password Authentication Protocol
PBX	private branch exchange
PCMCIA	Personal Computer Memory Card International Association
PCR	peak cell rate
PDU	protocol data unit
PE	provider edge router
PFC	Protocol Field Compression
PFS	perfect forward secrecy
PHB	per-hop behavior
PHP	penultimate hop pop
PIB	Policy Information Base
PIM	Protocol Independent Multicast; power input module
PIM DM	Protocol Independent Multicast dense mode
PIM S-DM	Protocol Independent Multicast sparse-dense mode
PIM SM	Protocol Independent Multicast sparse mode
PIM SSM	Protocol Independent Multicast source-specific multicast
PKI	public key infrastructure
PLCP	physical layer convergence procedure
PM	policy manager
PNNI	private network-to-network interface
POP	point of presence
POS	packet over SONET
POST	power-on self-test
PPP	Point-to-Point Protocol

Abbreviation or Acronym	Term
PPPoE	Point-to-Point Protocol over Ethernet
pps	packets per second
PROM	programmable read-only memory
PSC	per-hop scheduling class
PSNP	partial sequence number PDU (protocol data unit)
PVC	permanent virtual circuit (or connection)
Q	
QoS	quality of service
R	
RADIUS	Remote Authentication Dial-In User Service
RD	route distinguisher
RDBS	relational database system
RDI	remote defect indication
RED	random early detection
REI	remote error indication
RESV	reservation
RFC	Request for Comments
RIB	routing information base
RIP	Routing Information Protocol
RISC	reduced instruction set computing
RMI	Remote Method Invocation (Java)
RP	rendezvous point (router)
RPF	reverse-path forwarding
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol with traffic engineering extensions
RTM	resource threshold monitor
RTR	Response Time Reporter
RTSP	Real-Time Streaming Protocol
RWS	receive window size
RX	receive
S	
SA	security association
SAFI	subsequent address family identifier
SAR	segmentation and reassembly
SC	system controller
SCCRQ	Start-Control-Connection-Request
SCEP	Simple Certificate Enrollment Protocol

Abbreviation or Acronym	Term
SCR	sustained cell rate
SCSI	small computer system interface (abbreviation pronounced “scuzzy”)
SDH	Synchronous Digital Hierarchy
SDRAM	synchronous dynamic random access memory
SDSL	symmetric digital subscriber line
SDU	service data unit
SDX	Service Deployment System (formerly SSC)
SEF	severely errored framing
SES	severely errored second
SFP	small form-factor pluggable transceiver
(S,G)	source (S) of the multicast packet and the destination multicast group address (G)
SHA	Secure Hash Algorithm
SIP	SMDS Interface Protocol
SLA	service level agreement
SLARP	Serial Line Address Resolution Protocol
SM	Service line module
SMF	single-mode fiber
SMM	switch management module
SNAP	Subnetwork Access Protocol; subnetwork attachment point
SNI	SMDS network interface
SNMP	Simple Network Management Protocol
SNPA	subnet point of attachment
SNTP	Simple Network Time Protocol
SODIMM	small outline dual inline memory module
SONET	Synchronous Optical Network
SPD	security policy database
SPF	shortest path first
SPI	security parameter index
SPQ	strict-priority queues
SPVC	soft permanent virtual circuit
SQL	Structured Query Language
SRP	switch route processor
SRT	source-rooted tree
SSC	Service Selection Center (no longer used; *see* SDX)
SSH	Secure Shell
SSN	short sequence number
STM	Synchronous Transport module
SVC	switched virtual circuit

Abbreviation or Acronym	Term
S-VLAN	stacked virtual local area network
SYN	synchronize (bit)
T	
TAC	Technical Assistance Center
TACACS	Terminal Access Controller Access Control System
TC	transmission convergence
TCP	Transmission Control Protocol
TE	traffic engineering
TFTP	Trivial File Transfer Protocol
TIP	terminal interface processor
TLV	type-length-value
ToS	type of service
TPID	Tag Protocol Identifier
TSM	Tunnel Service line module
TTL	time-to-live
TU	tributary unit
TUG	tributary unit group
TX	transmit
U	
U	unit of measurement for rack-mounted equipment (a U is 1.75 in., or 4.44 cm)
UBR	unspecified bit rate
UDP	User Datagram Protocol
UI	user interface
UL	Underwriter Laboratories
UMTS	universal mobile telecommunications system
UNI	user-network interface (ATM usage); user-to-network interface
UPC	user parameter control
URL	Uniform Resource Locator
USM	user-based security model
UTC	Coordinated Universal Time
V	
VAC	volts alternating current
VBR	variable bit rate
VBR-NRT	variable bit rate, non–real time
VBR-RT	variable bit rate, real time
VC	virtual circuit (or connection)
VCC	virtual channel connection
VCCI	Voluntary Control Council for Interference

Abbreviation or Acronym	Term
VCD	virtual circuit descriptor
VCI	virtual channel identifier
VDC	volts direct current
VDSL	very-high-bit-rate digital subscriber line
VLAN	virtual local area network
VoIP	voice over Internet Protocol
VOQL	virtual output queue length
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPN	virtual private network
VR	virtual router
VRF	VPN routing and forwarding instance
VRID	virtual router identifier
VRRP	Virtual Router Redundancy Protocol
VSA	vendor-specific attribute (RADIUS)
VT	virtual tributary
VTS	VPN Tunnel Server
vty	virtual terminal
W	
WAN	wide area network
WAP	wireless access point
WEP	Wired Equivalent Privacy
WFQ	weighted fair queuing
WINS	Windows Internet Name Service (Microsoft)
WLAN	wireless local area network
WLL	wireless local loop
WRED	weighted random early detection
WRR	weighted round-robin
X	
xDSL	combined term used to refer to ADSL, HDSL, SDSL, and VDSL
XFP	10-gigabit small form-factor pluggable transceiver

Appendix B
References

This document lists RFCs, draft RFCs, other software standards, hardware standards, and other references that provide information about the protocols and features supported by the system.

- RFCs on page 578
- Draft RFCs on page 586
- Other Software Standards on page 588
- Hardware Standards on page 590

RFCs

Table 61: E-series RFCs

Reference	Protocol or Feature
RFC 4762—Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling (January 2007)	VPLS
RFC 4684—Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs) (2006)	BGP/MPLS VPNs
RFC 4679—DSL Forum Vendor-Specific RADIUS Attributes (September 2006)	RADIUS
RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) (April 2006)	VPLS
RFC 4379—Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (February 2006)	MPLS; BGP/MPLS VPNs
RFC 4243—Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option (December 2005)	DHCP
RFC 4090—Fast Reroute Extensions to RSVP-TE for LSP Tunnels (May 2005)	MPLS
RFC 3847—Restart Signaling for Intermediate System to Intermediate System (IS-IS) (July 2004)	IS-IS
RFC 3784—Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE) (June 2004)	IS-IS
RFC 3748—Extensible Authentication Protocol (EAP) (June 2004)	PPP
RFC 3715—IPsec-Network Address Transation (NAT) Compatibility Requirements (March 2004)	L2TP over IPSec
RFC 3710—Multicast Listener Discovery (MLD) for IPv6 (October 1999)	IPv6 multicasting
RFC 3706—A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers (February 2004)	IPSec
RFC 3646—DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (December 2003)	DHCP
RFC 3633—IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6 (December 2003)	DHCP
RFC 3630—Traffic Engineering (TE) Extensions to OSPF Version 2 (September 2003)	OSPF
RFC 3623—Graceful OSPF Restart (November 2003)	OSPF
RFC 3579—RADIUS EAP (September 2003)	PPP
RFC 3576—Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS) (July 2003)	RADIUS
RFC 3569—An Overview of Source-Specific Multicast (SSM) (July 2003)	IP multicasting
RFC 3564—Requirements for support of Differentiated Services-aware MPLS Traffic Engineering (July 2003)	MPLS
RFC 3539—Authentication, Authorization and Accounting (AAA) Transport Profile (June 2003)	RADIUS
RFC 3498—Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures (March 2003)	SONET APS redundancy
RFC 3479—Fault Tolerance for the Label Distribution Protocol (LDP) (February 2003)	MPLS
RFC 3478—Graceful Restart Mechanism for Label Distribution Protocol (February 2003)	MPLS
RFC 3473—Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions (January 2003)	MPLS
RFC 3471—Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description (January 2003)	MPLS

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 3447—Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 (February 2003)	Digital certificates
RFC 3443—Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks (January 2003)	MPLS
RFC 3419—Textual Conventions for Transport Addresses (December 2002)	IP
RFC 3418—Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (December 2002)	SNMP
RFC 3417—Transport Mappings for the Simple Network Management Protocol (SNMP) (December 2002)	SNMP
RFC 3416—Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) (December 2002)	SNMP
RFC 3415—View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) (December 2002)	SNMP
RFC 3414—User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (December 2002)	SNMP
RFC 3413—Simple Network Management Protocol (SNMP) Applications (December 2002)	SNMP
RFC 3412—Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (December 2002)	SNMP
RFC 3411—An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (December 2002)	SNMP
RFC 3410—Introduction and Applicability Statements for Internet Standard Management Framework (December 2002)	SNMP
RFC 3392—Capabilities Advertisement with BGP-4 (November 2002)	BGP; BGP/MPLS VPNs
RFC 3376—Internet Group Management Protocol (October 2002)	IP multicasting
RFC 3373—Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies (September 2002)	IS-IS
RFC 3344—IP Mobility Support for IPv4 (August 2002)	Mobile IP
RFC 3318—Framework Policy Information Base (March 2003)	COPS
RFC 3315—Dynamic Host Configuration Protocol for IPv6 (DHCPv6) (July 2003)	DHCP
RFC 3293—General Switch Management Protocol (GSMP) Packet Encapsulations for Asynchronous Transfer Mode (ATM), Ethernet and Transmission Control Protocol (TCP) (June 2002)	L2C
RFC 3292—General Switch Management Protocol (GSMP) V3 (June 2002)	IP multicasting; L2C
RFC 3291—Textual Conventions for Internet Network Addresses (May 2002)	IP
RFC 3280—Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (April 2002)	Digital certificates
RFC 3277—Intermediate System to Intermediate System (IS-IS) Transient Blackhole Avoidance (April 2002)	IS-IS
RFC 3270—Multi-Protocol Label Switching (MPLS) Support of Differentiated Services (May 2002)	MPLS
RFC 3260—New Terminology and Clarifications for Diffserv (April 2002)	QoS
RFC 3246—An Expedited Forwarding PHB (Per-Hop Behavior) (March 2002)	MPLS; QoS
RFC 3210—Applicability Statement for Extensions to RSVP for LSP-Tunnels (December 2001)	BGP/MPLS VPNs
RFC 3209—RSVP-TE: Extensions to RSVP for LSP Tunnels (December 2001)	BGP/MPLS VPNs
RFC 3198—Terminology for Policy-Based Management (November 2001)	Policy management

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 3193—Securing L2TP using IPSec (November 2001)	L2TP over IPSec
RFC 3159—Structure of Policy Provisioning Information (SPPI) (August 2001)	COPS
RFC 3145—L2TP Disconnect Cause Information (July 2001)	L2TP
RFC 3140—Per Hop Behavior Identification Codes (June 2001)	MPLS
RFC 3107—Carrying Label Information in BGP-4 (May 2001)	BGP/MPLS VPNs
RFC 3097—RSVP Cryptographic Authentication -- Updated Message Type Value (April 2001)	MPLS
RFC 3084—COPS Usage for Policy Provisioning (COPS-PR) (March 2001)	COPS
RFC 3065—Autonomous System Confederations for BGP (February 2001)	MPLS
RFC 3046—DHCP Relay Agent Information Option (January 2001)	Dynamic interfaces, RADIUS
RFC 3037—LDP Applicability (January 2001)	MPLS
RFC 3036—LDP Specification (January 2001)	MPLS, VPLS
RFC 3035—MPLS using LDP and ATM VC Switching (January 2001)	MPLS
RFC 3032—MPLS Label Stack Encoding (January 2001)	MPLS
RFC 3031—Multiprotocol Label Switching Architecture (January 2001)	MPLS
RFC 3027—Protocol Complications with the IP Network Address Translator (January 2001)	NAT
RFC 3024—Reverse Tunneling for Mobile IP, revised (January 2001)	Mobile IP
RFC 3022—Traditional IP Network Address Translator (Traditional NAT) (January 2001)	NAT
RFC 3014—Notification Log MIB (November 2000)	SNMP
RFC 2998—A Framework for Integrated Services Operation over Diffserv Networks (November 2000)	QoS
RFC 2993—Architecture Implications of NAT (November 2000)	NAT
RFC 2990—Next Steps for the IP QoS Architecture (November 2000)	QoS
RFC 2986—PKCS #10: Certification Request Syntax Specification Version 1.7 (November 2000)	Digital certificates
RFC 2981—Event MIB (October 2000)	Event Mgr
RFC 2973—IS-IS Mesh Groups (October 2000)	IS-IS
RFC 2966—Domain-wide Prefix Distribution with Two-Level IS-IS (October 2000)	IS-IS
RFC 2961—RSVP Refresh Overhead Reduction Extensions (April 2001)	MPLS
RFC 2934—Protocol Independent Multicast MIB for IPv4 (October 2000)	SNMP
RFC 2933—Internet Group Management Protocol MIB (October 2000)	SNMP
RFC 2932—IPv4 Multicast Routing MIB (October 2000)	SNMP
RFC 2925—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations (September 2000)	SNMP
RFC 2923—TCP Problems with Path MTU Discovery (September 2000)	IP
RFC 2918—Route Refresh Capability for BGP-4 (September 2000)	BGP
RFC 2917—A Core MPLS IP Architecture (September 2000)	MPLS
RFC 2890—Key and Sequence Number Extensions to GRE (September 2000)	GRE
RFC 2869—RADIUS Extensions (June 2000)	RADIUS
RFC 2868—RADIUS Attributes for Tunnel Protocol Support (June 2000)	RADIUS
RFC 2867—RADIUS Accounting Modifications for Tunnel Protocol Support (June 2000)	RADIUS

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 2866—RADIUS Accounting (June 2000)	Dynamic interfaces; RADIUS
RFC 2865—Remote Authentication Dial In User Service (RADIUS) (June 2000)	Dynamic interfaces; RADIUS; Mobile IP
RFC 2864—The Inverted Stack Table Extension to the Interfaces Group MIB (June 2000)	SNMP
RFC 2863—The Interfaces Group MIB (June 2000)	Ethernet; SNMP
RFC 2858—Multiprotocol Extensions for BGP-4 (June 2000)	BGP
RFC 2842—Capabilities Advertisement with BGP-4 (May 2000)	BGP
RFC 2836—Per Hop Behavior Identification Codes (May 2000)	MPLS; Policy, Management; QoS
RFC 2796—BGP Route Reflection—An Alternative to Full Mesh IBGP (April 2000)	BGP
RFC 2794—Mobile IP Network Access Identifier Extension for IPv4 (March 2000)	Mobile IP
RFC 2790—Host Resources MIB (March 2000)	SNMP
RFC 2787—Definitions of Managed Objects for the Virtual Router Redundancy Protocol (March 2000)	VRRP
RFC 2784—Generic Routing Encapsulation (GRE) (March 2000)	IP tunnels
RFC 2763—Dynamic Hostname Exchange Mechanism for IS-IS (February 2000)	IS-IS
RFC 2748—The COPS (Common Open Policy Service) Protocol (January 2000)	COPS
RFC 2747—RSVP Cryptographic Authentication (January 2000)	MPLS
RFC 2740—OSPF for IPv6	OSPF
RFC 2737—Entity MIB (Version 2) (December 1999)	SNMP
RFC 2716—PPP EAP TLS Authentication Protocol (October 1999)	PPP
RFC 2702—Requirements for Traffic Engineering over MPLS (September 1999)	MPLS
RFC 2698—A Two Rate Three Color Marker (September 1999)	Policy management; QoS
RFC 2697—A Single Rate Three Color Marker (September 1999)	Policy management
RFC 2694—DNS extensions to Network Address Translators (DNS_ALG) (September 1999)	NAT
RFC 2685—Virtual Private Networks Identifier (September 1999)	MPLS
RFC 2684—Multiprotocol Encapsulation over ATM Adaptation Layer 5 (September 1999)	ATM
RFC 2668—Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs) (August 1999)	Ethernet; SNMP
RFC 2667—IP Tunnel MIB (August 1999)	SNMP; IP tunnels
RFC 2665—Definitions of Managed Objects for the Ethernet-like Interface Types (August 1998)	Ethernet; SNMP
RFC 2663—IP Network Address Translator (NAT) Terminology and Considerations (August 1999)	NAT
RFC 2661—Layer Two Tunneling Protocol “L2TP” (August 1999)	L2TP
RFC 2616—Hypertext Transfer Protocol – HTTP/1.1 (June 1989)	HTTP
RFC 2615—PPP over SONET/SDH (June 1999)	POS
RFC 2598—An Expedited Forwarding PHB (June 1999)	QoS
RFC 2597—Assured Forwarding PHB Group (June 1999)	MPLS; Policy management; QoS
RFC 2580—Conformance Statements for SMIv2 (April 1999)	SNMP

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 2579—Textual Conventions for SMIv2 (April 1999)	SNMP
RFC 2578—Structure of Management Information Version 2 (SMIv2) (April 1999)	SNMP
RFC 2576—Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework (March 2000)	SNMP
RFC 2558—Definitions of Managed Objects for the SONET/SDH Interface Type (March 1999)	SNMP; cOCx/STMx and OCx/STMx interfaces
RFC 2547—BGP/MPLS VPNs (March 1999)	BGP/MPLS VPNs
RFC 2545—Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing (March 1999)	BGP
RFC 2519—A Framework for Inter-Domain Route Aggregation (February 1999)	BGP
RFC 2516—Method for Transmitting PPP over Ethernet (PPPoE) (February 1998)	PPPoE
RFC 2515—Definitions of Managed Objects for ATM Management (February 1999)	ATM; SNMP
RFC 2514—Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management (February 1999)	SNMP
RFC 2513—Managed Objects for Controlling the Collection and Storage of Accounting Information for Connection-Oriented Networks (February 1999)	SNMP
RFC 2496—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1999)	SNMP; cOCx/STMx, CT3, E3, and T3 interfaces
RFC 2495—Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types (January 1999)	SNMP; CE1, CT1, and CT3 interfaces
RFC 2493—Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals (January 1999)	SNMP
RFC 2486—The Network Access Identifier (January 1999)	Mobile IP
RFC 2475—An Architecture for Differentiated Services (December 1998)	MPLS; Policy, Management; QoS
RFC 2474—Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (December 1998)	MPLS; Policy management; QoS
RFC 2466—Management Information Base for IP Version 6: ICMPv6 Group (December 1998)	IPv6; Neighbor Discovery
RFC 2465—Management Information Base for IP Version 6: Textual Conventions and General Group (December 1998)	IPv6
RFC 2464—Transmission of IPv6 Packets over Ethernet Networks (December 1998)	IPv6; Neighbor Discovery
RFC 2463—Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification (December 1998)	IPv6
RFC 2462—IPv6 Stateless Address Autoconfiguration (December 1998)	IPv6; Neighbor Discovery
RFC 2461—Neighbor Discovery for IP Version 6 (IPv6) (December 1998)	IPv6; Neighbor Discovery
RFC 2460—Internet Protocol, Version 6 (IPv6) (December 1998)	IPv6
RFC 2459—Internet X.509 Public Key Infrastructure Certificate and CRL Profile (January 1999)	Digital certificates
RFC 2453—RIP Version 2 (November 1998)	RIP
RFC 2439—BGP Route Flap Damping (November 1998)	BGP

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 2427—Multiprotocol Interconnect over Frame Relay (September 1998)	Frame Relay
RFC 2410—The NULL Encryption Algorithm and Its Use With IPSec (November 1998)	IPSec
RFC 2409—The Internet Key Exchange (IKE) (November 1998)	IPSec
RFC 2408—Internet Security Association and Key Management Protocol (ISAKMP) (November 1998)	IPSec
RFC 2407—The Internet IP Security Domain of Interpretation for ISAKMP (November 1998)	IPSec
RFC 2406—IP Encapsulating Security Payload (ESP) (November 1998)	IPSec
RFC 2405—The ESP DES-CBC Cipher Algorithm With Explicit IV (November 1998)	IPSec
RFC 2404—The Use of HMAC-SHA-1-96 within ESP and AH (November 1998)	IPSec
RFC 2403—The Use of HMAC-MD5-96 within ESP and AH (November 1998)	IPSec
RFC 2402—IP Authentication Header (November 1998)	IPSec
RFC 2401—Security Architecture for the Internet Protocol (November 1998)	IPSec
RFC 2390—Inverse Address Resolution Protocol (September 1998)	ATM
RFC 2385—Protection of BGP Sessions via the TCP MD5 Signature Option (August 1998)	BGP
RFC 2373—IP Version 6 Addressing Architecture (July 1998)	IPv6
RFC 2370—The OSPF Opaque LSA Option (July 1998)	OSPF
RFC 2364—PPP over AAL5 (July 1998)	E3 and T3 interfaces
RFC 2362—Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (June 1998)	IP multicasting; SNMP
RFC 2338—Virtual Router Redundancy Protocol (April 1998)	VRRP
RFC 2328—OSPF Version 2 (April 1998)	OSPF
RFC 2308—Negative Caching of DNS Queries (DNS NCACHE) (March 1998)	System management
RFC 2284—PPP Extensible Authentication Protocol (EAP) (March 1998)	RADIUS
RFC 2270—Using a Dedicated AS for Sites Homed to a Single Provider (January 1998)	BGP
RFC 2246—The TLS Protocol Version 1.0 (January 1999)	PPP
RFC 2236—Internet Group Management Protocol, Version 2 (November 1997)	IP multicasting
RFC 2233—The Interfaces Group MIB using SMIv2 (November 1997)	Frame Relay
RFC 2211—Specification of the Controlled-Load Network Element Service (September 1997)	MPLS
RFC 2210—The Use of RSVP with IETF Integrated Services (September 1997)	MPLS
RFC 2209—Resource ReSerVation Protocol (RSVP) -- Version 1, Message Processing Rules (September 1997)	MPLS
RFC 2205—Resource ReSerVation Protocol (RSVP) -- Version 1, Functional Specification (September 1997)	MPLS
RFC 2153—PPP Vendor Extensions (May 1997)	PPP
RFC 2132—DHCP Options and BOOTP Vendor Extensions (March 1997)	DHCP
RFC 2131—Dynamic Host Configuration Protocol (March 1997)	DHCP
RFC 2115—Management Information Base for Frame Relay DTEs Using SMIv2 (September 1997)	Frame Relay; SNMP
RFC 2104—HMAC: Keyed-Hashing for Message Authentication (February 1997)	MPLS
RFC 2096—IP Forwarding Table MIB (January 1997)	SNMP
RFC 2030—Simple Network Time Protocol (SNTP) (Version 4) for IPv4, IPv6, and OSI (October 1996)	NTP

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 2013—SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2 (November 1996)	SNMP
RFC 2012—SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2 (November 1996)	SNMP
RFC 2011—SNMPv2 Management Information Base for the Internet Protocol using SMIv2 (November 1996)	SNMP
RFC 2006—The Definitions of Managed Objects for IP Mobility Support using SMIv2 (October 1996)	Mobile IP
RFC 2003—IP Encapsulation within IP (October 1996)	IP tunnels
RFC 1998—An Application of the BGP Community Attribute in Multi-home Routing (August 1996)	BGP
RFC 1997—BGP Communities Attribute (August 1996)	BGP
RFC 1994—PPP Challenge Handshake Authentication Protocol (CHAP) (August 1996)	MLPPP; PPP
RFC 1990—The PPP Multilink Protocol (MP) (August 1996)	MLPPP
RFC 1966—BGP Route Reflection An alternative to full mesh IBGP (June 1996)	BGP
RFC 1965—Autonomous System Confederations for BGP (June 1996)	BGP
RFC 1930—Guidelines for creation, selection, and registration of an Autonomous System (AS) (March 1996)	BGP
RFC 1901—Introduction to Community-based SNMPv2 (January 1996)	SNMP
RFC 1877—PPP Internet Protocol Control Protocol Extensions for Name Server Addresses (December 1995)	PPP
RFC 1863—A BGP/IDRP Route Server alternative to a full mesh routing (October 1995)	BGP
RFC 1850—OSPF Version 2 Management Information Base (November 1995)	OSPF
RFC 1812—Requirements for IP Version 4 Routers (June 1995)	IP
RFC 1774—BGP-4 Protocol Analysis (March 1995)	BGP
RFC 1773—Experience with the BGP-4 protocol (March 1995)	BGP
RFC 1772—Application of the Border Gateway Protocol in the Internet (March 1995)	BGP
RFC 1771—A Border Gateway Protocol 4 (BGP-4) (March 1995)	BGP
RFC 1745—BGP4/IDRP for IP—OSPF Interaction (December 1994)	BGP
RFC 1724—RIP Version 2 MIB Extension (November 1994)	RIP
RFC 1702—Generic Routing Encapsulation over IPv4 Networks (October 1994)	IP tunnels
RFC 1701—Generic Routing Encapsulation (October 1994)	IP tunnels
RFC 1700—Assigned Numbers (October 1994)	IP tunnels
RFC 1662—PPP in HDLC-like Framing (July 1994)	POS
RFC 1661—The Point-to-Point Protocol (PPP) (July 1994)	PPP; MLPPP; cOCx/STMx, channelized E1, channelized T1, channelized T3, E3, and T3 interfaces
RFC 1657—Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2 (July 1997)	BGP; SNMP
RFC 1587—The OSPF NSSA Option (March 1994)	OSPF
RFC 1493—Definitions of Managed Objects for Bridges (July 1993)	Transparent bridging

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 1490—Multiprotocol Interconnect over Frame Relay (July 1993)	Frame Relay
RFC 1483—Multiprotocol Encapsulation over ATM Adaptation Layer 5 (July 1993)	ATM; E3 and T3 interfaces
RFC 1473—The Definitions of Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol (June 1993)	SNMP
RFC 1472—The Definitions of Managed Objects for the Security Protocols of the Point-to-Point Protocol (June 1993)	SNMP
RFC 1471—The Definitions of Managed Objects for the Link Control Protocol of the Point-to-Point Protocol (June 1993)	SNMP
RFC 1407—Definitions of Managed Objects for the DS3/E3 Interface Types (January 1993)	SNMP; cOCx/STMx, channelized T3, E3, and T3 interfaces
RFC 1406—Definitions of Managed Objects for the DS1 and E1 Interface Types (January 1993)	SNMP; channelized E1, channelized T1, and channelized T3 interfaces
RFC 1350—Trivial File Transfer Protocol (TFTP) (Revision 2) (July 1992)	TFTP; System management
RFC 1332—The PPP Internet Protocol Control Protocol (IPCP) (May 1992)	PPP
RFC 1305—Network Time Protocol (version 3) Specification, Implementation and Analysis (March 1992)	NTP
RFC 1215—A Convention for Defining Traps for use with the SNMP (March 1991)	SNMP
RFC 1213—Management Information Base for Network Management of TCP/IP-based Internets: MIB-II (March 1991)	SNMP
RFC 1212—Concise MIB Definitions (March 1991)	SNMP
RFC 1195—Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (December 1990)	IS-IS
RFC 1158—Management Information Base for Network Management of TCP/IP-based internets: MIB-II (May 1990)	TCP/IP
RFC 1157—A Simple Network Management Protocol (SNMP) (May 1990)	SNMP
RFC 1155—Structure and Identification of Management Information for TCP/IP-based Internets (May 1990)	SNMP
RFC 1122—Requirements for Internet Hosts—Communication Layers (October 1989)	IP
RFC 1112—Host Extensions for IP Multicasting (August 1989)	Ethernet; IP
RFC 1094—Network File System Protocol Specification (March 1989)	NFS
RFC 1058—Routing Information Protocol (June 1998)	RIP
RFC 1057—Remote Procedure Call Protocol Specification (June 1988)	RPC
RFC 1042—A Standard for the Transmission of IP Datagrams over IEEE 802 Networks (February 1988)	Ethernet
RFC 1035—Domain Names – Implementation and Specification (November 1987)	System management
RFC 959—File Transfer Protocol (FTP) (October 1985)	FTP; System management
RFC 950—Internet Standard Subnetting Procedure (August 1985)	IP
RFC 922—Broadcasting Internet Datagrams in the Presence of Subnets (October 1984)	IP
RFC 919—Broadcasting Internet Datagrams (October 1984)	IP

Table 61: E-series RFCs (continued)

Reference	Protocol or Feature
RFC 894—A Standard for the Transmission of IP Datagrams over Ethernet Networks (April 1984)	Ethernet
RFC 854—Telnet Protocol Specification (May 1983)	IP
RFC 826—An Ethernet Address Resolution Protocol (November 1982)	Ethernet
RFC 793—Transmission Control Protocol (September 1981)	IP
RFC 792—Internet Control Message Protocol (September 1981)	IP
RFC 791—Internet Protocol DARPA Internet Program Protocol Specification (September 1981)	IP
RFC 768—User Datagram Protocol (August 1980)	IP

Draft RFCs

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

Table 62: E-series Draft RFCs

Reference	Protocol or Feature
Address Prefix Based Outbound Route Filter for BGP-4—draft-chen-bgp-prefix-orf-07.txt (March 2004 expiration)	BGP
A Policy Control Mechanism in IS-IS Using Administrative Tags—draft-ietf-isis-admin-tags-02.txt (January 2005 expiration)	IS-IS
A "traceroute" Facility for IP Multicast—draft-ietf-idmr-traceroute-ipm-07.txt (January 2001 expiration)	IP multicasting
BFD for IPv4 and IPv6 (Single Hop)—draft-ietf-bfd-v4v6-1hop-00.txt (January 2005 expiration)	BFD
BGP Extended Communities Attribute—draft-ietf-idr-bgp-ext-communities-07.txt (February 2004 expiration)	BGP
BGP/MPLS IP VPNs—draft-ietf-l3vpn-rfc2547bis-03.txt (April 2005 expiration)	BGP/MPLS VPNs
BGP-MPLS VPN extension for IPv6 VPN—draft-ietf-l3vpn-bgp-ipv6-03.txt (December 2004 expiration)	BGP/MPLS VPNs
BGP support for four-octet AS number space—draft-ietf-idr-as4bytes-08.txt (February 2004 expiration)	BGP
Bidirectional Forwarding Detection—draft-ietf-bfd-base-00.txt. (January 2005 expiration)	BFD
Connecting IPv6 Islands across IPv4 Clouds with BGP—draft-ietf-ngtrans-bgp-tunnel-04.txt (July 2002 expiration)	BGP
Cooperative Route Filtering Capability for BGP-4—draft-ietf-idr-route-filter-09.txt (February 2003 expiration)	BGP
Definitions of Managed Objects for SONET Linear APS Architectures—draft-ietf-atommib-sonetaps-mib-05.txt (November 2001 expiration)	SONET APS redundancy
Distance Vector Multicast Routing Protocol—draft-ietf-idmr-dvmrp-v3-11.txt (April 2004 expiration)	IP multicasting
Dynamic Capability for BGP-4—draft-ietf-idr-dynamic-cap-04.txt (February 2004 expiration)	BGP
Encapsulation Methods for Transport of ATM Over MPLS Networks—draft-ietf-pwe3-atm-encap-07.txt (April 2005 expiration)	Layer 2 services
Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks—draft-ietf-pwe3-ethernet-encap-05.txt (June 2004 expiration)	Layer 2 services

Table 62: E-series Draft RFCs (continued)

Reference	Protocol or Feature
Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks—draft-martini-l2circuit-encap-mpls-08.txt (March 2005 expiration)	Layer 2 services
Encapsulation Methods for Transport of PPP/HDLC Over IP and MPLS Networks—draft-ietf-pwe3-hdlc-ppp-encap-mpls-03.txt (October 2004 expiration)	Layer 2 services
Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)—draft-ietf-mpls-in-ip-or-gre-03.txt (September 2003 expiration)	MPLS
Extended Authentication within IKE (XAUTH)—draft-beaulieu-ike-xauth-02.txt (April 2002 expiration	Dynamic IPSec subscribers
Extended Authentication within ISAKMP/Oakley (XAUTH)—draft-ietf-ipsec-isakmp-xauth-06.txt (May 2000 expiration)	Dynamic IPSec subscribers
Extended Ethernet Frame Size Support—draft-ietf-isis-ext-eth-01.txt (November 2001 expiration)	IS-IS
Extensions to a Method for Transmitting PPP over Ethernet (PPPoE)—draft-carrel-info-pppoe-ext-00.txt (November 2000 expiration)	PPPoE
Fail Over extensions for L2TP "failover"—draft-ietf-l2tpext-failover-06.txt (April 2006 expiration)	L2TP
Framework for Pseudo Wire Emulation Edge-to-Edge (PWE3)—draft-ietf-pwe3-arch-06.txt (April 2004 expiration)	Layer 2 services
Graceful Restart Mechanism for BGP—draft-ietf-idr-restart-10.txt (March 2004 expiration)	BGP
GSMPv3 Base Specification—draft-ietf-gsmp-v3-base-spec-07.txt (March 2006 expiration)	L2C
GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration—draft-wadhwa-gsmp-l2control-configuration-00.txt (July 2006 expiration)	L2C
IGMP-based Multicast Forwarding ("IGMP Proxying")—draft-ietf-magma-igmp-proxy-00.txt (May 2002 expiration)	IP multicasting
IGMP/MLD-based Multicast Forwarding ('IGMP/MLD Proxying')—draft-ietf-magma-igmp-proxy-06.txt (October 2004 expiration)	IPv6 multicasting
L2TP Proxy Authenticate Extensions for EAP—draft-ietf-l2tpext-proxy-authen-ext-eap-01.txt (December 2006 expiration)	PPP
Layer 2 VPNs over Tunnels—draft-kompella-l2vpn-l2vpn-01.txt (July 2006 expiration)	L2VPNs
LDP IGP Synchronization—draft-jork-ldp-igp-sync-01.txt (August 2005 expiration)	MPLS
Management Information Base for IS-IS—draft-ietf-isis-wg-mib-16.txt (January 2005 expiration)	IS-IS; SNMP
Multicast Group Membership Discovery MIB—draft-ietf-magma-mgmd-mib-06.txt (October 2004 expiration)	IPv6 multicasting
Multicast in MPLS/BGP VPNs—draft-rosen-vpn-mcast-06.txt (April 2004 expiration)	Multicast VPNs
Multicast in MPLS/BGP IP VPNs—draft-rosen-vpn-mcast-08.txt (June 2005 expiration)	Multicast VPNs
Negotiation of NAT-Traversal in the IKE—draft-ietf-ipsec-nat-t-ike-08.txt (July 2004 expiration)	L2TP over IPSec
Point-to-point operation over LAN in link-state routing protocols—draft-ietf-isis-igp-p2p-over-lan-05.txt (January 2005 expiration)	IS-IS
Protocol Independent Multicast MIB for IPv4—draft-ietf-idmr-pim-mib-10.txt (July 2000 expiration)	IP multicasting
Pseudowire Setup and Maintenance Using LDP—draft-ietf-pwe3-control-protocol-08.txt (January 2005 expiration)	Layer 2 services
Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)—draft-ietf-pwe3-requirements-08.txt (June 2004 expiration)	Layer 2 services
Routing IPv6 with IS-IS—draft-ietf-isis-ipv6-06.txt (April 2006 expiration)	IS-IS
Source-Specific Multicast for IP—draft-ietf-ssm-arch-06.txt (March 2005 expiration)	IP multicasting

Table 62: E-series Draft RFCs (continued)

Reference	Protocol or Feature
Source-Specific Protocol Independent Multicast in 232/8—draft-ietf-mboned-ssm232-08.txt (September 2004 expiration)	IP multicasting
Subcodes for BGP Cease Notification Message—draft-ietf-idr-cease-subcode-05.txt (March 2004 expiration)	BGP
The ISAKMP Configuration Method—draft-dukes-ike-mode-cfg-02.txt (March 2002 expiration)	Dynamic IPSec subscribers
The TACACS+ Protocol, Version 1.78—draft-grant-tacacs-02.txt (January 1997 expiration)	TACACS+
Transport of Layer 2 Frames Over MPLS—draft-martini-12circuit-trans-mpls-11.txt (October 2003 expiration)	Layer 2 services
UDP Encapsulation of IPsec ESP Packets—draft-ietf-ipsec-udp-encaps-09.txt (November 2004 expiration)	L2TP over IPSec
Virtual Private LAN Service—draft-ietf-l2vpn-vpls-bgp-05.txt (October 2005 expiration)	VPLS

Other Software Standards

Table 63: E-series Non-RFC Software Standards

Reference	Protocol or Feature
ANSI T1.107a-1990 Standard for Telecommunications—Digital Hierarchy – Supplement to Formats Specification (August 1990)	MDL (T3 interfaces)
ANSI T1.403-1989 Standard for Telecommunications—Network and Customer Installation Interfaces – DS1 Metallic Interface – Robbed-bit Signaling State Definitions (1989)	FDL (T1 interfaces)
ANSI T1.404-1994 Standard for Telecommunications—Network-to-Customer – DS3 Metallic Interface Specification (1994)	Remote loopback (T3 interfaces
ANSI T1.617 Annex D	Frame Relay
AT&T Technical Reference 54016—Requirements for Interfacing Digital Terminal Equipment to Services Employing the Extended Superframe Format (September 1989)	FDL (T1 interfaces)
ATM Forum—ATM User-Network Interface Specification, Version 3.0 (September 1993)	ATM
ATM Forum—ATM User-Network Interface Specification, Version 3.1 (September 1994)	ATM
ATM Forum—Integrated Local Management Interface (ILMI) Specifications, Versions 3.0, 3.1, and 4.0 (September 1996)	ATM
ATM Forum—Traffic Management Specification, Version 4.0 (April 1996)	ATM
ATM Forum—User-Network Interface (UNI) versions 3.0, 3.1, 4.0	ATM
Draft Standard P802.1Q/D9 IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	Ethernet; VLANs; Transparent bridging
DSL Forum Technical Report (TR)-059—DSL Evolution - Architecture Requirements for the Support of QoS-Enabled IP Services	QoS; DSL
DSL Forum Technical Report (TR)-101—Migration to Ethernet-Based DSL Aggregation (April 2006)	Dynamic VLANs; PPPoE; DHCP
ERX system Cisco HDLC is compatible with Cisco Systems HDLC protocol	Cisco HDLC
Frame Relay Forum—Frame Relay Fragmentation Implementation Agreement, FRF.12 (December 1997)	Frame Relay
Frame Relay Forum—User-to-Network Implementation Agreement (UNI), FRF 1.1 (January 1996)	Frame Relay
IEEE 802.1D—Media access control (MAC) bridges	Transparent bridging

Table 63: E-series Non-RFC Software Standards (continued)

Reference	Protocol or Feature
IEEE 802.1q (Virtual LANs)	Ethernet; VLANs
IEEE 802.1w (Rapid Reconfiguration of Spanning Tree)	Ethernet
IEEE 802.1x-2001—Port-Based Network Access Control	Wireless authentication
IEEE 802.3 (Fast Ethernet and Gigabit Ethernet)	Ethernet
IEEE 802.3ad (Link Aggregation)	Link Aggregation, Layer 2 over MPLS
IEEE 802.3ae (10-Gigabit Ethernet only)	10-Gigabit Ethernet
IEEE 802.3u (Fast Ethernet only)	Ethernet
IEEE 802.3z (Gigabit Ethernet only)	Ethernet
ISO International Standard 8473-1:1993—Information technology – Protocol for providing the connectionless-mode network service	IS-IS
ISO International Standard 9542:1988 (E)—Information processing systems – Telecommunications and information exchange between systems – End System-to-Intermediate System Routing Exchange Protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)	IS-IS
ISO/IEC 10589:1992—Information technology – Telecommunications and information exchange between systems – Intermediate System-to-Intermediate System Intra-Domain Routing Exchange Protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)	IS-IS
ITU O.151—Error performance measuring equipment operating at the primary rate and above (October 1992)	BERT Patterns
ITU O.153—Basic parameters for the measurement of error performance at bit rates below the primary rate (October 1992)	BERT Patterns
ITU-T Draft Recommendation I.363 (AAL5 support) (January 1993)	ATM
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)	SDH MSP redundancy
ITU-T Q.933 Annex A	Frame Relay
ITU-T Recommendation I.610—B-ISDN Operation and Maintenance Principles and Functions (February 1999)	ATM
ITU-T Recommendation Q.922, Integrated Services Digital Network (ISDN) Data Link Layer Specification for Frame Mode Bearer Services; Annex A (February 1992)	Frame Relay
ITU-T V.35: Data transmission at 48 kbit/s using 60-108 kHz group band circuits (October 1984 - now obsolete)	V.35
ITU-T X.21: Interface between Data Terminal Equipment and Data Circuit-terminating Equipment for synchronous operation on public data networks (September 1992)	X.21
Lawfully Authorized Electronic Surveillance (LAES) for IP Network Access, American National Standard for Telecommunications, version PTSC-LAES-2006-084R6	Packet Mirroring
Multilink Frame Relay UNI/NNI Implementation Agreement, FRF.16 (April 2000)	Multilink Frame Relay
T1M1.3 Working Group—A Technical Report on Test Patterns for DS1 Circuits (November 1993)	BERT Patterns
Telcordia document GR-253—Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria, Revision 3 (September 2000)	SONET APS redundancy

Hardware Standards

Table 64: E-series Hardware Standards

Reference	Protocol or Feature
ACA TS 016-1997	Telecom
ANSI T1.102-1993 Digital Hierarchy – Electrical Interfaces (1999)	Cables
ANSI T1.646-1995 Telecommunications – Broadband ISDN—Physical Layer Specification for User-Network Interfaces Including DS1/ATM (1995)	Cables and connectors
ANSI T1.646a-1997 Telecommunications – Broadband ISDN—Physical Layer Specification for User-Network Interfaces Including DS1/ATM (1997)	Cables and connectors
AS/NZS 3260:1993, Safety of Information Technology Equipment Including Electrical Business Equipment	Safety
AS/NZS 3548:1995 (CISPR 22 Class A)	EMC
CAN/CSA C22.2, No. 60950-00, 3rd Edition, Safety of Information Technology Equipment	Safety
CTR13—Commission Decision of 9 July 1997 on a common technical regulation for attachment requirements for terminal equipment interface for connection to 2048 kbit/s digital structured ONP leased lines: 97/521/EC – OJ No. L215 Vol. 40, August 1997	Telecom
CTR24—Commission Decision of 9 September 1997 on a common technical regulation for attachment requirements for terminal equipment interface for connection to 34 Mbit/s digital unstructured and structured leased lines: 97/639/EC – OJ No. L271 Vol. 40, 3 October 1997	Telecom
EIA-310-D Cabinets, Racks, Panels, and Associated Equipment, September 1992	Mechanical
EMC Directive (89/336/EEC)	EMC
EN300 386-2:1997 EMC requirements for Telecom Network Equipment-Telco Centers	Telecom
EN55022 Class A (CISPR-22 Class A)	EMC
EN55024, Annex C for WAN Equipment Performance Criteria A, B, and C	EMC
EN60825-1, Safety of Laser Products - Part 1: Equipment Class, Requirements, and User's Guide (2001)	Safety
EN60950:2000, 3rd Edition, Safety of Information Technology Equipment	Safety
ETSI 300-386, Telecommunication Network Equipment; ElectroMagnetic Compatibility (EMC) requirements	EMC
FCC Part 15 Class A	EMC
FCC PART 68	EMC
GR-63 (LSSGR, FD-15): Network Equipment Building System (NEBS) Requirements: Physical Protection, Issue 1, October 1995	NEBS
GR-1089 (LSSGR, FD-15): Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment, Issue 2, Revision 1, February 1999	NEBS
IEC 825-1, Safety of Laser Products - Part 1	Safety
IEC 60950-1(2001-10) Ed. 1.0 Information technology equipment - Safety - Part 1: General requirements	Safety
IECS-003 Issue 3 Class A	EMC
ITUT G.703, Physical/electrical characteristics of hierarchical digital interfaces (November 2001)	Cables
Low Voltage Directive (73/23/EEC)	Safety
PD7024—Essential requirements for terminal equipment intended for connection to unstructured digital leased circuits of the public telecommunications network using a CCITT recommendation G,703 interface at a rate of 2048 kbit/s with a 75 ohm unbalanced presentation, 1994	Telecom

:

Table 64: E-series Hardware Standards (continued)

Reference	Protocol or Feature
RTTE Directive (1999/5/EEC)	Telecom
SR-3580 (FD-15): Network Equipment Building System (NEBS) Criteria Levels, Issue 1, November 1995	Safety
UL 60950, 3rd Edition, Safety of Information Technology Equipment	Safety
VCCI (Voluntary Control Council for Interference by Information Technology Equipment)	EMC

Index

Symbols

.cnf files 235, 245
.dmp files 245, 276
.hty files 245
.log files 246
.pub files 246
.rel files 246
.scr files 246
.sts files 246
.txt files 246
? command 32, 62, 64

Numerics

3des-cbc encryption algorithm for SSH 463

A

AAA (authentication, authorization, accounting)
    configuring 454
aaa commands
    aaa accounting vr-group 112
    aaa authentication enable default 455
    aaa authentication login 455
    aaa domain-map 83, 558
    aaa local database 96
    aaa local username 96
    aaa new-model 456
    aaa profile 79
AAA Profile Configuration mode 67, 79
AAL5 layer (ATM) 19
abbreviating keywords 31, 32, 65
abbreviations and acronyms 563
access and uplink methods 3
access-class in command 459
access levels (CLI) 46
access lists 24
    for Telnet sessions 458
access-list command 459, 544
adapter commands
    adapter accept 318
    adapter disable 311
    adapter enable 312
    adapter erase 319
Address Family Configuration mode 67, 79
address-family ipv4 command 79
address-family vpnv4 command 79
agent, SNMP 136, 138
algorithm negotiation, SSH 460
arrow keys 33, 65, 66
assembly numbers, displaying for hardware 338, 531
assembly revisions, displaying for hardware 338, 531
assigning an IP address 116, 122, 126
ATM interfaces 17
ATM VC Class Configuration mode 67, 80
ATM VC Configuration mode 67, 80
attributes, SNMP 143
audience for documentation xix
authentication
    AAA 454
    FTP server 263
    hmac-md5 for SSH 466
    hmac-sha1 for SSH 466
    hmac-sha1-96 for SSH 466
    new model AAA 454
    SSH user 460
authentication trap, SNMP 155
authorization
    AAA 454
Automatic Commit mode 235
automatic switchover 328
automatic synchronization
    disabling 346
    enabling 344
autoupgrade 217
avp command 94

B

backing up software configuration 124
Backspace key 33, 65
backup router 24
bandwidth
    associated error messages 326
    line modules 323
    SRP modules 323
bandwidth errors
    troubleshooting 326
bandwidth oversubscription
    configuring 325
    monitoring 326
    overview 322

bandwidth oversubscription command 325
banner command 241
banners
  configuring 241
baseline commands
  baseline show-delta-counts 288
  baseline snmp 204
BGP (Border Gateway Protocol) 23
blowfish-cbc encryption algorithm for SSH 463
boot commands
  boot backup 524
  boot config 525
  boot config factory-defaults 525
  boot config once 525
  boot config running-configuration 525
  boot config startup-configuration 525
  boot force-backup 526
  boot hotfix 358
  boot revert-tolerance 526
  boot revert-tolerance never 527
  boot subsystem 527
  boot system 527
Boot mode 350, 351
Boot mode software installation 125
Boot mode, accessing 126
booting modules 334
booting the system 119, 124, 127, 523
  rebooting 528
  while running scripts or macros 530
Border Gateway Protocol. *See* BGP
bottom-up approach to network configuration 5
B-RAS applications 4
  overview 26
B-RAS commands
  aaa accounting vr-group 112
bridge commands
  bridge subscriber-policy 109
broadcasts, NTP 536, 544
bulk statistics, SNMP
  collecting 178, 204
  configuring
    collectors and receivers 182
    schemas 197
  formatter 203
  if-stats objects 197, 198, 199
  monitoring
    collection statistics 187
    schema statistics 201
bulkstats commands
  bulkstats collector 173, 176, 183, 187
  bulkstats collector collect-mode 183
  bulkstats collector description 183
  bulkstats collector interval 183
  bulkstats collector max-size 184
  bulkstats collector primary-receiver 184
  bulkstats collector secondary-receiver 184
  bulkstats collector single-interval 184
  bulkstats file-format endOfLine-Lf 204
  bulkstats interfaces description-format
    common 185
  bulkstats interface-type 185
  bulkstats receiver remote-name 186
  bulkstats schema 199
  bulkstats schema subtree 200
  bulkstats schema subtree policy 200
  bulkstats traps 186
  bulkstats virtual-router-group 186
  See also show bulkstats commands

C

caching, configuration 530
capitalization. *See* case sensitivity
case sensitivity 65
channelized E1 interfaces
  configuring 13
channelized T1 interfaces
  configuring 13
channelized T3 interfaces
  configuring 11
  line rates 9
characters on terminal screen, setting
  bits for 238, 239
Classifier Group Configuration mode 68, 81
clear commands
  clear line 224
  clear redundancy history 399
CLI (command-line interface) 219
  abbreviating keywords 31, 32, 65
  accessing 47
  command modes. *See* command modes
  context-sensitive help 61, 222
  editing keys 65
  editing on 65
  logging in 47
  pausing 222
  system prompts 45
CLI access levels, VSA descriptions 470, 471
CLI command execution by macro file 495
CLI messages
  configuring 241
CLI status indicator 45
client, SNMP 136, 137
  configuring access 147, 148
clock 539
clock commands 539
  clock set 539
  clock summer-time date 540

clock summer-time recurring 540
clock timezone 540
.cnf files 235, 236, 245, 523
cOCx/STMx interfaces
line rates....9
coldStart, SNMP trap 155
Color Mark Profile Configuration mode 68, 81
color-mark-profile command 81
command history keys....66
command modes 28
accessing 67–112
exiting....50, 221
command-line interface. *See* CLI
command-line prompts 30
commands
abbreviating....65
editing on CLI 65
issuing from other command modes ...34, 220, 222
listing available....62
pausing before executing....222
using 32
commands for troubleshooting....275
community table, SNMP
community name....147
configuring....147
IP access list....147
privilege levels....147
community, SNMP....136, 147
configuration caching....530
configuration file....523
running....235
configuration modes. *See* command modes
configuration tasks, general 7
configuration, software 119, 124
configure command....78
configuring. *See specific feature or protocol*
confirmations explicit command 45
console
monitoring settings....243
password....450
restricting login....239
setting speed....237
console lines
clearing....224
contact person for SNMP server 149
context-sensitive help 61, 222
control flow monitoring....475
Control Plane Configuration mode....82, 84, 86
control plane security....475
controller commands....82
Controller Configuration mode 68, 82
control-plane command 82
conventions defined
icons....xx
text and syntax....xxi
copy commands
copy 258, 281, 282
copy running-configuration....235
copy running-configuration
startup-configuration 236
copy startup-configuration 236
examples 260
copying the software release file 119, 124, 127
core dump files for troubleshooting 245, 276
core dumps....282
corrupted files. *See* flash cards, scanning
crypto key dss command 461, 467
Ctrl-key combinations (CLI)
command history....66
command-line editing....65
current configuration
saving....236, 237
customer support
gathering information for....285
customer support, contacting....xxvi

D

data link-layer interfaces
configuring 15
data set ready signal. *See* DSR
data-character-bits command 238
default version....34
default virtual router....553
delete command....249
Delete key....33, 65
denial of service (DoS) 484
attaching groups....485
attacks....475
protection 473
protocol mapping....486
DHCP Pool Configuration mode....68, 83
diag command 368
diagnostics
enabling at warm restart 367
Diffie-Hellman key exchange 459
digital subscriber line access multiplexers. *See* DSLAMs
dir command....251
disable command 50, 220
disable-autosync command....346
disable-switch-on-error command....335
disconnect ssh command....469
display terminal
configuring 238
displaying configuration information. *See* show commands
distributed denial of service (DDoS) attack 475

distribution lists 25
.dmp files 245, 276
DNS (Domain Name System) 272
  configuring 272
do command 34, 220, 222
documentation set, E-series and JUNOSe xxii
  comments on xxvi
  obtaining xxv
Domain Map Configuration mode 68, 83
Domain Map Tunnel Configuration mode 68, 84
DoS protection group commands
  atm dos-protection-group 489
  bridge1483 dos-protection-group 489
  dos-protection-group 489
  ethernet dos-protection-group 489
  frame-relay dos-protection-group 489
  hdlc dos-protection-group 490
  ip dos-protection-group 490
  ipv6 dos-protection-group 490
  lag dos-protection-group 490
  ppp dos-protection-group 490
  pppoe dos-protection-group 491
  priority burst 491
  priority over-subscription-factor 491
  priority rate 491
  protocol burst 491
  protocol drop-probability 492
  protocol priority 492
  protocol rate 492
  protocol skip-priority-rate-limiter 492
  protocol weight 493
  use canned-group 493
  vlan dos-protection-group 493
Down Arrow key 33, 66
draft RFCs 586
Drop Profile Configuration mode 68, 85
drop-profile command 85
DS1 channels 11
DS3 channels 11
DSLAM aggregation 4
DSLAMs (digital subscriber line access multiplexers) 4, 16, 17, 26
DSR (data set ready), restricting login with 239
dsr-detect command 239
dump files, core 276

E

E120 and E320 routers
  managing 307
E120 routers ..... xx, xxii
E3 interfaces
  configuring 12
  line rates 9
E320 routers ..... xx, xxii
  interface specifiers 2
edge aggregation applications 2
  private line aggregation 3
  xDSL session termination 4
editing on command-line interface 65
enable commands
  enable 49, 77, 220, 470
  enable password 444
  enable privilege-level 446
  enable secret 444
enable passwords, erasing 446
encrypt passwords 445
encryption
  3des-cbc for SSH 463
  blowfish-cbc for SSH 463
  configuring SSH 463
  twofish-cbc for SSH 463
end command 221
Enter key 33, 65, 67
Enterprise SNMP MIB 138
entity, SNMP 136
environment, system 288
erase secrets command 446, 447
ERX-14xx models xx
ERX-310 router xx
ERX-7xx models xx
Esc-key combinations (CLI) 66
E-series and JUNOSe documentation set xxii
  comments on xxvi
  obtaining xxv
E-series router models xx
E-series routers
  assigning IP address to 126
  booting 119, 124, 127
  remote access. *See* B-RAS applications
  See also system
Ethernet
  Telnet on 271
Ethernet port on SRP module 365
  monitoring 366
events
  SNMP 136
exception commands
  exception dump 277
  exception gateway 277
  exception monitor 280
  exception protocol ftp 277
  exception source 278
  See also show exception commands
exclude-subsystem command 267
exec-banner command 242
exec-timeout command 240
exit command 50, 221

exiting the system 50
Explicit Path Configuration mode 68, 85

F

failover. *See* switchover
Fast Ethernet interfaces
  specifying an interface 365
file corruptions 352
file system configuration, saving current 235
files
  copying 255, 258, 282
  deleting 249
  macro 495
  managing 245
  monitoring 251
  redirecting 255
  renaming 248
  transferring 254
  types of 246
  viewing 254
flash (NVS or nonvolatile storage) cards 341
  copying 351
  device names 342
  different capacities 341
  E120 and E320 router features 342
  formatting 350
  halt command to prevent corruption 343
  installing 343
  managing 341
  monitoring 354
  primary 341
  rebooting and configuration data 341
  rebooting in response to corrupt sectors 341
  replacing 343
  scanning
    physical errors 352
    structural errors in data 352
  scanning utility 341
  secondary 341
  synchronizing 344
  synchronizing with different capacities 345
  validating and recovering file integrity 347
flash cards
  scanning 352
flash-disk commands
  flash-disk compare 348
  flash-disk duplicate 351
  flash-disk initialize 350
  flash-disk scan 353
Frame Relay interfaces 16
FTP access 117, 126
  configuring 123
FTP client 254
FTP server 254
  authentication 263
  configuring 262
  monitoring 265
ftp-server enable command 263

G

Get operation, SNMP 143
GetBulk operation, SNMP 143
GetBulk PDU type, SNMP 144
GetNext operation, SNMP 143
GetNextRequest PDU type, SNMP 144
GetRequest PDU type, SNMP 144
GetResponse PDU type, SNMP 144
Global Configuration mode 28, 69, 78
  exiting 221
group, SNMP 136

H

halt command 313, 343
hardware
  monitoring information 338, 369
  standards 590
  versions, displaying 369, 533
HDLC parameters 11
help 222
  CLI system 61
help command 61, 64, 222
high availability
  activating 389
  deactivating 390
  monitoring 391
  overview 377
history command 66
hmac-md5 authentication for SSH 466
hmac-sha1 authentication for SSH 466
hmac-sha1-96 authentication for SSH 466
host command 269
host ftp command 258
host table, modifying 258, 269
hostname command 217
hotfix activate command 359
hotfix files, monitoring 360
hotfixes 355
  activating 355
  arming 355
  backup settings and 357
  compatibility 356
  dependencies 356
  displaying 361
  hot-patchable 355
  startup 355
  synchronizing on SRP modules 357
.hty files 245

I

I/O adapters. *See* IOAs
I/O modules
  software compatibility ... 321
icons defined, notice ... xx
if constructs, macro ... 503
ILMI (integrated local management interface) ... 19
image on primary SRP module, copying ... 351
in-service software upgrade. *See* unified ISSU
installing system software ... 113, 346
  required information ... 115, 121, 125
integrated local management interface. *See* ILMI
interactive help system. *See* help
interface commands
  interface ... 80, 86, 109
  interface fastEthernet ... 365
  interface loopback ... 271
Interface Configuration mode ... 69, 86
interfaces ... 6
  configuring ... 86
  Fast Ethernet ... 365
  physical, configuring ... 82, 86
  shared interfaces ... 22
  subscriber interfaces ... 22
IOA configurations
  deleting ... 318, 319
IOAs
  disabling ... 311
  enabling ... 311
  erasing configurations ... 318, 319
  replacing ... 317
IP access list, SNMP ... 147
IP addresses
  assigning ... 116, 122, 126
  configuring ... 116
ip commands
  ip atm-vc ... 97
  ip dhcp-local pool ... 83
  ip domain-lookup ... 273
  ip domain-lookup transit-virtual-router ... 275
  ip domain-name ... 274
  ip ftp source-address ... 259
  ip ftp source-interface ... 260
  ip name-server ... 274
  ip vrf ... 112, 558
IP multicast ... 23
IP NAT Pool Configuration mode ... 69, 87, 88
ip nfs commands
  ip nfs ... 270
  ip nfs host ... 270
ip pim commands
  ip pm dr-priority ... 425
ip rate-limit-profile command ... 103
ip ssh commands
  ip ssh authentication-retries ... 465
  ip ssh crypto ... 464
  ip ssh disable-user-authentication ... 465
  ip ssh mac ... 466
  ip ssh sleep ... 465
  ip ssh timeout ... 465
IP support ... 17
  IP/ATM ... 17
  IP/Ethernet ... 22
  IP/FR ... 16
  IP/HDLC ... 21
  IP/PPP ... 20
IP tunnels ... 22
ip vrf commands
  ip vrf ... 558
IPSec (IP Security)
  AH ... 9
  ESP ... 9
IPSec CA Identity Configuration mode ... 88
ipsec commands
  ipsec ca identity ... 88
  ipsec identity ... 89
  ipsec ike-policy-rule ... 89
  ipsec key manual ... 90
  ipsec key pubkey-chain rsa ... 90
IPSec Identity Configuration mode ... 69, 89
IPSec IKE Policy Configuration mode ... 69, 89
IPSec Manual Key Configuration mode ... 70, 90
IPSec Peer Public Key Configuration mode ... 70, 90
IPSec Transport Profile Configuration mode ... 70, 91
IPSec Tunnel Profile Configuration mode ... 91
IS-IS protocol ... 23
issu commands
  issu initialize ... 434
  issu start ... 434
  issu stop ... 435
ISSU. *See* unified ISSU
issuing commands from other CLI modes ... 34, 220, 222

J

Juniper Networks E-series enterprise SNMP MIB ... 138
JUNOSe software CD ... xxiv

K

keywords ... 30, 31
  partial-keyword <Tab> ... 64

L

L2 Transport Load-Balancing-Circuit Configuration mode ... 70, 92
L2C commands
  l2c ... 94
  neighbor ... 95
L2TP (Layer 2 Tunneling Protocol) ... 26
l2tp commands
  l2tp destination profile ... 93
  l2tp rate-limit-profile ... 103
  l2tp switch-profile ... 94
L2TP Destination Profile Configuration mode ... 70, 93
L2TP Destination Profile Host Configuration mode ... 70, 93
L2TP Tunnel Switch Profile Configuration mode ... 71, 94
Layer 2 Control Configuration mode ... 71, 94
Layer 2 Control Neighbor Configuration mode ... 71, 95
Layer 2 Tunneling Protocol. *See* L2TP
layered approach to network configuration ... 5
LDP Configuration mode ... 71, 95
LEDs
  monitoring status ... 337
Left Arrow key ... 33, 65
levels of CLI access ... 469
line command ... 448, 452, 457
Line Configuration mode ... 71, 95
line module configurations
  deleting ... 319, 320
line module redundancy
  configuring ... 327, 329
  E120 and E320 routers ... 327
    IOA behavior ... 328
  ERX-7xx models and ERX-14xx models ... 327
  managing ... 330
  monitoring ... 338
line modules
  allowed combinations ... 323, 325
  bandwidth ... 323
  combinations ... 322
  disabling ... 310
  enabling ... 311
  erasing configurations ... 319, 320
  initialization sequence ... 46
  line rates ... 9
  performance rate ... 322
  replacing ... 314
  restricted combinations ... 326
  slot groups ... 322, 323, 325
  software compatibility ... 321
  switch usage ... 323
  troubleshooting ... 276
line rates ... 9
line vty command ... 95, 223
lines
  clearing ... 224
  configuring ... 222
  monitoring ... 224
  setting on terminal screen ... 238
link-up, link-down traps, SNMP ... 158
linking to an FTP server. *See* FTP access
listing configuration settings. *See* show commands
listing commands available ... 62
listing files on system ... 251
LLC layer (ATM) ... 19
LMI (local management interface) ... 17
Local IPSec Transport Profile Configuration mode ... 71, 74, 96
local management interface. *See* LMI
Local User Configuration mode ... 71, 96
location of SNMP server ... 149
log commands ... 275
  log severity ... 160
.log files ... 246
logging in to system ... 47
logging system events
  viewing logs ... 510
login banner ... 241
login commands
  login ... 238, 449, 452
  login authentication ... 457
login conditions
  configuring ... 239
long scripts, copying ... 346

M

MAC (media access control) addresses
  configuring for SSH ... 466
macro (.mac) files ... 246, 495
macro command ... 514
macros
  comments ... 496
  conditional execution ... 503
  control expressions ... 496
  environment commands ... 497
  executing ... 514
  if constructs ... 503
  invoking from another macro file ... 507, 508
  literals ... 498
  naming ... 496
  noncontrol expressions ... 496
  operators ... 498
    arithmetic ... 502
    assignment ... 500
    extraction ... 501
    increment and decrement ... 500
    logical ... 502
    miscellaneous ... 503

relational ... 502
string ... 501
resetting system while running ... 530
running ... 514
variables ... 497
while constructs ... 505
writing ... 495, 508
managed object, SNMP ... 136
Management Information Bases. *See* MIBs
Manual Commit mode ... 235
manuals, E-series and JUNOSe ... xxii
comments on ... xxvi
Map Class Configuration mode ... 71, 97
Map List Configuration mode ... 71, 97
map-class frame-relay command ... 97
map-list command ... 97
master router ... 24
master, NTP ... 538, 547
MD5 authentication
SSH ... 466
memory (hardware), displaying ... 338, 531
memory management ... 245
memory warning command ... 149
message authentication code. *See* MAC addresses
message-of-the-day (MOTD) banner ... 241, 242
MIBs (Management Information Bases) ... xxv
definition of ... 136
Juniper Networks E-series enterprise ... 138
standard SNMP ... 138
models
E120 ... xx
E320 ... xx
ERX-14xx ... xx
ERX-310 ... xx
ERX-7xx ... xx
modules
disabling ... 310
E120 and E320 routers ... 307
enabling ... 310
E-series, managing ... 306
monitoring ... 373
replacing ... 314
monitor. *See* terminal
more command ... 254
--More-- prompt ... 40, 41, 67
motd-banner command ... 242
mount command ... 344
mounting a CD on an FTP server ... 117, 124, 127
MPLS (Multiprotocol Label Switching) ... 24
mpls commands
mpls explicit-path name ... 85
mpls ldp profile ... 95
mpls rsvp profile ... 106
mpls tunnels profile ... 111
Multiprotocol Label Switching. *See* MPLS

N

names
renaming local files ... 248
system name ... 217
network configuration ... 1
layered (bottom-up) approach ... 5
routing protocols ... 23
network elements, SNMP ... 136
Network File System. *See* NFS client
network planning ... 1
access lists ... 24
BGP ... 23
COCX-F3 modules ... 12
configurable HDLC parameters ... 11
configuration overview ... 2
CT3 12-F0 modules ... 11
data link-layer interfaces ... 15
distribution lists ... 25
E3 modules ... 12
Ethernet modules ... 14
general configuration tasks ... 7
interfaces and subinterfaces ... 6
IP multicast ... 23
IP/ATM ... 17
IP/Frame Relay ... 16
IP/HDLC ... 21
IP/PPP ... 20
L2TP ... 26
layered approach ... 5
line module features ... 10
MPLS ... 24
non-PPP equal access ... 26
OSPF ... 23
physical layer interfaces ... 9
policy management
configuring ... 25
private line aggregation ... 3
RIP ... 24
route maps ... 24
routing policy ... 24
routing protocols ... 23
SONET ... 13
virtual routers ... 8
VRRP ... 24
xDSL session termination ... 4
network servers, displaying list of ... 294
Network Time Protocol. *See* NTP
new model AAA authentication ... 454
NFS client
configuring ... 269
overview
no boot hotfix all-releases command ... 359

no command....33, 34
non-PPP equal access....26
nonvolatile storage. *See* flash (NVS or nonvolatile storage) cards
notice icons defined....xx
NTP (Network Time Protocol)
  best server....538, 547
  broadcasts....536, 544
  client-server associations....535
  configuring....541
  master....538, 547
  monitoring....547
  overview....535
  peers....535
  replies....536, 543
  requests....536
  servers....536, 541, 545
  synchronization....537
  virtual routers....535, 541
NTP client
  configuring the system as....542
  system operation as....536
ntp commands
  ntp access-group....544
  ntp broadcast....545
  ntp broadcast-client....542
  ntp broadcast-delay....542
  ntp disable....543
  ntp enable....542
  ntp master....545
  ntp server....543
  ntp server enable....546
  ntp source....543
  See also show ntp commands
NTP control queries....544
NTP servers
  assigning....541
  best....537
  choosing....541
  configuring virtual routers as....545
  enabling NTP broadcasting....545
  enabling on a virtual router....546
  primary....536
  selecting....541
  system operation as....538

O

objects, tracking reachability....284
OC48/STM16 interfaces, configuring....13
OCx/STMx interfaces
  configuring....13
Open Shortest Path First. *See* OSPF
OSPF (Open Shortest Path First)....23
output filtering
  from the --More-- prompt....41
  show command....36
overload advertise-high-metric issu command....423, 425
oversubscription, bandwidth
  configuring....325
  monitoring....326
  overview....322
overview, NTP....535

P

packet mirroring
  and SNMP....137
packet size, SNMP....149
pagination keys....67
parameters....30
parent-group command....98, 99
partial releases, copying....266
password command....223, 449, 452, 457
passwords....65, 77, 441
  encryption....442
  erasing console passwords....450
  erasing enable passwords....446
  See also Privileged Exec mode
passwords and secrets
  deleting....446
passwords, enabling....444
patching the system with hotfixes....355
pausing before command execution....222
PDU (protocol data unit)....144
performance rate, line modules....9, 322
  configuring....322
physical errors in flash cards....352
physical interfaces, configuring....82, 86
physical slots
  rebooting....334
  rebooting selected....529
ping command....76, 543
platform considerations
  high availability....378
  installing JUNOSe software....115
  macros....495
  managing modules....306
  network planning....2
  passwords and security....442
  SNMP....144
  system booting....523
  system clock....538
  system management....216
  using the CLI....47
  virtual routers....555
Policy List Configuration mode....72, 98

Policy List Parent Group Configuration mode ... 68, 69, 72, 98, 99
policy management ... 25
QoS classification and marking ... 25
rate limiting ... 26
types of services ... 25, 26
polling NTP servers ... 536
POS interfaces ... 20
PPP (Point-to-Point Protocol)
protocol support ... 20
PPPoE Service Name Table Configuration mode ... 72, 99
pppoe-service-name-table command ... 99
primary flash card
initializing ... 350
reformatting ... 350
primary NTP servers ... 536
private line aggregation ... 3
privilege groups ... 50
privilege level
accessing ... 48
ambiguous commands ... 56
changing command privileges ... 50
command exceptions ... 55
defining CLI ... 48
keyword mapping ... 56
password encryption ... 442
setting
default line ... 59
multiple commands ... 57
no or default versions ... 57
SNMP ... 147
viewing information ... 60
privilege level command ... 60
Privileged Exec mode ... 72, 77, 116, 121
accessing ... 48, 49, 77, 116, 121, 220
exiting ... 50, 220
See also passwords
privileged-level access (CLI) ... 46, 48
See also Privileged Exec mode
profile commands
profile ... 100
Profile Configuration mode ... 72, 100
progress indicator (CLI) ... 45
prompts, CLI system ... 45
protocol data unit. *See* PDU
protocols
xDSL supported ... 5
proxy, SNMP ... 141, 204
.pub files ... 246
pvc command ... 80

Q

QoS (Quality of Service) ... 25
QoS commands
qos-profile command ... 100
QoS Parameter Definition Configuration mode ... 72, 100
QoS Profile Configuration mode ... 73, 100, 101
QoS Shared Shaper Control Configuration mode ... 73
qos-profile command ... 101
qos-shared-shaper-control command ... 101
Queue Profile Configuration mode ... 73, 102
queue-profile command ... 102

R

RADIUS (Remote Authentication Dial-In User Service)
authentication, restricting access ... 471
password authentication ... 460
per-user enable authentication ... 470
restricting access to commands ... 469, 472
user authentication ... 462
radius commands
radius accounting server ... 102
radius authentication server ... 102
radius dynamic-request server ... 102
RADIUS Configuration mode ... 73, 102
radius relay commands
radius relay accounting server ... 103
radius relay authentication server ... 103
RADIUS Relay Configuration mode ... 73
Rate Limit Profile Configuration mode ... 73, 103
rate limiting
per priority ... 475
per protocol ... 475
reachability
tracking ... 284
reachability, tracking ... 284
reaching an FTP server. *See* FTP access
reboot history (reboot.hty) file ... 245
reboot history, displaying ... 297
rebooting the system ... 523, 533
See also booting the system
redistribute routes ... 25
redundancy
line module. *See* line module redundancy
SRP module. *See* SRP module redundancy
redundancy commands
redundancy force-switchover ... 330, 336
redundancy lockout ... 329
redundancy revert ... 330
redundancy revertive ... 329
Redundancy Configuration mode ... 73, 104
references
draft RFCs ... 586
hardware standards ... 590

non-RFC software standards....588
RFCs....578
refusing NTP broadcasts....544
regular expressions....36, 40
metacharacters....41
specifying as literals....41
.rel files....246
specifying for reboot....527
release notes....xxiv
releasing available memory....245
reload commands
reload....278, 528
reload at....529
reload in....529
reload slot....334, 529
Remote Authentication Dial-In User Service. *See* RADIUS
remote host command....93
Remote Neighbor Configuration mode....73, 104
remote-neighbor command....104
rename command....248
renaming files....248
replies, NTP....536, 543
requests, NTP....536
reset button, software....450
resetting while running scripts or macros....530
resource commands
resource if-type....286
resource threshold....286
resources
monitoring....373
reversion
after switchover....329
revisions, displaying assembly....338, 531
RFC 1213 interface numbering....202
RFCs....578
draft....586
Right Arrow key....33, 65
RIP (Routing Information Protocol)....24
Route Map Configuration mode....73, 105
route maps....24
route-map command....105
router commands
router....105
router bgp....79
router ospf....104
router pim....104
router rip....79, 104
Router Configuration mode....74, 105
routers. *See* system
Routing Information Protocol. *See* RIP
routing policy
configuring....24
routing protocols....23
configuring....23
routing, IP
configuring other protocols....23
monitoring....561
RSVP Configuration mode....74, 106
rtr commands
rtr....106
RTR Configuration mode....74, 106
run command....34, 222

S

schedule-profile command....107
Scheduler Profile Configuration mode....74, 107
.scr files....246
screen. *See* terminal
script files....246
scripts
resetting system while running....530
secondary NTP servers....536
secrets, erasing....446
secure IP tunnels....15
Secure Shell Server protocol. *See* SSH
security
administration through SSH instead of Telnet....459
SSH issues....462
security features of SNMP....139
send command....245
sending messages to terminals....244
serial numbers, displaying for hardware....338, 531
servers, NTP....536
service commands
service....99
service ctrl-x-reboot....66, 530
service manual-commit....236
service password-encryption....443, 445
service unattended password-recovery....448
Service Manager commands
service-management service-session-profile....107
Service Session Profile Configuration mode....74, 107
service show-config format command....232
Set operation, SNMP....143
SetRequest PDU type, SNMP....144
SFMs (switch fabric modules)
accepting configurations....319
disabling....310, 368
enabling....311, 334
erasing configurations....320
overview....309
replacing....317
shared interfaces....22
show aaa commands
show aaa domain-map....560
show bandwidth oversubscription....326

show boot command 531
show bulkstats commands
show bulkstats 187
show bulkstats collector interface-type 192
show bulkstats collector interval 191
show bulkstats collector max-size 192
show bulkstats collector transfer-mode 192
show bulkstats receiver 193
show bulkstats router-group 196
show bulkstats statistics 194
show bulkstats traps 196
show command output, filtering 36
show commands 34, 36
show output filtering feature 560, 561
show policy-list 480
show redirecting output 40
show configuration commands 232
show configuration 288, 467
show configuration category 230
show configuration interface 230
show configuration virtual-router 230, 560
show dos-protection-group 493
show environment command 288, 338
show exception commands
show exception dump 278
show exception monitor 280
show fabric weights command 294
show flash command 354
show ftp-server command 265
show hardware command 338, 369, 531
show hosts command 294
show hotfix command 361
show ip commands
show ip domain-lookup command 275
show ip forwarding-table slot 561
show ip ssh 467
show ip nfs command 270
show issu command 437
show last-reset command 532
show line console 0 command 243
show line vty command 224, 453
show log commands
show log data 510
show ntp commands
show ntp associations 547
show ntp associations detail 548
show ntp status 550
show nvs command 355
show processes command 245, 295
show reboot-history command 297
show redundancy commands
show redundancy 338, 392, 397
show redundancy clients 394
show redundancy switchover-history 399
show reload command 533
show running-configuration command 234, 298
show secrets command 450
show snmp commands
show snmp 205
show snmp community 147
show snmp interfaces 153, 484
show snmp notificationLog 209
show snmp trap 210
show snmp trapstat 211
show subsystems command 268
show suspicious-control-flow-detection commands
show suspicious-control-flow-detection counts 479
show suspicious-control-flow-detection flows 480
show suspicious-control-flow-detection info 480
show suspicious-control-flow-detection protocol 482
show tech-support command 285
show terminal command 243
show timing command 219
show users command 265
show utilization command 245, 373
show version command 46, 283, 298, 340, 533
show virtual-router command 561
Simple Network Management Protocol. *See* SNMP
sleep command 222
slot commands
slot accept 319
slot disable 310
slot enable 311
slot erase 319, 320
slot groups and module arrangements 322, 323
slots. *See* physical slots
SNMP (Simple Network Management Protocol) 135
agent software 136, 138
attributes 143
bulk statistics collection 178
client software 136, 137
configuring access 147, 148
communities 136, 147
compressing interfaces 151
configuration tasks 145
enabling 146
encoding method 150
engine 142
entity 136
group 136
interface numbering 152
management features 140
managing interface sublayers 150
memory warning 149
monitoring interface tables 153
monitoring status 204, 205
multiple virtual routers 141, 204

operations 143
packet mirroring 137
packet size, setting....149
PDU....144
proxy, creating 141
RFC 1213 compatibility....152
schema
configuring....197
monitoring....201
security features....139
server....136
server parameters, setting 149
traps. *See* SNMP traps
users, configuring....148
versions 138
view 137, 140
viewing status....205
virtual routers 141
SNMP commands
agent context-name....169
bulkstats interfaces rfc 1213 202
delta-sampling....170
enable....170
event....170
frequency 171
notification id....171
resource....171
trigger 173
See also bulkstats commands; show bulkstats commands
snmp commands
snmp interfaces description-format....150
snmp trap ip link-status....157
snmp trap link-status 158
snmp-server....146
snmp-server community....147
snmp-server contact 149
snmp-server enable traps....156
snmp-server host....157, 159, 161
snmp-server interfaces compress 151
snmp-server interfaces compress-restriction....152
snmp-server interfaces rfc1213 152
snmp-server location 149
snmp-server notificationLog ageOut....160
snmp-server notificationLog entryLimit 160
snmp-server notificationLog log....161
snmp-server packetsize....149
snmp-server trap-proxy....159
snmp-server trap-source 157
snmp-server user....148
See also show snmp commands
SNMP Event Manager Configuration mode....74, 108
SNMP traps....137, 153, 210
enabling....156
software
compatibility....321
configuration....119, 124
backing up....119
saving 119
installing 113, 346
line rates....9
release file 119
updating 355
upgrading 113, 129, 130, 337
software release file....246
accessing 119, 124, 127
specifying for reboot....527
software reset button 446, 450
software standards
draft RFCs....586
non-RFC standards....588
RFCs....578
software versions, displaying 298, 533
software, installing or updating....xix
SONET (Synchronous Optical Network)
configuring 13
Space key....61, 67
speed command 237
SRP module configurations
deleting....319, 320
SRP module redundancy 331
hotfixes and 357
installing 333
managing....335
monitoring 338
validating and recovering file integrity....347
SRP modules
bandwidth 323
configuring 307
copying image 351
core dump file....281
disabling 310
enabling....311
erasing configurations 319, 320
installing a redundant module....333
overview 309
removing 313
replacing....318
reset button....331, 450
synchronizing 344
srp switch command....336
SSH (Secure Shell Server)....459
algorithm negotiation 460
client configuration 461
configuration prerequisites 462
configuring 463
connections....460
disabling 467

enabling ... 467
encryption algorithms
3des-cbc ... 463
blowfish-cbc ... 463
twofish-cbc ... 463
encryption, configuring ... 463
generating host keys ... 461
host key management ... 461
key exchange ... 460
message authentication
configuring ... 466
hmac-md5 ... 466
hmac-sha1 ... 466
hmac-sha1-96 ... 466
monitoring ... 467
performance issues ... 462
security concerns ... 462
server public key files ... 246
terminating ... 468
user authentication ... 460
configuring ... 464
user key management ... 461
standards
draft RFCs ... 586
hardware standards ... 590
non-RFC software standards ... 588
RFCs ... 578
startup configuration
saving ... 236
stateful SRP switchover. *See also* high availability
static host maps, adding ... 258, 269
static tunnels ... 22
statistics
SNMP ... 178, 204
Statistics Profile Configuration mode ... 74, 108
statistics (.sts) files ... 246
statistics-profile command ... 108
status indicator (CLI) ... 45
status LEDs, monitoring ... 337
stratum 1 servers. *See* NTP servers, primary
structural errors in flash data ... 352
.sts files ... 246
Subinterface Configuration mode ... 74, 108
subinterfaces ... 7, 108
configuring ... 108
subscriber interfaces ... 22
subscriber policy commands
subscriber-policy ... 109
Subscriber Policy Configuration mode ... 74, 109
summer time, specifying ... 540
support, requesting ... xxvi
suspicious control flow detection ... 475
display options ... 477
logs ... 477
parameters ... 476
traps ... 477
suspicious control flow monitoring ... 475
suspicious-control-flow-detection commands
baseline suspicious-control-flow-detection counts ... 477
clear suspicious-control-flow-detection ... 477
suspicious-control-flow-detection grouping-off ... 478
suspicious-control-flow-detection off ... 478
suspicious-control-flow-detection protocol backoff-time ... 478
suspicious-control-flow-detection protocol low-threshold ... 478
suspicious-control-flow-detection protocol threshold ... 479
switch fabric modules. *See* SFMs
switch usage, line modules ... 323
switchover ... 327
synchronization
NTP ... 537, 538
synchronization process ... 344, 345
synchronization reserve file ... 345
synchronize command ... 334, 336, 345, 349
system
autoupgrade feature ... 217
basic parameters ... 441
booting ... 523, 533
rebooting ... 528
command-line interface. *See* CLI
configuring automatically ... 234
environment information ... 288
exiting ... 50
FTP client ... 254
FTP server ... 254
initializing line modules ... 46
levels of access ... 469, 470
logging in ... 47
logging/troubleshooting, commands for ... 275, 300
managing ... 215
monitoring ... 288
passwords ... 441
patching with hotfixes ... 355
physical slots, rebooting ... 529
RADIUS password authentication ... 460
software reset button ... 446, 450
system configuration files ... 245
system name ... 217
TFTP client ... 254
timing ... 217
updating with hotfixes ... 355
virtual router limitations ... 554
VPN and VRF limitations ... 554
system clock
setting ... 539

system commands
privilege....54
privilege-group alias....55
privilege-group membership....55
privilege-group membership clear....55
write core....282
system configuration
saving current....236, 237
saving startup....236
system passwords. *See* passwords
system security....441
system.log file....246

T

T1 lines, controllers for....11
T3 interfaces
configuring....12
controllers for....11
line rates....9
Tab key....33, 61, 64
TACACS +
aaa authentication login....455
restricting access to commands....469
tag-group command....234
technical support, requesting....xxvi
tech-support encoded-string command....285
Telnet
access lists....458
client, using....271
configuring to listen in nondefault virtual router....271
logins....47
telnet commands
telnet....271
telnet listen....272
terminal
configuring display....238
displaying configuration....243
displaying international characters....238, 239
sending messages to....244
setting length (in lines)....238
setting width (in characters)....238
terminal commands
terminal data-character-bits....239
terminal length....238
terminal speed....238
terminal width....238
See also show terminal command
text and syntax conventions defined....xxi
text files....246
TFTP client....254
thermal protection mode....288
time limits, setting
for user input....240
for user login....240
time zone, specifying....540
timeout login response command....240
timing commands
timing disable-auto-upgrade....218
timing select....218
timing source....218
timing, system
configuring....217
monitoring....219
See also system clock
trace command....76
tracking objects....284
Traffic Class Configuration mode....75, 109
Traffic Class Group Configuration mode....75, 110
traffic-class command....109
traffic-class-group command....110
transport protocols, xDSL....5
traps command....158
traps, SNMP
categories....154
configuring....153
configuring notification logs for....159
configuring trap queues....159
operation....143
PDU type....144
recovering lost traps....161
severity levels....156
specifying an egress point for....158
statistics....211
status information....210
troubleshooting core dump files....276
tunnel commands
tunnel....84, 110
Tunnel Group Configuration mode....75, 110
Tunnel Group Tunnel Configuration mode....75, 110
Tunnel Profile Configuration mode....75, 111
Tunnel Server Configuration mode....75, 111
tunnels, IP....22
tunnel-server command....111
twofish-cbc encryption algorithm for SSH....463
.txt files....246

U

unified ISSU (in-service software upgrade)....401
AAA support....418
application support....412
application-specific behavior....418
ATM support....418
ATM port date rate....419
ILMI sessions....419
OAM CC effects....419

OAM VC integrity ... 419
VC and VP statistics ... 419
DHCP support ... 419
common component ... 419
external server ... 420
packet capture ... 420
relay and relay proxy ... 420
DoS protection support ... 420
Ethernet support ... 420
ARP entries ... 420
LAG ... 421
port data rate ... 421
VLAN statistics ... 421
FTP support ... 421
halting during initialization ... 435
halting during upgrade ... 436
initialization phase ... 405
application data on standby SRP module ... 406
line module arming ... 406
SNMP traps ... 406
IS-IS support ... 421
graceful restart ... 421
high link cost ... 422
L2TP support ... 423
layer 3 protocol traffic forwarding ... 427
monitoring ... 437
OSPF support ... 423
dead interval ... 424
graceful restart ... 424
high link cost ... 424
overview ... 401
phases
initialization ... 405
overview of ... 404
service restoration ... 411
upgrade ... 407
PIM support ... 425
platform ... 403
procedure for upgrade ... 432
references ... 404
requirements
hardware ... 430
software ... 431
traffic forwarding ... 431
verification in upgrade phase ... 409
restoring original router state ... 435
router behavior ... 402
service restoration phase ... 411
SONET/SDH support ... 426
subscriber support ... 426
logins ... 426
statistics ... 426
support, application ... 412
TACACS+ support ... 427
terms ... 403
timer settings for routing protocol timers ... 429
upgrade phase ... 407
exceptions ... 408
line module control plane ... 410
line module forwarding plane upgrade ... 411
process steps ... 407
setup ... 409
SRP module switchover ... 410
verification requirements ... 409
upgrade procedure ... 432
Universal Coordinated Time. *See* UTC
Up Arrow key ... 33, 66
updating the system software ... 113
updating the system with hotfixes ... 355
upgrading software ... 337
systems with one SRP module ... 113
systems with two SRP modules ... 129
uplink methods ... 3
user access, restricting ... 469
user authentication, configuring ... 464
See also authentication
User Exec mode ... 28, 75
See also Privileged Exec mode
user interface commands ... 219
user interface, customizing ... 237
user level access (CLI) ... 46
UTC (Universal Coordinated Time) ... 540

V

vc-class atm command ... 80
vendor-specific attributes. *See* VSAs
versions
default ... 34
displaying for hardware ... 369
displaying for hardware/software ... 533
displaying for software ... 298
SNMP ... 138
view, SNMP ... 137, 140
viewing files ... 254
See also show commands
virtual interfaces (subinterfaces) ... 7
virtual private networks. *See* VPNs
virtual router commands
ip vrf ... 558
virtual-router ... 141, 472, 559
Virtual Router Redundancy Protocol (VRRP). *See* VRRP
virtual routers ... 8, 553
configuring ... 8, 555
default virtual router ... 553
map VR to domain map ... 555, 558
monitoring ... 560
name resolvers for multiple ... 274
NTP ... 535, 541, 545, 546

restricting access 470
SNMP 141
managing 204
VPNs 553, 554
VRFs 554
VSAs 471
with routing protocols 554, 557
VPN routing and forwarding instance. *See* VRF
VPNs (virtual private networks) 555
VR Group Configuration mode 75, 112
VRF (VPN routing and forwarding instance) 554
VRF Configuration mode 75, 112
VRRP (Virtual Router Redundancy Protocol) 24
VSAs (vendor-specific attributes)
levels of CLI access 469
restricting access to virtual routers 471
vty lines
clearing 224
configuring 222
managing 222
monitoring 224
users of 265

W

waiting before command execution 222
warm restart
enabling diagnostics at 367
warmStart, SNMP trap 155
while constructs, macro 505
width of terminal screen, setting 238
write memory command 237
writing macros 495

X

xDSL
protocols 5
session termination 4