



SRC-PE Software

Monitoring and Troubleshooting Guide

Release 3.0.x

Juniper Networks, Inc.

1194 North Mathilda Avenue
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Part Number: 530-026633-01, Revision 1

This product includes the following software: Fontconfig, X FreeType library, X Render extension headers, and X Render extension library, copyright © 2001, 2003 Keith Packard.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Keith Packard not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Keith Packard makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

KEITH PACKARD DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL KEITH PACKARD BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Juniper Networks, the Juniper Networks logo, JUNOS, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOSe is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

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

SRC-PE Software Monitoring and Troubleshooting Guide
Release 3.0.x
Copyright © 2008, Juniper Networks, Inc.
All rights reserved. Printed in USA.

Writing: Linda Creed, Diane Florio, Justine Kangas, Sarah Lesway-Ball, Betty Lew, Helen Shaw, Brian Wesley Simmons
Editing: Fran Mues
Illustration: Nathaniel Woodward
Cover Design: Edmonds Design

Revision History
15 August 2008— Revision 1

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

YEAR 2000 NOTICE

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

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

Abbreviated Table of Contents

About This Guide

xvii

Part 1	Monitoring and Troubleshooting the SRC Software and C-series Controllers	
Chapter 1	Overview of Monitoring and Troubleshooting Tools	3
Part 2	Using Logging for the SRC Software and C-series Controllers	
Chapter 2	Configuring Logging for SRC Components	7
Chapter 3	Configuring Logging for SRC Components with the CLI	11
Chapter 4	Configuring Logging for SRC Components (C-Web Interface)	17
Part 3	Using Simulated Router Drivers and Simulated Subscribers for Testing	
Chapter 5	Configuring a Simulated Router Driver for Testing (SRC CLI)	23
Chapter 6	Configuring a Simulated Router Driver for Testing (C-Web Interface)	27
Chapter 7	Using Simulated Subscribers for Testing (SRC CLI)	29
Part 4	Using SNMP for Monitoring and Troubleshooting	
Chapter 8	Creating Custom SNMP Monitors	39
Chapter 9	Configuring the SNMP Traps (SRC CLI)	49
Chapter 10	Understanding Traps	55
Part 5	Monitoring the SRC Software and the C-series Controller with the C-Web Interface and the SRC CLI	
Chapter 11	Monitoring the SRC CLI and the C-Web Interface	73
Chapter 12	Monitoring the System (SRC CLI)	77
Chapter 13	Monitoring the System (C-Web Interface)	81
Chapter 14	Monitoring SAE Data (SRC CLI)	89
Chapter 15	Monitoring SAE Data (C-Web Interface)	109
Chapter 16	Monitoring and Troubleshooting NIC (SRC CLI)	133
Chapter 17	Monitoring the NIC (C-Web Interface)	143
Chapter 18	Monitoring NTP (SRC CLI)	149
Chapter 19	Monitoring NTP (C-Web Interface)	151

Chapter 20	Monitoring Redirect Server (SRC CLI)	155
Chapter 21	Monitoring the Redirect Server and Filtered Traffic (C-Web Interface)	157
Chapter 22	Troubleshooting Network Connectivity (SRC CLI)	159
Chapter 23	Monitoring Network Connectivity (C-Web Interface)	163

Part 6

Index

Index	167
-------	-----

Table of Contents

	About This Guide	xvii
	SRC Guides and Release Notes	xvii
	Audience	xvii
	Documentation Conventions	xvii
	Related Juniper Networks Documentation	xix
	Obtaining Documentation	xxi
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
Part 1	Monitoring and Troubleshooting the SRC Software and C-series Controllers	
Chapter 1	Overview of Monitoring and Troubleshooting Tools	3
	Overview of Monitoring and Troubleshooting Tools	3
Part 2	Using Logging for the SRC Software and C-series Controllers	
Chapter 2	Configuring Logging for SRC Components	7
	Overview of Logging for SRC Components	7
	Categories and Severity Levels for Event Messages	7
	Defining Categories	8
	Defining Severity Levels	8
	Defining Filters	9
	Rotation of Log Files	10
Chapter 3	Configuring Logging for SRC Components with the CLI	11
	Configuration Statements for Component Logging	11
	Configuring a Component to Store Log Messages in a File with SRC CLI	12
	Configuring System Logging with SRC CLI	13

Chapter 4	Configuring Logging for SRC Components (C-Web Interface)	17
	Before You Configure Logging	17
	Configuring ACP to Store Log Messages in a File (C-Web Interface)	17
	Configuring the SAE to Store Log Messages in a File (C-Web Interface)	18
	Configuring NIC to Store Log Messages in a File (C-Web Interface)	18
	Configuring the SNMP to Store Log Messages in a File (C-Web Interface)	18
	Configuring JPS to Store Log Messages in a File (C-Web Interface)	19
 Part 3	 Using Simulated Router Drivers and Simulated Subscribers for Testing	
 Chapter 5	 Configuring a Simulated Router Driver for Testing (SRC CLI)	 23
	Overview of Simulated Router Drivers for the SRC Software	23
	Configuring Simulated Router Drivers (SRC CLI)	23
 Chapter 6	 Configuring a Simulated Router Driver for Testing (C-Web Interface)	 27
	Configuring a Simulated Router Driver for Testing (C-Web Interface)	27
 Chapter 7	 Using Simulated Subscribers for Testing (SRC CLI)	 29
	Overview of Simulated Subscribers	29
	Commands to Manage Simulated Subscribers	29
	Logging In Simulated Subscribers with the CLI	30
	Logging In Authenticated DHCP Subscribers	30
	Logging In Authenticated Interface Subscribers	31
	Logging In Unauthenticated DHCP Subscribers	31
	Logging In Unauthenticated Interface Subscribers	32
	Viewing Subscriber Sessions	33
	Logging Out Simulated Subscribers with the CLI	33
	Logging Out Subscribers by DN	33
	Logging Out Subscribers by IP Address	34
	Logging Out Subscribers by Login Name	34
	Logging Out Subscribers by Session ID	34

Part 4**Using SNMP for Monitoring and Troubleshooting****Chapter 8****Creating Custom SNMP Monitors 39**

SNMP Monitoring on C-series Controllers	39
Configuration Statements for Customized SRC SNMP Monitors	41
Configuring an SNMP Alarm on a C-series Controller (SRC CLI)	42
Defining an Alarm for an SNMP Monitor That Compares Object Values (SRC CLI)	43
Defining an Alarm to Monitor the Status of an Object (SRC CLI)	44
Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds (SRC CLI)	44
Defining a Discontinuity Check to Validate Delta Values (SRC CLI)	45
Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI)	46
Defining Events for Which SNMP Sends Notifications (SRC CLI)	46
Defining Events That Set Values for SNMP MIB Objects (SRC CLI)	47
Example: SNMP Monitoring of Multiple MIB Objects	47

Chapter 9**Configuring the SNMP Traps (SRC CLI) 49**

Overview of SNMP Traps	49
MIBs	49
Configuration MIBs	50
MIB Structure	50
MIB Location	50
Traps	50
SNMP Traps and Informs	51
Configuration Statements for the SNMP Traps	51
Configuring Performance Traps	52
Configuring Event Traps	53

Chapter 10**Understanding Traps 55**

Performance Traps	55
R/AV	56
Trap Numbers in Performance Traps	56
Decoding Trap Numbers for Raised Trap Actions	57
Decoding Trap Numbers for Clear Trap Actions	57
SRC Performance Traps	57
SAE Performance Traps	58
Accounting Performance Traps	59
Authentication Performance Traps	61
NIC Performance Traps	62
Router Driver Performance Traps	63
System Management Performance Traps	64
Policy Engine Performance Traps	65
SRC Redirector Performance Traps	65
SRC-ACP Performance Traps	65

JPS Performance Traps	66
Chassis Performance Traps	66
Event Traps	67
Alarm State Transitions	69

Part 5 Monitoring the SRC Software and the C-series Controller with the C-Web Interface and the SRC CLI

Chapter 11 Monitoring the SRC CLI and the C-Web Interface 73

Monitoring with the SRC CLI and the C-Web Interface	73
SRC Monitoring Options	73

Chapter 12 Monitoring the System (SRC CLI) 77

Viewing Information About a C-series Controller	77
Viewing Information About Components Installed (SRC CLI)	78
Viewing Information About Boot Messages (SRC CLI)	78
Viewing Information About Security Certificates (SRC CLI)	80

Chapter 13 Monitoring the System (C-Web Interface) 81

Viewing Information About the System (C-Web Interface)	81
Viewing the System Date and Time (C-Web Interface)	82
Viewing Information About Components Installed (C-Web Interface)	83
Viewing Information About Boot Messages (C-Web Interface)	83
Viewing Information About Security Certificates (C-Web Interface)	84
Viewing Information About System Disk Status	85
Viewing Information About the Users on the System	85
Viewing Information About the Juniper Networks Database in Community Mode	86
Viewing Statistics for the Juniper Networks Database	87
Viewing Information About the SRC CLI (C-Web Interface)	87
Viewing Information About the SRC CLI	87
Viewing Information About SRC CLI User Permissions	88

Chapter 14 Monitoring SAE Data (SRC CLI) 89

Viewing SAE Data with the CLI	89
Viewing Information About the Directory Blacklist with the CLI	89
Viewing Information About SAE Device Drivers with the CLI	89
Viewing Information About SAE Interfaces with the CLI	91
Viewing Information About SAE Licenses with the CLI	91
Viewing Information About Policies on the SAE with the CLI	92
Viewing Login Registrations with the CLI	93
Viewing Equipment Registrations with the CLI	93

Viewing Information About Services with the CLI	94
Viewing Information About Threads with the CLI	96
Viewing Information About Subscriber Sessions with the CLI	97
Viewing General Information for Subscriber Sessions	97
Viewing Information About Subscriber Sessions by DN with the CLI	98
Viewing Information About Subscriber Sessions by IP Address with the CLI	98
Viewing Information About Subscriber Sessions by Login Name with the CLI	99
Viewing Information About Subscriber Sessions by Service Name with the CLI	100
Viewing Information About Subscriber Sessions by Session ID with the CLI	100
Viewing SAE SNMP Information with the CLI	101
Viewing Statistics About the Directory with the CLI	102
Viewing Statistics for Directory Connections with the CLI	102
Viewing SNMP Information for Client Licenses with the CLI	103
Viewing SNMP Information for Local Licenses with the CLI	103
Viewing SNMP Information for Licenses on Virtual Routers with the CLI	104
Viewing SNMP Information for Policies with the CLI	104
Viewing SNMP Information for the SAE Server Process with the CLI	104
Viewing Statistics for RADIUS Clients with the CLI	105
Viewing SNMP Information for RADIUS Clients with the CLI	105
Viewing SNMP Information for Routers and Devices with the CLI	105
Viewing Statistics for Device Drivers with the CLI	106
Viewing Statistics for Specific Device Drivers with the CLI	107
Viewing Statistics for Subscriber and Service Sessions with the CLI	107

Chapter 15

Monitoring SAE Data (C-Web Interface) 109

Viewing SAE Data (C-Web Interface)	109
Viewing Information About the Directory Blacklist	109
Viewing Information About Services	110
Viewing Information About Licenses	111
Viewing Information About Policies	111
Viewing Information About Device Drivers	112
Viewing Information About Interfaces	113
Viewing Equipment Registrations	114
Viewing Login Registrations	115
Viewing Information About Threads	116
Viewing Information About Subscriber Sessions (C-Web Interface)	117
Viewing Information About Subscriber Sessions by DN	117
Viewing Information About Subscribers by IP Address	118
Viewing Information About Subscriber Sessions by Login Name	119
Viewing Information About Subscriber Sessions by Service Name	120
Viewing Information About Subscriber Sessions by Session ID	121
Viewing SNMP Information (C-Web Interface)	122
Viewing SNMP Statistics for the Directory	123
Viewing SNMP Statistics for Directory Connections	123

Viewing SNMP Statistics for Client Licenses	124
Viewing SNMP Statistics for Licenses by Device	125
Viewing SNMP Statistics for Local Licenses	126
Viewing SNMP Statistics About Policies	127
Viewing SNMP Statistics About Server Processes	128
Viewing SNMP Statistics About RADIUS	128
Viewing SNMP Statistics About RADIUS Clients	129
Viewing SNMP Statistics for Devices	130
Viewing SNMP Statistics for Specific Devices	131
Viewing SNMP Statistics for Subscriber Sessions and Service Sessions	131

Chapter 16 Monitoring and Troubleshooting NIC (SRC CLI) 133

SRC CLI Commands to View Statistics About NIC Operations	133
Viewing Statistics for the NIC Process	134
Viewing Statistics for a NIC Host	134
Viewing Statistics for NIC Resolvers	135
Viewing Statistics for NIC Agents	136
SRC CLI Commands to View NIC Resolution Data	137
Viewing Data for NIC Resolvers	137
Viewing Data for NIC Agents	138
Troubleshooting NIC Data Resolution	140

Chapter 17 Monitoring the NIC (C-Web Interface) 143

Viewing Hosts (C-Web Interface)	143
Viewing Host Statistics	143
Viewing Host Process Statistics	144
Viewing Resolvers (C-Web Interface)	144
Viewing Resolvers	144
Viewing Resolver Statistics	145
Viewing Agents (C-Web Interface)	146
Viewing Agents	146
Viewing Agent Statistics	147

Chapter 18 Monitoring NTP (SRC CLI) 149

Viewing NTP Peers (SRC CLI)	149
Viewing Statistics for NTP (SRC CLI)	149
Viewing Internal Variables for NTP (SRC CLI)	150

Chapter 19 Monitoring NTP (C-Web Interface) 151

Viewing NTP Peers (C-Web Interface)	151
Viewing Statistics for NTP (C-Web Interface)	151
Viewing NTP Status (C-Web Interface)	152

Chapter 20	Monitoring Redirect Server (SRC CLI)	155
	Viewing Statistics for the Redirect Server (SRC CLI)	155
	Viewing Statistics for Filtered Traffic	155
Chapter 21	Monitoring the Redirect Server and Filtered Traffic (C-Web Interface)	157
	Viewing Statistics for the Redirect Server (C-Web Interface)	157
	Viewing Information About Filtered Traffic (C-Web Interface)	158
Chapter 22	Troubleshooting Network Connectivity (SRC CLI)	159
	Overview of Commands to Troubleshoot Connections to Remote Hosts	159
	Testing Connectivity to Remote Hosts	159
	Viewing the Route Information	160
	Viewing Routing Table Information	160
	Viewing Interface Information	161
Chapter 23	Monitoring Network Connectivity (C-Web Interface)	163
	Viewing Information About the Routing Table (C-Web Interface)	163
	Viewing Information About System Interfaces (C-Web Interface)	164
Part 6	Index	
	Index	167

List of Tables

Table 1: Notice Icons	xviii
Table 2: Text Conventions	xviii
Table 3: Juniper Networks C-series and SRC Technical Publications	xix
Table 4: Named Severity Levels	8
Table 5: Examples of Filters for Event Messages	10
Table 6: Example Table for junisaeRouterTable Object	48
Table 7: Symbols in Performance Traps Tables	55
Table 8: Performance Traps–SAE	58
Table 9: Performance Traps–Accounting	59
Table 10: Performance Traps–Authentication	61
Table 11: Performance Traps–NIC	63
Table 12: Performance Traps–Router Drivers	63
Table 13: Performance Traps–System Management Event	64
Table 14: Performance Traps–Policy Engine	65
Table 15: Performance Traps–SRC Redirector	65
Table 16: Performance Traps–SRC-ACP	66
Table 17: Performance Traps–JPS	66
Table 18: Performance Traps–Chassis	67
Table 19: Event Traps	67
Table 20: Alarm State Transitions	69
Table 21: Comparison of SRC Monitoring Options	74
Table 22: Output Fields for show component	78
Table 23: Commands to Display NIC Statistics	133
Table 24: Output Fields for show nic statistics process	134
Table 25: Output Fields for show nic statistics test	135
Table 26: Output Fields for show nic statistics resolver	136
Table 27: Output Fields for show nic statistics agent	137
Table 28: Commands to Display NIC DataTable 23: Commands to Display NIC Data	137
Table 29: Output Fields for show nic data resolver	138
Table 30: Output Fields for show nic data agent	139
Table 31: Output Fields for show ntp associations command	149

About This Guide

- SRC Guides and Release Notes on page xvii
- Audience on page xvii
- Documentation Conventions on page xvii
- Related Juniper Networks Documentation on page xix
- Obtaining Documentation on page xxi
- Documentation Feedback on page xxi
- Requesting Technical Support on page xxi

SRC Guides and Release Notes

If the information in the latest *SRC Release Notes* differs from the information in the SRC guides, follow the *SRC Release Notes*.

Audience

This guide is intended for experienced system and network specialists working with JUNOS routers and JUNOS routing platforms in an Internet access environment. We assume that readers know how to use the routing platforms, directories, and RADIUS servers that they will deploy in their SRC networks.

If you are using the SRC software in a cable network environment, we assume that you are familiar with the PacketCable Multimedia Specification (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs) and with the Data-over-Cable Service Interface Specifications (DOCSIS) 1.1 protocol. We also assume that you are familiar with operating a multiple service operator (MSO) multimedia-managed IP network.

Documentation Conventions

Table 1 on page xviii defines the notice icons used in this guide. Table 2 on page xviii defines text conventions used throughout this documentation.

Table 1: Notice Icons





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

Table 2: Text Conventions

Convention	Description	Examples
Bold text like this	<ul style="list-style-type: none"> ■ Represents keywords, scripts, and tools in text. ■ Represents a GUI element that the user selects, clicks, checks, or clears. 	<ul style="list-style-type: none"> ■ Specify the keyword exp-msg. ■ Run the install.sh script. ■ Use the pkgadd tool. ■ To cancel the configuration, click Cancel.
Bold text like this	Represents text that the user must type.	<code>user@host# set cache-entry-age cache-entry-age</code>
Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	<pre>nic-locators { login { resolution { resolver-name /realms/ login/A1; key-type LoginName; value-type SaeId; } } }</pre>
Regular sans serif typeface	<ul style="list-style-type: none"> ■ Represents configuration statements. ■ Indicates SRC CLI commands and options in text. ■ Represents examples in procedures. ■ Represents URLs. 	<ul style="list-style-type: none"> ■ <code>system ldap server{ stand-alone;</code> ■ Use the <code>request sae modify device failover</code> command with the <code>force</code> option ■ <code>user@host# . . .</code> ■ <code>http://www.juniper.net/techpubs/software/ management/src/api-index.html</code>
<i>Italic sans serif typeface</i>	Represents variables in SRC CLI commands.	<code>user@host# set local-address local-address</code>
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <code>< gfwif > .</code>
Key name	Indicates the name of a key on the keyboard.	Press Enter.

Table 2: Text Conventions (continued)

Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<i>Italic typeface</i>	<ul style="list-style-type: none"> ■ Emphasizes words. ■ Identifies book names. ■ Identifies distinguished names. ■ Identifies files, directories, and paths in text but not in command examples. 	<ul style="list-style-type: none"> ■ There are two levels of access: <i>user</i> and <i>privileged</i>. ■ <i>SRC-PE Getting Started Guide</i> ■ <i>o = Users, o = UMC</i> ■ The <i>/etc/default.properties</i> file.
Backslash	At the end of a line, indicates that the text wraps to the next line.	Plugin.radiusAcct-1.class = \net.juniper.srmt.sae.plugin\RadiusTrackingPluginEvent
Words separated by the symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic line

Related Juniper Networks Documentation

With each SRC software release, we provide the *SRC Documentation CD*, which contains the documentation described in Table 3 on page xix.

A complete list of abbreviations used in this document set, along with their spelled-out terms, is provided in the *SRC —PE Getting Started Guide*.

Table 3: Juniper Networks C-series and SRC Technical Publications

Document	Description
Core Documentation Set	
<i>C2000 and C4000 Hardware Guide</i>	Describes the hardware platforms and how to install, maintain, replace, and troubleshoot them. The guide also includes specifications.
<i>C2000 and C4000 Quick Start Guide</i>	Describes how to get the C-series Controller up and running quickly. Intended for experienced installers who want to expedite the installation process.
<i>SRC-PE Getting Started Guide</i>	Describes the SRC software, how to set up an initial software configuration, how to integrate RADIUS servers, and how to upgrade the SRC software. It also explains how to manage a C-series Controller. The guide describes how to set up and start the SRC CLI and the C-Web interface, as well as other SRC configuration tools. It includes reference material for the SRC documentation.
<i>SRC-PE CLI User Guide</i>	Describes how to use the SRC CLI, configure and monitor the platform with the CLI, and control the CLI environment. The guide also describes how to manage SRC components with the CLI.

Table 3: Juniper Networks C-series and SRC Technical Publications *(continued)*

Document	Description
<i>SRC-PE Network Guide: SAE, Juniper Networks Routers, NIC, and SRC-ACP</i>	Describes how to use and configure the SAE, the NIC, and the SRC-ACP (Admission Control Plug-In) application. This guide also provides detailed information about using JUNOSe routers, JUNOS routing platforms, and other network devices in the SRC network.
<i>SRC-PE Services and Policies Guide</i>	Describes how to work with services and policies. The guide provides an overview, configuration procedures, and management information. The guide also provides information about the SRC tools for configuring policies.
<i>SRC-PE Subscribers and Subscriptions Guide</i>	Describes how to work with residential and enterprise subscribers and subscriptions. The guide provides an overview, configuration procedures, and management information. This guide also provides information about the enterprise service portals, including the Enterprise Manager Portal.
<i>SRC-PE Monitoring and Troubleshooting Guide</i>	Describes how to use logging, the SNMP agent, the SRC CLI, and the C-Web interface to monitor and troubleshoot SRC components. This guide also describes the SNMP traps.
<i>SRC-PE Solutions Guide</i>	Provides high-level instructions for SRC implementations. The guide documents the following scenarios: managing QoS services on JUNOSe routers; managing subscribers in a wireless roaming environment; providing voice over IP (VoIP) services; integrating the SRC software in a PCMM environment, including the use of the Juniper Policy Server (JPS); and mirroring subscriber traffic on JUNOSe routers.
<i>SRC-PE CLI Command Reference, Volume 1</i> <i>SRC-PE CLI Command Reference, Volume 2</i>	Together constitute information about command and statement syntax; descriptions of commands, configuration statements, and options; editing level of statement options; and a history of when a command was added to the documentation.
<i>SRC-PE NETCONF API Guide</i>	Describes how to use the NETCONF application programming interface (API) to configure or request information from the NETCONF server on a C-series Controller that runs the SRC software.
<i>SRC-PE XML API Configuration Reference</i>	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to configuration statements in the SRC command-line interface (SRC CLI).
<i>SRC-PE XML API Operational Reference</i>	Describes the tag elements in the SRC Extensible Markup Language (XML) application programming interface (API) that are equivalent to operational commands in the SRC command-line interface (SRC CLI).
Application Library	
<i>SRC Application Library Guide</i>	Describes how to install and work with applications that you can use to extend the capabilities of the SRC software. The guide documents the following applications: SRC-SG (SOAP Gateway) Web applications, an application to provide threat mitigation, an application to provide tracking and QoS control at the application level by integrating the SRC software with the Ellacoya deep packet inspection (DPI) platform, and an application to control volume usage .
Release Notes	

Table 3: Juniper Networks C-series and SRC Technical Publications *(continued)*

Document	Description
<i>SRC-PE Release Notes</i>	In the <i>Release Notes</i> , you will find the latest information about features, changes, known problems, resolved problems, supported platforms and network devices (such as Juniper Networks routers and CMTS devices), and third-party software. If the information in the <i>Release Notes</i> differs from the information found in the documentation set, follow the <i>Release Notes</i> .
<i>SRC Application Library Release Notes</i>	
Release notes are available on the Web.	

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 guide, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the documentation 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. You can 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 (not required for *Network Operations Guides [NOGs]*)

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).

Part 1

Monitoring and Troubleshooting the SRC Software and C-series Controllers

- Overview of Monitoring and Troubleshooting Tools on page 3

Chapter 1

Overview of Monitoring and Troubleshooting Tools

- Overview of Monitoring and Troubleshooting Tools on page 3

Overview of Monitoring and Troubleshooting Tools

The SRC software provides the following tools to help you monitor and troubleshoot your SRC environment:

- Logging support for SRC components
- System log server on C-series controllers
- NIC test commands to troubleshoot NIC configuration
- Router simulation to facilitate application testing
- Subscriber simulation to facilitate application testing
- SNMP agent to monitor SRC components as well as system performance. The agent can send data to SNMP network management systems.
- SNMP trap notification to SNMP management systems
- SRC CLI to monitor specified SRC components and C-series controllers
- C-Web interface to monitor specified SRC components and C-series controllers

In addition, the SRC Volume Tracking Application (SRC-VTA) in the SRC application library includes a Web-based application to test events.

The SRC software also includes various sample and test clients for the dynamic service activator, the SAE remote interface, and the SAE plug-in interface.

Related Topics

- Overview of Logging for SRC Components
- Monitoring with the SRC CLI and the C-Web Interface
- SRC Monitoring Options
- Overview of SNMP Traps

Part 2

Using Logging for the SRC Software and C-series Controllers

- Configuring Logging for SRC Components on page 7
- Configuring Logging for SRC Components with the CLI on page 11
- Configuring Logging for SRC Components (C-Web Interface) on page 17

Chapter 2

Configuring Logging for SRC Components

- Overview of Logging for SRC Components on page 7
- Categories and Severity Levels for Event Messages on page 7
- Rotation of Log Files on page 10

Overview of Logging for SRC Components

SRC components and applications generate event messages that you can save in logs—either by writing the messages to text files or by using the system log (syslog) facilities. You can use these logs to monitor the SRC components and troubleshoot problems.

Each SRC component has its own logging configuration. For example, the license server, the NIC, the SAE, and SNMP each have logging configuration. The C-series Controller includes a system log server that you can configure to manage messages generated on that platform. You can use the CLI and the C-Web interface to configure logging on a C-series Controller and to configure the system log server on a C-series Controller.

When you enable logging to a file, by default SRC components and applications write log files in the `/opt/UMC/<component-directory>/var/log` folder for a component, such as `/opt/UMC/sae/var/log`.

All log files with the file extension `.log` in a `var/log` directory are rotated daily. When a new log file is created, the previous day's file is compressed and saved.

Related Topics For additional information, see the following sources:

- Overview of the C-series Controller Log Server
- The syslog Protocol—draft-ietf-syslog-protocol-16.txt (July 2006 expiration)
- Configuring the SDX SNMP Agent

Categories and Severity Levels for Event Messages

In the logging configuration, you can specify a filter for each type of log. This filter can include an expression that defines the *categories* and *severity levels* of event messages that the software saves.

Defining Categories

The category of an event message defines the SRC component that generated the event message. If you want to view only event logs in a specific category, you can define a variable `<category>`, which is a text string that matches the name of a category. This variable is not case sensitive. To view the names of categories for event messages, view a log file for one of the default filters.

For example, the category `Cops` defines event messages generated by the COPS server. Similarly, the category `CopsMsg` defines a particular sort of event message that the COPS server generates.

Juniper Networks Customer Service can also provide names of categories, especially for troubleshooting purposes.

Defining Severity Levels

The event filter provides 128 levels of severity numbered 1–127. A higher number indicates a higher level of severity. Common levels of severity also have a specific name, as shown in Table 4 on page 8.



CAUTION: Enabling the generation of debug log messages has a negative affect on system performance. Do not enable debug log messages unless you are instructed to do so by Juniper Networks Technical Assistance Center (JTAC).

Table 4: Named Severity Levels

Name	Severity Level
logmin	1
debug	10
info	20
notice	30
warning	40
error	50
crit	60
alert	70
emerg	80
panic	90
logmax	127

You can define a severity level as follows:

- Specify an explicit severity. For example:
 - debug—Defines only debug messages
- Specify a minimum severity and a maximum severity. For example:
 - info-warning—Defines messages of minimum severity level of info and a maximum severity level of warning
 - Accept the default minimum (logmin) or maximum (logmax) severity by omitting the minimum or maximum severity. For example:
 - info—Defines messages of minimum severity level info and maximum severity level logmax
 - -warning—Defines messages of minimum severity level logmin and maximum severity level warning
- Specify no severities to log all event messages.

The syntax for the severity takes the format:

[< severity >] | [< minimumSeverity >]-[< maximumSeverity >]

Use either the name or the number of a severity level shown in Table 4 on page 8 for the variables in this syntax.

Defining Filters

You specify a filter by defining an expression with the following format:

singlematch [,singlematch]*

- singlematch—[!] (< category > | ([< category >]/[< severity >] | [< minimumSeverity >]-[< maximumSeverity >]))
- !—Do not log matching events
- < category > —See “Defining Categories” on page 8
- [< severity >] | [< minimumSeverity >]-[< maximumSeverity >]—See “Defining Severity Levels” on page 8 .

The software filters events by evaluating each subexpression in order from left to right. When the software determines that an event message matches a subexpression, the software logs or ignores the message accordingly. You can specify an unlimited number of subexpressions; however, the order in which you specify the subexpressions affects the result.

Table 5 on page 10 shows some examples of filters.

Table 5: Examples of Filters for Event Messages

Syntax	Event Messages Saved
/	All event messages
/info-	Event messages of level info and above from all categories
Cops/debug	Debug events from COPS category only
!Cops,/debug	All debug events except those from COPS category
CopsMsg/info-,!CopsMsg,Cops	All messages from COPS category, except those from CopsMsg category with level less than info

Rotation of Log Files

On C-series Controllers, log files that contain entries are rotated daily when other daily system tasks run on the system. The system retains 5 log files for a component before overwriting the oldest file.

When a new log file is opened to replace a file from the previous day that contains content, a number (1–4) is appended to the name of the older file. For example, *sae_debug.log.4* would be the oldest file in the rotation, *sae_debug.log.1* would be the newest file in the rotation; *sae_debug.log* would be the active log file for SAE.

On C-series Controllers, the software compresses log files and appends the *.gz* suffix; for example, *sae_debug.log.4.gz*. Log files are stored in the */opt/UMC/component-name/var/log* directory; for example, */opt/UMC/sae/var/log*.



NOTE: On a C-series Controller, log files are automatically rotated on a daily basis. Typically, you do not specify a maximum file size when log files are rotated. Consider whether specifying a rollover filename is needed for SRC software running on a C-series controller. If you do configure a rollover file when files are rotated, the software creates five compressed versions of partial log files, and one uncompressed log file.

You can configure components to send log messages to the system log server (also called a syslog server) on the platform on which the SRC software is running.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component.

Chapter 3

Configuring Logging for SRC Components with the CLI

- Configuration Statements for Component Logging on page 11
- Configuring a Component to Store Log Messages in a File with SRC CLI on page 12
- Configuring System Logging with SRC CLI on page 13

Configuration Statements for Component Logging

Use the following configuration statements to configure logging for SRC components. You access these statements from the hierarchy for a component, such as:

- [edit shared acp configuration]
- [edit shared sae configuration]
- [edit shared nic scenario *scenario-name*]
- [edit snmp agent]
- [edit slot 0 jps]

```
logger name {
  file-logger {
    filter filter ;
    filename filename ;
    rollover-filename rollover-filename ;
    maximum-file-size maximum-file-size ;
  }
  syslog-logger {
    filter filter ;
    syslog-host syslog-host ;
    syslog-facility syslog-facility ;
    format format ;
  }
}
```

- Related Topics** ■ For detailed information about each configuration statement, see *SRC-PE CLI Command Reference*.

Configuring a Component to Store Log Messages in a File with SRC CLI

Use the following statements to configure an SRC component to store log messages in a file:

```
logger name file {
    filter filter;
    filename filename;
    rollover-filename rollover-filename;
    maximum-file-size maximum-file-size;
}
```

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See *Categories and Severity Levels for Event Messages*.

To configure component logging to a file:

1. From configuration mode, access the configuration statement that configures the logging destination for the component.

```
[edit]
user@host# component-hierarchy logger name file
```

For example:

```
[edit]
user@host# edit shared sae configuration logger sae-file-log-1 file
```

```
[edit]
user@host# edit snmp agent logger snmp-file-log-1 file
```

```
[edit]
user@host# edit slot 0 jps logger jps-file-log-1 file
```

2. Specify the filter to define which event messages the software logs or disregards.

```
[edit shared sae configuration logger sae-file-log-1 file]
user@host# set filter filter
```

If you do not specify a filter, logging to the specified file is disabled.

Filters can specify the logging level, such as debug, or can specify expressions.

3. Specify the absolute path of the filename that contains the current log files.

```
[edit shared sae configuration logger sae-file-log-1 file]
user@host# set filename filename
```

Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

4. (Optional) Specify the absolute path of the filename that contains the log history.

```
[edit shared sae configuration logger sae-file-log-1 file]
user@host# set rollover-filename rollover-filename
```

When the log file reaches the maximum size, the software closes the log file and renames it. If a previous rollover file exists, the software overwrites it. The software then reopens the log file and continues to save event messages in it.



NOTE: On a C-series controller, log files are automatically rotated on a daily basis. If you do configure a rollover file when files are rotated, the software creates five compressed versions of partial log files, and one uncompressed log file.

5. (Optional) Specify the maximum size of the log file and the rollover file.

```
[edit shared sae configuration logger sae-file-log-1 file]
user@host# set maximum-file-size maximum-file-size
```

Do not set the maximum file size to a value greater than the available disk space.



NOTE: On a C-series controller, log files are automatically rotated on a daily basis.

Configuring System Logging with SRC CLI

Use the following statements to configure the SRC software to send log messages to the system logging facility:

```
logger name syslog {
  filter filter;
  host host;
  facility facility;
  format format;
}
```

You can configure components to send log messages to the system log server (also called a syslog server) on the platform on which the SRC software is running.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See Categories and Severity Levels for Event Messages.

To configure component logging to the system log server:

1. From configuration mode, access the configuration statement that configures the logging destination for the component. For example:

```
[edit]
user@host# component-hierarchy logger name syslog
```

For example:

```
[edit]
user@host# edit shared sae configuration logger sae-sys-1 syslog
```

```
[edit]
user@host# edit snmp agent logger snmp-sys-1 syslog
```

```
[edit]
user@host# edit slot 0 jps logger jps-sys-1 syslog
```

2. (Optional) Specify the filter to define which event messages the software logs or disregards.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set filter filter
```

Filters can specify the logging level, such as debug, or can specify expressions.

3. (Optional) Change the IP address or name of a host that collects event messages by means of a standard system logging daemon.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set host host
```

By default, the host is `loghost` for the syslog server on the local host. (Configuration in the `/etc/hosts` file sets `loghost` to `localhost`.)

Make sure that the user under which the J2EE application server or Web application server runs has write access to this folder. If this user does not have write access to the default folder, configure the component or application to write logs in folders to which the user has write access.

4. (Optional) Specify the type of system log in accordance with the system logging protocol, a value of 0–23.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set facility facility
```

5. (Optional) Specify the MessageFormat string that indicates how the information in an event message is printed.

```
[edit shared sae configuration logger sae-sys-1 syslog]
user@host# set format format
```

Specify a MessageFormat string as defined in

<http://java.sun.com/j2se/1.4.2/docs/api/java/text/MessageFormat.html>

The fields available for events are:

- 0—Time and date of the event
- 1—Name of the thread generating the event
- 2—Text message of the event
- 3—Category of the event
- 4—Priority of the event

Chapter 4

Configuring Logging for SRC Components (C-Web Interface)

- Before You Configure Logging on page 17
- Configuring ACP to Store Log Messages in a File (C-Web Interface) on page 17
- Configuring the SAE to Store Log Messages in a File (C-Web Interface) on page 18
- Configuring NIC to Store Log Messages in a File (C-Web Interface) on page 18
- Configuring the SNMP to Store Log Messages in a File (C-Web Interface) on page 18
- Configuring JPS to Store Log Messages in a File (C-Web Interface) on page 19

Before You Configure Logging

Before you configure logging for SRC components, you should be familiar with the logging filters that you can configure. If you use a syslog log facility, you should be familiar with the syslog protocol. For information about logging filters see Overview of Logging for SRC Components.

If you plan to filter log messages, you should be familiar with severity levels and filters for logging before you configure system logging for a component. See Categories and Severity Levels for Event Messages.

Configuring ACP to Store Log Messages in a File (C-Web Interface)

To configure component logging for ACP:

1. Click **Configure**, expand **Shared**, expand **ACP**, and then click **Configuration**.

The Configuration pane appears.

2. From the Create new list, select **Logger**.
3. In the dialog box, type a name for the new logger, and click **OK**.

The name of the logger appears in the side pane and the Logger pane.

4. Expand the logger in the side pane, and then click **File** or **Syslog**.
5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the SAE to Store Log Messages in a File (C-Web Interface)

To configure component logging for SAE:

1. Click **Configure**, expand **Shared**, expand **ACP**, and then click **Configuration**.

The Configuration pane appears.

2. From the Create new list, select **Logger**.

The name of the logger appears in the side pane and the Logger pane.

3. Expand the logger in the side pane, and then click **File** or **Syslog**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring NIC to Store Log Messages in a File (C-Web Interface)

To configure component logging for NIC:

1. Click **Configure**, expand **Shared**, and then click **NIC**.

The NIC pane appears.

2. In the side pane, expand a configuration scenario, such as Scenario:OnePopSharedlp.
3. In the side pane, expand a host, such as Demohost.

The Hosts pane appears.

4. From the Create new list, select **Logger**.

The name of the logger appears in the side pane and the Logger pane.

5. Expand the logger in the side pane, and then click **File** or **Syslog**.
6. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring the SNMP to Store Log Messages in a File (C-Web Interface)

To configure component logging for SNMP:

1. Click **Configure**, expand **Snmp**, and then click **Agent**.

The Agent pane appears.

2. From the Create new list, select **Logger**.

The name of the logger appears in the side pane and the Logger pane.

3. Expand the logger in the side pane, and then click **File** or **Syslog**.
4. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Configuring JPS to Store Log Messages in a File (C-Web Interface)

To configure component logging for JPS:

1. Click **Configure**, expand **Slot**, and then expand the slot for which you want to configure component logging.
2. Click **JPS**.

The JPS pane appears.

3. From the Create new list, select **Logger**.

The name of the logger appears in the side pane and the Logger pane.

4. Expand the logger in the side pane, and then click **File** or **Syslog**.
5. Click **Create**, enter information as described in the Help text in the main pane, and click **Apply**.

Part 3

Using Simulated Router Drivers and Simulated Subscribers for Testing

- Configuring a Simulated Router Driver for Testing (SRC CLI) on page 23
- Configuring a Simulated Router Driver for Testing (C-Web Interface) on page 27
- Using Simulated Subscribers for Testing (SRC CLI) on page 29

Chapter 5

Configuring a Simulated Router Driver for Testing (SRC CLI)

- Overview of Simulated Router Drivers for the SRC Software on page 23
- Configuring Simulated Router Drivers (SRC CLI) on page 23

Overview of Simulated Router Drivers for the SRC Software

Simulated router drivers allow you to create subscriber sessions without connecting to a router. You can then use the simulated subscriber sessions to test SAE applications.

The SRC software has a default simulated router driver instance called `default@simJunos`.

Related Topics ■ Configuring Simulated Router Drivers (SRC CLI)

Configuring Simulated Router Drivers (SRC CLI)

You configure a simulated router in the same way that you configure a real router.

Before you configure a simulated router driver:

- Make sure that you configure an interface classification script for the simulated router.

See Overview of Classification Scripts.

- Configure the SAE to instantiate a simulated router driver for each simulated router that you create.
- (Optional) Configure a session store for a simulated router driver. The driver uses the session store to store subscriber sessions, service sessions, and policies.

See Configuring the Session Store Feature

Use the following configuration statements to configure simulated router drivers:

```
shared sae configuration driver simulated name {  
    driver-type (junos | junose | pcmm);  
    router-version router-version ;  
}
```

```

    driver-address driver-address ;
    transport-router transport-router ;
}

```

To configure simulated router drivers:

1. From configuration mode, access the configuration statement that configures simulated router drivers. In this sample procedure, *west-region* is the name of the SAE group, and *default@simjunos* is the name of the simulated router driver.

```

[edit]
user@host# edit shared sae group west-region configuration driver simulated
default@simJunos

```

2. Configure the type of device that the simulated driver simulates.

```

[edit shared sae group west-region configuration driver simulated
default@simJunos]
user@host# set driver-type (junos | junose | pcmm)

```

3. (Optional) Configure the version of the router software to simulate. This is the software version that is sent by the router.

```

[edit shared sae group west-region configuration driver simulated
default@simJunos]
user@host# set router-version router-version

```

4. Configure the IP address of the device driver.

```

[edit shared sae group west-region configuration driver simulated
default@simJunos]
user@host# set driver-address driver-address

```

5. (Optional) Configure the name of a virtual router that is used to connect to the SAE. This value is passed to the router initialization script. It is not supported on the JUNOS routing platform.

```

[edit shared sae group west-region configuration driver simulated
default@simJunos]
user@host# set transport-router transport-router

```

6. (Optional) Verify the configuration of the simulated driver.

```

[edit shared sae group west-region configuration driver simulated
default@simJunos]

user@host# show

driver-type junos;
router-version 8.4;
driver-address 10.10.90.5;

```

Related Topics ■ Overview of Simulated Router Drivers for the SRC Software

- For information about setting up SAE groups, see [Configuring an SAE Group](#).

Chapter 6

Configuring a Simulated Router Driver for Testing (C-Web Interface)

- Configuring a Simulated Router Driver for Testing (C-Web Interface) on page 27

Configuring a Simulated Router Driver for Testing (C-Web Interface)

You configure a simulated router in the same way that you configure a real router.

Before you configure a simulated router driver:

- Make sure that you configure an interface classification script for the simulated router.

See Overview of Classification Scripts.

- Configure the SAE to instantiate a simulated router driver for each simulated router that you create.
- (Optional) Configure a session store for a simulated router driver. The driver uses the session store to store subscriber sessions, service sessions, and policies.

See Configuring the Session Store Feature.

To configure simulated router drivers:

1. Click **Configure**, expand **Shared**, expand **SAE**, expand **Configuration**, and then click **Driver**.

The Driver pane appears.

2. From the Create new list, select **Simulated**.
3. In the dialog box, type a name for the new simulated driver, and click **OK**.

The name of the simulated driver appears in the side pane and the Driver pane.

4. Enter information as described in the Help text in the main pane, and click **Apply**.

Related Topics

- Overview of Simulated Router Drivers for the SRC Software
- Configuring Simulated Router Drivers (SRC CLI)
- For information about setting up SAE groups, see Configuring an SAE Group

Chapter 7

Using Simulated Subscribers for Testing (SRC CLI)

- Overview of Simulated Subscribers on page 29
- Commands to Manage Simulated Subscribers on page 29
- Logging In Simulated Subscribers with the CLI on page 30
- Viewing Subscriber Sessions on page 33
- Logging Out Simulated Subscribers with the CLI on page 33

Overview of Simulated Subscribers

Simulated subscribers allow you to create subscriber sessions without connecting to a router or other device. When developing an application, you can log in as a simulated subscriber to test a portal without a router or a client PC. You can log out from the simulated subscriber session in the same way that you log out from other subscriber sessions.

Commands to Manage Simulated Subscribers

You can use the following operational mode commands to manage simulated subscribers.

- `request sae login ipv4 authenticated-dhcp`
- `request sae login ipv4 authenticated-interface`
- `request sae login ipv4 unauthenticated-dhcp`
- `request sae login ipv4 unauthenticated-interface`
- `request sae logout dn`
- `request sae logout ip`
- `request sae logout login-name`
- `request sae logout session-id`
- `show sae subscribers`
- `show sae subscribers dn`
- `show sae subscribers ip`

- `show sae subscribers login-name`
- `show sae subscribers session-id`

Related Topics ■ For detailed information about each command, see the *SRC-PE CLI Command Reference*

Logging In Simulated Subscribers with the CLI

You can log in IPv4 subscribers in the following ways:

- Logging In Authenticated DHCP Subscribers on page 30
- Logging In Authenticated Interface Subscribers on page 31
- Logging In Unauthenticated DHCP Subscribers on page 31
- Logging In Unauthenticated Interface Subscribers on page 32

Logging In Authenticated DHCP Subscribers

Use the following command to log in simulated IPv4 authenticated DHCP subscribers:

```
request sae login ipv4 authenticated-dhcp virtual-router virtual-router address address
login-name login-name mac-address mac-address <service-bundle service-bundle
> <radius-class radius-class > <interface-name interface-name > <interface-alias
interface-alias > <interface-description interface-description > <nas-port-id nas-port-id
>
```

To log in a simulated IPv4 authenticated DHCP subscriber:

1. Issue the `request sae login ipv4 authenticated-dhcp` command. Specify the `virtual-router`, `address`, `login-name`, and `mac-address` options.

```
user@host> request sae login ipv4 authenticated-dhcp virtual-router virtual-router
address address login-name login-name mac-address mac-address
```

2. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the `service-bundle` option.
3. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the `radius-class` option.
4. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the `interface-name` option.
5. (Optional) To specify the interface description used when logging in the simulated subscriber, use the `interface-alias` option.

If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the `interface description` command.

6. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the `interface-description` option.
7. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the `nas-port-id` option.

Logging In Authenticated Interface Subscribers

Use the following command to log in simulated IPv4 authenticated interface subscribers:

```
request sae login ipv4 authenticated-interface virtual-router virtual-router address
address login-name login-name <service-bundle service-bundle > <radius-class
radius-class > <interface-name interface-name > <interface-alias interface-alias >
<interface-description interface-description > <nas-port-id nas-port-id >
```

To log in a simulated IPv4 authenticated interface subscriber:

1. Issue the `request sae login ipv4 authenticated-interface` command. Specify the `virtual-router`, `address`, and `login-name` options.

```
user@host> request sae login ipv4 authenticated-interface virtual-router
virtual-router address address login-name login-name
```

2. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the `service-bundle` option.
3. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the `radius-class` option.
4. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the `interface-name` option.
5. (Optional) To specify the interface description used when logging in the simulated subscriber, use the `interface-alias` option.

If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the `interface description` command.

6. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the `interface-description` option.
7. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the `nas-port-id` option.

Logging In Unauthenticated DHCP Subscribers

Use the following command to log in simulated IPv4 unauthenticated DHCP subscribers:

```
request sae login ipv4 unauthenticated-dhcp virtual-router virtual-router address
address mac-address mac-address <login-name login-name > <service-bundle
service-bundle > <radius-class radius-class > <interface-name interface-name >
<interface-alias interface-alias > <interface-description interface-description >
<nas-port-id nas-port-id >
```

To log in a simulated IPv4 unauthenticated DHCP subscriber:

1. Issue the `request sae login ipv4 unauthenticated-dhcp` command. Specify the `virtual-router`, `address`, and `mac-address` options.

```
user@host> request sae login ipv4 unauthenticated-dhcp virtual-router
virtual-router address address mac-address mac-address
```

2. (Optional) To specify the fully-qualified name used to log in the simulated subscriber, use the **login-name** option.
3. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the **service-bundle** option.
4. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the **radius-class** option.
5. (Optional) To specify the virtual interface used when logging in the simulated subscriber, use the **interface-name** option.
6. (Optional) To specify the interface description used when logging in the simulated subscriber, use the **interface-alias** option.

If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the **interface description** command.

7. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the **interface-description** option.
8. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the **nas-port-id** option.

Logging In Unauthenticated Interface Subscribers

Use the following command to log in simulated IPv4 unauthenticated interface subscribers:

```
request sae login ipv4 unauthenticated-interface virtual-router virtual-router
interface-name interface-name <address address > <login-name login-name >
<service-bundle service-bundle > <radius-class radius-class > <interface-alias
interface-alias > <interface-description interface-description > <nas-port-id nas-port-id
>
```

To log in a simulated IPv4 authenticated interface subscriber:

1. Issue the **request sae login ipv4 authenticated-interface** command. Specify the **virtual-router** and **interface-name** options.

```
user@host> request sae login ipv4 authenticated-interface virtual-router
virtual-router interface-name interface-name
```

2. (Optional) To specify the IP address from which you log in the simulated subscriber, use the **address** option.
3. (Optional) To specify the fully-qualified name used to log in the simulated subscriber, use the **login-name** option.
4. (Optional) To specify the service bundle used when logging in the simulated subscriber, use the **service-bundle** option.
5. (Optional) To specify the RADIUS class used when logging in the simulated subscriber, use the **radius-class** option.

6. (Optional) To specify the interface description used when logging in the simulated subscriber, use the **interface-alias** option.

If you are simulating JUNOSe routers, the interface alias is the description that is configured on JUNOSe routers with the **interface description** command.

7. (Optional) To specify the alternate interface name used when logging in the simulated subscriber, use the **interface-description** option.
8. (Optional) To specify the port identifier of an interface used when logging in the simulated subscriber, use the **nas-port-id** option.

Viewing Subscriber Sessions

Purpose View all subscriber sessions.

Action `user@host> show sae subscribers`

Logging Out Simulated Subscribers with the CLI

You can view subscribers who are logged in and then log out subscribers who are accessible:

- Logging Out Subscribers by DN on page 33
- Logging Out Subscribers by IP Address on page 34
- Logging Out Subscribers by Login Name on page 34
- Logging Out Subscribers by Session ID on page 34

Logging Out Subscribers by DN

To log out subscribers who are accessible by DN:

1. Issue the **show sae subscribers dn** command to view the subscribers who are accessible by DN.
2. Issue the **request sae logout dn** command to log out all subscribers who are accessible by DN.
3. To log out specific subscribers, use the **filter** option and specify all or part of the DN for the subscribers that you want to log out.

```
user@host> request sae logout dn filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout dn force
user@host> request sae logout dn filter filter force
```

Logging Out Subscribers by IP Address

To log out subscribers who are accessible by IP address:

1. Issue the **show sae subscribers ip** command to view the subscribers who are accessible by IP address.
2. Issue the **request sae logout ip** command to log out all subscribers who are accessible by IP address.
3. To log out specific subscribers, use the **filter** option and specify the IP address for the subscribers that you want to log out.

```
user@host> request sae logout ip filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout ip force
user@host> request sae logout ip filter filter force
```

Logging Out Subscribers by Login Name

To log out subscribers who are accessible by login name:

1. Issue the **show sae subscribers login-name** command to view the subscribers accessible by login name.
2. Issue the **request sae logout login-name** command to log out all subscribers accessible by login name.
3. To log out specific subscribers, use the **filter** option and specify all or part of the login name for the subscribers that you want to log out.

```
user@host> request sae logout login-name filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout login-name force
user@host> request sae logout login-name filter filter force
```

Logging Out Subscribers by Session ID

To log out subscribers who are accessible by session ID:

1. Issue the **show sae subscribers session-id** command to view the subscribers accessible by session ID.
2. Issue the **request sae logout session-id** command to log out all subscribers accessible by session ID.
3. To log out specific subscribers, use the **filter** option and specify all or part of the session ID for the subscribers that you want to log out.

```
user@host> request sae logout session-id filter filter
```

4. To specify that no confirmation is requested before the software logs out the subscribers, use the **force** option.

```
user@host> request sae logout session-id force
```

```
user@host> request sae logout session-id filter filter force
```


Part 4

Using SNMP for Monitoring and Troubleshooting

- Creating Custom SNMP Monitors on page 39
- Configuring the SNMP Traps (SRC CLI) on page 49
- Understanding Traps on page 55

Chapter 8

Creating Custom SNMP Monitors

- SNMP Monitoring on C-series Controllers on page 39
- Configuration Statements for Customized SRC SNMP Monitors on page 41
- Configuring an SNMP Alarm on a C-series Controller (SRC CLI) on page 42
- Defining an Alarm for an SNMP Monitor That Compares Object Values (SRC CLI) on page 43
- Defining an Alarm to Monitor the Status of an Object (SRC CLI) on page 44
- Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds (SRC CLI) on page 44
- Defining a Discontinuity Check to Validate Delta Values (SRC CLI) on page 45
- Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI) on page 46
- Defining Events for Which SNMP Sends Notifications (SRC CLI) on page 46
- Defining Events That Set Values for SNMP MIB Objects (SRC CLI) on page 47
- Example: SNMP Monitoring of Multiple MIB Objects on page 47

SNMP Monitoring on C-series Controllers

You can create custom SNMP monitors to detect changes in MIB objects. Use custom monitors to generate an alarm and take action in response to an alarm.

To configure a monitor, you define a condition that when met generates an SNMP notification. You can define a monitor for any single MIB object (of type integer) supported on a C-series Controller. These MIBs include Juniper Networks enterprise-specific objects as well as standard MIB objects.

You can configure the following for custom monitors:

- Alarms—Define an alarm condition and an event to generate in response to the alarm.

An alarm identifies the object to be monitored, the frequency with which the monitor retrieves a sample value for the object, and a condition that triggers an event.

- Events—Define the type of action (SNMP set or notification) to be taken in response to an alarm condition. If you do not define an event for an alarm, SNMP sends the notifications based on the monitor type.

The SRC software supports the following types of alarm conditions for monitors:

- Boolean test—Compares a sample value with a specified value or range of values.
- Existence test—Monitors when an object appears, disappears, or changes value.
- Threshold test—Monitors when an object's value rises above or falls below specified values.

A monitor supports only one type of alarm condition, or test, at a time. Each alarm can use one of the following sampling methods:

- Absolute value—Uses the actual value of the object.

Existence tests support only absolute values.

- Delta value—Uses the difference between two sample values.

By using the delta value sampling method, you can configure SNMP to detect a discontinuity in values to prevent false alarms caused by the value of a MIB object being reset. At the end of a polling interval before the SNMP agent calculates a delta value, SNMP checks the value of a MIB object called a discontinuity marker. If the value of the discontinuity marker changes, SNMP does not perform the test for the associated condition until the next polling interval.

For alarms that do not have a configured event, SNMP sends the following notifications that are defined in RFC 2981—Event MIB (October 2000):

- Boolean or existence test—`mteTriggerFired`
- Threshold test (rising value)—`mteTriggerRising`
- Threshold test (falling value)—`mteTriggerfalling`

The default configuration for SNMP custom monitors assesses all objects in a MIB branch based on the object identifier specified for the monitor. For this type of monitor, you can configure SNMP notification MIB objects located in the same row as the object that generates the event, as well as for a single object. You can create sophisticated monitors by monitoring an entire branch, then creating notifications for multiple objects.

Related Topics

- Configuration Statements for Customized SRC SNMP Monitors
- Configuring an SNMP Alarm on a C-series Controller (SRC CLI)
- Example: SNMP Monitoring of Multiple MIB Objects
- Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI)
- Overview of SNMP Traps
- Information about SRC MIBs on the Juniper Web site at <http://www.juniper.net/techpubs/software/management/src>
- Also, see information about the `disman` event MIB in RFC 2981—Event MIB (October 2000)

Configuration Statements for Customized SRC SNMP Monitors

Use the following configuration statements to configure the SNMP custom monitoring at the [edit] hierarchy level.

```
snmp monitor {
  security-name security-name;
}
snmp monitor alarm name{
  interval interval;
  sample-type (absolute-value | delta-value);
  ignore-startup-alarm;
  event event;
  variable variable;
  strict-oid;
}
snmp monitor alarm name boolean-test {
  comparison (equal | unequal | less | less-or-equal | greater | greater-or-equal);
  value value;
}
snmp monitor alarm name existence-test {
  type (present | absent | changed);
}
snmp monitor alarm name threshold-test {
  rising-threshold rising-threshold;
  falling-threshold falling-threshold;
}
snmp monitor alarm name delta-discontinuity-check {
  variable variable;
}
snmp monitor event namenotification {
  oid oid;
  strict-object [strict-object...];
  wildcarded-object [wildcarded-object...];
}
snmp monitor event name snmp-set {
  variable variable;
  value value;
  strict-oid;
}
```

- Related Topics**
- Configuring an SNMP Alarm on a C-series Controller (SRC CLI)
 - SNMP Monitoring on C-series Controllers
 - For detailed information about each configuration statement, see the SRC-PE CLI Command Reference.

Configuring an SNMP Alarm on a C-series Controller (SRC CLI)

You can configure SNMP to establish alarms for custom monitors.



NOTE: Configure only one monitor test at a time.

To configure an SNMP alarm:

1. Specify an SNMP username.

See Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI).

2. From configuration mode, access the configuration statements that configures an alarm. For example:

```
[edit]
user@host# edit snmp monitor alarm saeHeapUsage
```

where **saeHeapUsage** is the name of the alarm.

3. Specify the number of seconds between which SNMP samples the value of an object. For example:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set interval 60
```

4. Specify whether to sample the actual value of the object or the difference between two values. For example, to use the actual of the object:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set sample-type absolute-value
```

If you set the sample type to **delta-value**, you can configure a discontinuity check. See Defining a Discontinuity Check to Validate Delta Values (SRC CLI).

5. (Optional) Indicate that an alarm not be sent when the alarm is initially activated.

```
[edit snmp monitor alarmsaeHeapUsage]
user@host# set ignore-startup-alarm
```

6. (Optional) Specify the name of the event to be generated in response to an alarm condition. For example:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set event saeHeapUsageEvent
```

7. Specify the name or object identifier (OID) of the MIB variable to be monitored. For example:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set variable juniSdxSaeHeapUsed.0
```

8. (Optional) Specify whether to monitor the SNMP object instance identified by a variable attribute. To monitor the SNMP object instance specified by the variable attribute:

```
[edit snmp monitor alarm saeHeapUsage]
user@host# set strict-oid
```

Do not enable the **strict-oid** option when you monitor a column of an SNMP MIB table. An alarm for a column monitors the column on all entries of the table. If an entry for an object in the column passes an alarm test, an event is generated for that object.

9. Configure a boolean, existence, or threshold test for the alarm.

- Related Topics**
- Defining an Alarm for an SNMP Monitor That Compares Object Values (SRC CLI)
 - Defining an Alarm to Monitor the Status of an Object (SRC CLI)
 - Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds (SRC CLI)
 - SNMP Monitoring on C-series Controllers
 - Configuration Statements for Customized SRC SNMP Monitors

Defining an Alarm for an SNMP Monitor That Compares Object Values (SRC CLI)

You can configure a monitor to compare a sample value to a specified value or range of values by using one of the following types of comparisons:

- equal
- unequal
- less
- less-or-equal
- greater
- greater-or-equal



NOTE: Configure only one monitor test at a time.

Before you define an alarm type, configure the associated SNMP alarm.

See [Configuring an SNMP Alarm on a C-series Controller \(SRC CLI\)](#).

To configure a monitor to compare a sample to a specified value or range of values:

1. From configuration mode, access the configuration statements that configure SNMP monitoring for a boolean test. For example:

```
[edit]
user@host# edit snmp monitor alarm saeHeapUsage boolean-test
```

where **saeHeapUsage** is the name of the alarm.

- Specify the type of boolean test. For example:

```
[edit snmp monitor alarm saeHeapUsage boolean-test]
user@host# set comparison greater
```

- Define the value that the test uses. For example:

```
[edit snmp monitor saeHeapUsage boolean-test]
user@host# value 14000000
```

- Related Topics**
- SNMP Monitoring on C-series Controllers
 - Configuration Statements for Customized SRC SNMP Monitors

Defining an Alarm to Monitor the Status of an Object (SRC CLI)

You can configure a monitor to identify when a MIB object appears, disappears, or changes value. If the test criteria are met, the test is considered to be successful.



NOTE: Configure only one monitor test at a time.

Before you define an alarm type, configure the associated SNMP alarm.

See [Configuring an SNMP Alarm on a C-series Controller \(SRC CLI\)](#).

To configure an alarm to monitor the status of an object:

- Specify the type of alarm: present, absent, or changed. For example for an alarm named existence-alarm:

```
[edit snmp monitor alarm existence-alarm existence-test]
user@host# set type present
```

- Related Topics**
- SNMP Monitoring on C-series Controllers
 - Configuration Statements for Customized SRC SNMP Monitors

Defining an Alarm for an SNMP Monitor That Compares Values Against Thresholds (SRC CLI)

You can configure a monitor to compare a sample value for a MIB object to a threshold encountered as the value rises and a threshold encountered as the value falls.



NOTE: Configure only one monitor test at a time.

Before you define an alarm type, configure the associated SNMP alarm.

See Configuring an SNMP Alarm on a C-series Controller (SRC CLI).

To configure an alarm for a monitor that compares a sample value to an upper threshold value and a lower threshold value:

1. Define the upper threshold against which to compare a rising sample value. For example:

```
[edit snmp monitor alarm thresholds threshold-test]
user@host# set rising-threshold 2
```

2. Define the lower threshold against which to compare a falling sample value. For example:

```
[edit snmp monitor alarm threshold-alarm]
user@host# set falling-threshold 1
```

- Related Topics**
- SNMP Monitoring on C-series Controllers
 - Configuration Statements for Customized SRC SNMP Monitors

Defining a Discontinuity Check to Validate Delta Values (SRC CLI)

You can configure a monitor to use a discontinuity check to prevent sending false alarms when the value of the monitored object is reset between two samples.

Use a discontinuity check when the sampling type for a monitor is **delta-value** and the test type is boolean or threshold. You define a variable, called a discontinuity marker (a MIB object used to validate the delta, or difference, between values). Typically, the marker object is of the type TimeTicks, DateAndTime, or Timestamp.

To define a discontinuity check:

1. Configure an SNMP alarm with the sample type set to **delta-value**.

See Configuring an SNMP Alarm on a C-series Controller (SRC CLI).

2. From configuration mode, access the configuration statements that configures a discontinuity check. For example, for an alarm named ifErrorsDelta:

```
[edit]
user@host# edit snmp monitor alarm ifErrorsDelta delta-discontinuity-check
```

3. Specify the name or object identifier (OID) of the discontinuity marker. For example:

```
[edit snmp monitor alarm sequence-check ifErrorsDelta delta-discontinuity-check]
user@host# set variable ifTable.ifEntry.ifLastChange
```

- Related Topics**
- SNMP Monitoring on C-series Controllers
 - Configuration Statements for Customized SRC SNMP Monitors

Configuring an SNMPv3 Security Name for SNMP Monitoring (SRC CLI)

To configure an SNMPv3 security name to access a monitored MIB object:

1. From configuration mode, access the configuration statements that configure SNMP monitoring.

```
[edit]
user@host# edit snmp monitor
```

2. Specify an SNMPv3 security name.

```
[edit snmp monitor]
user@host# set security-name your-security-name
```

- Related Topics**
- Configuring an SNMP Alarm on a C-series Controller (SRC CLI)
 - SNMP Monitoring on C-series Controllers
 - Configuration Statements for Customized SRC SNMP Monitors

Defining Events for Which SNMP Sends Notifications (SRC CLI)



NOTE: Do not define an event notification and an SNMP set for the same event.

To define an event for which SNMP sends a notification:

1. From configuration mode, access the configuration statements that configure SNMP event notification and provide a name for the event. For example:

```
[edit]
user@host# edit snmp monitor event routerErrorEvent notification
```

2. Specify the object identifier (OID) object identifier of the notification object. For example:

```
[edit snmp monitor event routerErrorEvent notification]
user@host# set oid junisdxmibs.24.2.1
```

3. (Optional) Allow wildcards in the OID to include instances of subidentifiers that correspond to the monitored object. For example:

```
[edit snmp monitor event routerErrorEvent notification notification]
user@host# set wildcarded-object [juniSaeRouterMsgErrors,
juniSaeRouterMsgTimeouts]
```

Alternatively, you can configure event notification to use a specific OID.

- Related Topics**
- Example: SNMP Monitoring of Multiple MIB Objects
 - Configuring an SNMP Alarm on a C-series Controller (SRC CLI)

- SNMP Monitoring on C-series Controllers
- Configuration Statements for Customized SRC SNMP Monitors

Defining Events That Set Values for SNMP MIB Objects (SRC CLI)

You can configure SNMP to set the value of a MIB object in response to an SNMP event.



NOTE: Do not define an event notification and an SNMP set for the same event.

To define an event that sets the value for a MIB variable in response to an SNMP event:

1. From configuration mode, access the configuration statements that configure an SNMP set for an event.

```
[edit]
user@host# edit snmp monitor event event-name snmp-set
```

2. Specify the object identifier (OID) of the MIB variable to set.

```
[edit snmp monitor event event-name snmp-set]
user@host# set oid OID
```

3. Specify the value for the object.

```
[edit snmp monitor event event-name snmp-set]
user@host# set value value
```

4. (Optional) Specify whether the software monitors only the OID specified by the variable option. If you do not set this option, the index of the object triggering the alarm is appended to the variable to be set.

```
[edit snmp monitor event event-name snmp-set]
user@host# set strict-oid
```

- Related Topics**
- Configuring an SNMP Alarm on a C-series Controller (SRC CLI)
 - SNMP Monitoring on C-series Controllers
 - Configuration Statements for Customized SRC SNMP Monitors

Example: SNMP Monitoring of Multiple MIB Objects

You can configure SNMP to monitor a column of a MIB table and configure SNMP notifications to include MIB objects located in the same row as the object that generates the event. This example shows how to configure an alarm to generate an event in response to error conditions and send notifications that contain both the number of router errors and router timeouts .

This example uses the `juniSaeRouterTable` shown in Table 6 on page 48. SNMP monitors the `juniSaeRouterMsgErrors` branch, and sends a notification object (`juniSdxMibs.24.2.1`) for the objects in the same row as the object attached to the notification: `juniSaeRouterMsgTimeouts` and `juniSaeRouterMsgErrors`. The monitor generates an event named `routerErrorEvent` for the column `juniSaeRouterMsgErrors`.

Table 6: Example Table for `juniSaeRouterTable` Object

<code>juniSaeRouterClinetId</code>	<code>juniSaeRouterMsgErrors</code>	<code>juniSaeRouterMsgTimeouts</code>
<code>default@router1</code>	100	5
<code>default@router2</code>	11	0
<code>default@router3</code>	52	2
...

The following example shows the configuration for this scenario.

```
snmp monitor {
  alarm saeRouterErrors {
    variable juniSaeRouterMsgErrors;
    //strict-oid;
    event routerErrorEvent;
    ...
  }
  event routerErrorEvent notification {
    oid juniSdxMibs.24.2.1
    wildcarded-object [juniSaeRouterMsgErrors,
juniSaeRouterMsgTimeouts]
  }
}
```

- Related Topics**
- SNMP Monitoring on C-series Controllers
 - Configuring an SNMP Alarm on a C-series Controller (SRC CLI)
 - Configuration Statements for Customized SRC SNMP Monitors

Chapter 9

Configuring the SNMP Traps (SRC CLI)

- Overview of SNMP Traps on page 49
- Configuration Statements for the SNMP Traps on page 51
- Configuring Performance Traps on page 52
- Configuring Event Traps on page 53

Overview of SNMP Traps

The SNMP agent provides network management systems with SNMP trap notifications in case of component failure or when critical resources are out of configurable limits. This information is captured in a Management Information Base (MIB).

The SNMP agent can be run on each SRC host. It can monitor any SRC process running on the host and is preconfigured to monitor SRC processes. Additionally, it provides detailed monitoring and configuration of SRC server components.

MIBs

The SNMP agent monitors MIB variables. Most variables measure the performance of the system. Some variables are counters, such as the `saeLogins` variable, which counts the total number of subscriber logins since startup. Some variables are gauges, and their numbers go up and down, such as the `saeHeapUsed` variable, which measures the Java Virtual Machine heap that is currently in use.

A MIB defines a trap type that is associated with many MIB variables. For traps based on counters, the SNMP agent periodically polls each specified variable. It takes the difference between the previous and current values of the variable and compares that difference with the threshold. If the difference has moved up across thresholds, the SNMP agent sends a trap raising an alarm (minor, major, or critical) for the highest threshold crossed to all configured receivers. If the difference has moved down across thresholds, the agent sends a trap clearing the alarm of the lowest threshold crossed.

You can configure the polling interval between samples. If you change the polling interval, also adjust the thresholds. For instance, if the critical threshold for SAE logins is 1,000 and the interval is 60 seconds, then a critical alarm is raised if there are more than 1,000 logins in 60 seconds. But if you change the interval to 600 seconds, then you would need to change the threshold to 10,000 to have the same meaning.

For traps based on gauges, the previous value is not needed; the current value is compared with the thresholds.

In the trap tables, there is a field named R/AV, where R means rate, and AV means absolute value. Rate is used for variables that are counters, and it measures the rate of change of the counter. Absolute value is used for variables that are gauges.

Configuration MIBs

The SRC software has a limited number of MIB variables that can be set, such as variables to shut down or start components.

MIB Structure

The SNMP agent MIB uses the following Juniper Networks MIBs:

- Juniper-SDX-ACP-MIB—SRC-ACP MIB
- Juniper-SDX-CHASSIS-MIB—Chassis MIB (for C-series Controllers)
- Juniper-SDX-DES-MIB—Directory eventing system MIB
- Juniper-SDX-GW-MIB—Gateway applications MIB (includes the NIC MIB)
- Juniper-SDX-JPS-MIB—JPS MIB
- Juniper-SDX-LICENSE-MIB—Licensing MIB
- Juniper-SDX-MIB—Main Juniper Networks SDX MIB
- Juniper-SDX-MIBS—Collection of Juniper Networks SDX MIB modules
- Juniper-SDX-POM-MIB—Policy management MIB
- Juniper-SDX-REDIRECTOR-MIB—Redirector MIB
- Juniper-SDX-SAE-MIB—SAE MIB
- Juniper-SDX-TC-MIB—Textual conventions MIB
- Juniper-SDX-TRAP-MIB—SRC trap definition MIB
- Juniper-UNI-SMI—Base SMI MIB

MIB Location

The MIBs are located on the Juniper Networks Web site at

<http://www.juniper.net/techpubs/software/management/src>

Traps

Traps are individual events that the SNMP agent can monitor, such as the number of timeouts or errors that have occurred or connections that have opened or closed. There are two types of traps:

- Performance traps—Traps that poll MIB variables associated with the trap to determine whether a variable has crossed configured thresholds. If the variable crosses a threshold, an alarm is triggered and a trap is sent to the list of configured receivers.

- Event traps—Traps that are sent when an event occurs; for example, when a connection is established or closed.

SNMP Traps and Informs

SNMP notifications can be sent as traps or inform requests. SNMP traps are unconfirmed notifications. SNMP informs are confirmed notifications.

SNMP traps are defined in either standard or enterprise-specific MIBs. The standard and enterprise-specific traps are compiled into the network management software.

With traps, the receiver does not send any acknowledgment when it receives a trap and the sender cannot determine if the trap was received. To increase reliability, SNMP informs are supported in SNMPv3. With an inform, the receiver acknowledges the message with a response. For information about configuring SNMP notification handling,

Related Topics

- SAE Performance Traps
- Accounting Performance Traps
- Authentication Performance Traps
- NIC Performance Traps
- Router Driver Performance Traps
- System Management Performance Traps
- Policy Engine Performance Traps
- SRC Redirector Performance Traps
- SRC-ACP Performance Traps
- JPS Performance Traps
- For information on system logging severity levels for SNMP traps, see Categories and Severity Levels for Event Messages
- Configuring the SDX SNMP Agent

Configuration Statements for the SNMP Traps

Use the following configuration statements to configure the SNMP traps and the notification target at the [edit] hierarchy level.

```
snmp notify alarm category category-name ...
snmp notify alarm category category-name alarm alarm-name {
    interval interval;
    critical critical;
    major major;
    minor minor;
}
snmp notify event category category-name ...
snmp notify event category category-name event event-name ...
snmp notify target target-name {
```

```

    address;
    port;
    community;
    type (trapv1|trapv2|inform);
}

```

Related Topics ■ For detailed information about each configuration statement, see the *SRC-PE CLI Command Reference*.

Configuring Performance Traps

Use the following configuration statements to configure performance traps:

```

snmp notify alarm category category-name ...
snmp notify alarm category category-name alarm alarm-name {
    interval interval;
    critical critical;
    major major;
    minor minor;
}

```

To configure performance traps:

1. From configuration mode, access the configuration statement that configures the type of performance trap.

```

[edit]
user@host# edit snmp notify

```

2. Specify the type of trap and the trap name.

```

[edit snmp notify]
user@host# set alarm category category-name alarm alarm-name

```

You can select from the list of trap types and their associated traps or create new traps.

3. (Optional) Specify the interval at which the variable associated with the trap is polled.

```

[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set interval interval

```

4. Specify the threshold above which a critical alarm is generated.

```

[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set critical critical

```

5. Specify the threshold above which a major alarm is generated.

```

[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set major major

```

6. Specify the threshold above which a minor alarm is generated.

```
[edit snmp notify alarm category category-name alarm alarm-name]
user@host# set minor minor
```

Configuring Event Traps

Use the following configuration statements to configure event traps:

```
snmp notify event category category-name ...
snmp notify event category category-name event event-name ...
```

To configure event traps:

1. From configuration mode, access the configuration statement that configures the type of event trap.

```
[edit]
user@host# edit snmp notify
```

2. Specify the type of trap and the trap name.

```
[edit snmp notify]
user@host# set event category category-name event event-name
```

You can select from the list of trap types and their associated traps or create new traps.

Chapter 10

Understanding Traps

- Performance Traps on page 55
- Trap Numbers in Performance Traps on page 56
- Decoding Trap Numbers for Raised Trap Actions on page 57
- Decoding Trap Numbers for Clear Trap Actions on page 57
- SRC Performance Traps on page 57
- Event Traps on page 67
- Alarm State Transitions on page 69

Performance Traps

Trap tables list all the traps supported by the SNMP agent, the text displayed for each trap, trap thresholds and intervals, and any special notes pertaining to the trap.

Table 7 on page 55 describes the symbols used in the performance traps tables.

Table 7: Symbols in Performance Traps Tables

Symbol	Description
\$S	Severity level of the trap: MINOR, MAJOR, CRITICAL, or CLEAR
\$D	Status data
\$P	Polling interval
\$T	Threshold value
\$A	Trap action; displayed as RAISED or CLEARED
\$L	“Exceeded” if the trap is raised; “ is below” if the trap is cleared

SRC performance trap tables contain a trap ID, text displayed, and default values for alarm threshold levels, as well as rate (R) and absolute values (AV) fields.

R/AV

Each performance trap table has a field called R/AV. R means rate, and AV means absolute value.

- Rate is used for variables that are counters. The rate is the difference between the current value of the underlying MIB variable being monitored and its previous value, which was read <interval> time ago. The interval length affects those values that are appropriate for the thresholds; that is, the longer the interval, the larger the thresholds must be. For instance, saeLogins is a counter of the total number of SAE logins. With the default interval of 60 seconds, the critical threshold of 2,000 means that a critical trap is sent if there are more than 2,000 logins within one minute. If you change the interval to 300 seconds (5 minutes), to keep the critical threshold at 2,000 logins a minute, you need to change the threshold to 10,000 (the number of logins in 5 minutes for a rate of 2,000 per minute).
- Absolute value is used for variables that are gauges, and they transition from one alarm threshold level to the next.

Trap Numbers in Performance Traps

Performance traps contain a trap ID, a severity, and an action. The trap ID, severity, and action are encoded in the trap number to make it easy to configure trap receivers, such as HP OpenView, to color and highlight traps.

Every performance trap has four trap definitions: one for critical, major, and minor severity levels, and one for the clear action. For critical, major, and minor severity levels, the action is raise. For the clear action, there is no severity level, because the severity level is implied by the last raise action for the trap ID.

Severity levels are assigned the following numbers:

- Critical = 1
- Major = 2
- Minor = 3
- Information = 5

The JunoSdxTrapID ::= TEXTUAL-CONVENTION section in the Juniper-SDX-TC MIB lists the trap IDs for all traps. The Juniper-SDX-TRAP MIB defines the SDX traps.

You can access the MIBs on the Juniper Web site at

<http://www.juniper.net/techpubs/software/management/src>

Related Topics

- Decoding Trap Numbers for Raised Trap Actions
- Decoding Trap Numbers for Clear Trap Actions

Decoding Trap Numbers for Raised Trap Actions

To decode a trap number for raised trap actions:

- Use the following equation:

$$\text{Trap number} = \text{Trap ID} * 10 + \text{severity}$$

For example, if the trap number is 43, then the trap ID is 4 (saeServiceActivations) and the severity is 3 (MINOR). Therefore, a trap number of 43 means that a MINOR event has occurred for the saeServiceActivations trap.

- Related Topics**
- Trap Numbers in Performance Traps
 - Decoding Trap Numbers for Clear Trap Actions

Decoding Trap Numbers for Clear Trap Actions

To decode a trap number for clear trap actions:

- Use the following equation:

$$\text{Trap number} = \text{Trap ID} * 10$$

For example, if the trap number is 250, then the trap ID is 25 (saeAccPendingRequests). Therefore, a trap number of 250 means that the saeAccPendingRequests alarm has been cleared.

- Related Topics**
- Trap Numbers in Performance Traps
 - Decoding Trap Numbers for Raised Trap Actions

SRC Performance Traps

The following SRC performance trap tables are available:

- SAE Performance Traps on page 58
- Accounting Performance Traps on page 59
- Authentication Performance Traps on page 61
- NIC Performance Traps on page 62
- Router Driver Performance Traps on page 63
- System Management Performance Traps on page 64
- Policy Engine Performance Traps on page 65
- SRC Redirector Performance Traps on page 65
- SRC-ACP Performance Traps on page 65
- JPS Performance Traps on page 66
- Chassis Performance Traps on page 66

SAE Performance Traps

Table 8 on page 58 lists the performance traps for the SAE.

Table 8: Performance Traps–SAE

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)			Interval (sec)	R/AV
			Critical	Major	Minor		
saeHeapUsed	1	\$\$SAE:\$D% of Java VM heap is in use. This \$L the threshold of \$T %::\$A	95	90	80	60	AV
saeLogins	2	\$\$SAE:During the last \$Ps, \$D logins occurred. This \$L the threshold of \$T logins::\$A	2000	1000	400	60	R
saeLogouts	3	\$\$SAE:During the last \$Ps, \$D logouts occurred. This \$L the threshold of \$T logouts::\$A	2000	1000	400	60	R
saeServiceActivations	4	\$\$SAE:During the last \$Ps, \$D services were activated. This \$L the threshold of \$T service activations::\$A	2000	1000	500	60	R
saeServiceDeactivations	5	\$\$SAE:During the last \$Ps, \$D services were deactivated. This \$L the threshold of \$T service deactivations::\$A	2000	1000	500	60	R
saeCurrentUsers	6	\$\$SAE:The number of user sessions is \$D. This \$L the threshold of \$T users sessions::\$A	18000	14000	12000	60	AV

Table 8: Performance Traps–SAE (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				Interval (sec)	R/AV
			Critical	Major	Minor			
saeUserNumberLicense	7	\$\$:SAE:\$D % of the available licenses are in use. This \$L the threshold of \$T.:\$A	99	95	90		60	AV
saeUserLicenseExpiry	8	\$\$:SAE:The SAE license is about to expire in \$D days. This \$L the threshold of \$T.:\$A	1	10	14		3500	AV
saeClientLicExpiry	12	\$\$:SAE:The client has consumed \$D % of its available license. This \$L the threshold of \$T.:\$A	90	70	40		900	AV

Accounting Performance Traps

Table 9 on page 59 lists the performance traps for accounting.

Table 9: Performance Traps–Accounting

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				Interval (sec)	R/AV
			Critical	Major	Minor			
saeAccInvalidServerAddresses	20	\$\$:SAE RADIUS Accounting Client:During the last \$Ps, \$D invalid server address errors occurred. This \$L the threshold of \$T invalid server address errors.:\$A	5	2	1		60	R

Table 9: Performance Traps–Accounting (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				Interval (sec)	R/AV
			Critical	Major	Minor			
saeAccRoundTripTime	21	\$\$:SAE RADIUS Accounting Client:The round trip message time is \$Dms. This \$L the threshold of \$Tms.:\$A	2250	1500	750		60	AV
saeAccRetransmissions	22	\$\$:SAE RADIUS Accounting Client:During the last \$Ps, \$D retransmissions occurred. This \$L the threshold of \$T retransmissions.:\$A	5	2	1		60	R
saeAccMalformedResponses	23	\$\$:SAE RADIUS Accounting Client:During the last \$Ps, \$D malformed responses occurred. This \$L the threshold of \$T malformed responses.:\$A	5	2	1		60	R
saeAccBadAuthenticators	24	\$\$:SAE RADIUS Accounting Client:During the last \$Ps, \$D bad authenticator error occurred. This \$L the threshold of \$T bad authenticators errors.:\$A	5	2	1		60	R
saeAccPendingRequests	25	\$\$:SAE RADIUS Accounting Client:The number of pending requests is \$D. This \$L the threshold of \$T pending requests:\$A	50	25	10		60	AV

Table 9: Performance Traps–Accounting (continued)

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				Interval (sec)	R/AV
			Critical	Major	Minor			
saeAccTimeouts	26	\$\$:SAE RADIUS Accounting Client:During the last \$Ps, \$D timeouts occurred. This \$L the threshold of \$T timeouts.:\$A	30	20	10		60	R
saeAccUnknownTypes	27	\$\$:SAE RADIUS Accounting Client:During the last \$Ps, \$D unknown type errors occurred. This \$L the threshold of \$T unknown type errors.:\$A	30	20	10		60	R
saeAccPacketsDropped	28	\$\$:SAE RADIUS Accounting Client:During the last \$Ps, \$D packets were dropped. This \$L the threshold of \$T dropped packets.:\$A	30	20	10		60	AV

Authentication Performance Traps

Table 10 on page 61 lists the performance traps for authentication.

Table 10: Performance Traps–Authentication

Trap Event	Trap ID	Text Displayed	Alarm Threshold Levels (default values)				Interval(sec)	R/AV
			Critical	Major	Minor			
saeAuthInvalidServerAddresses	40	\$\$:SAE RADIUS Authentication Client:During the last \$Ps, \$D invalid server address errors occurred. This \$L the threshold of \$T invalid server address errors.:\$A	10	5	1		60	AV

Table 10: Performance Traps—Authentication (continued)

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
saeAuthRoundTripTime	41	\$\$:SAE RADIUS Authentication Client:The round trip message time is \$Dms. This \$L the threshold of \$Tms:\$A	2250	1500	750	60	R
saeAuthAccessRetransmissions	42	\$\$:SAE RADIUS Authentication Client:During the last \$Ps, \$D retransmissions occurred. This \$L the threshold of \$T retransmissions.:\$A	5	2	1	60	R
saeAuthMalformedAccessResponses	43	\$\$:SAE RADIUS Authentication Client:During the last \$Ps, \$D malformed responses occurred. This \$L the threshold of \$T malformed responses.:\$A	5	2	1	60	R
saeAuthBadAuthenticators	44	\$\$:SAE RADIUS Authentication Client:During the last \$Ps, \$D bad authenticators errors occurred. This \$L the threshold of \$T.:\$A	5	2	1	60	
saeAuthPendingRequests	45	\$\$:SAE RADIUS Authentication Client:The number of pending requests is \$D. This \$L the threshold of \$T pending requests:\$A	50	25	10	60	AV
saeAuthTimeouts	46	\$\$:SAE RADIUS Authentication Client:During the last \$Ps, \$D timeouts occurred. This \$L the threshold of \$T timeouts.:\$A	5	2	1	60	R
saeAuthUnknownTypes	47	\$\$:SAE RADIUS Authentication Client:During the last \$Ps, \$D unknown type errors occurred. This \$L the threshold of \$T unknown type errors.:\$A	5	2	1	60	R
saeAuthPacketsDropped	48	\$\$:SAE RADIUS Authentication Client:During the last \$Ps, \$D packets were dropped. This \$L the threshold of \$T dropped packets.:\$A	5	2	1	60	R

NIC Performance Traps

Table 11 on page 63 lists the performance traps for NIC.

Table 11: Performance Traps–NIC

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
nicHostReslvErrors	230	\$\$NIC Host: During the last \$Ps, the number of resolution errors that occurred is \$D. This \$L is the threshold of \$T errors.:\$A	10	5	1	60	R
nicHostAvgReslvTime	231	\$\$NIC Host: During the last \$Ps, the average time this NIC Host spent on resolutions is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	250	60	R

Router Driver Performance Traps

Table 12 on page 63 lists the performance traps for router drivers.

Table 12: Performance Traps–Router Drivers

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
routerMsgErrors	190	\$\$SAE Router Driver (\$juniSaeRouterClientId):During the last \$Ps, \$D router errors occurred. This \$L the threshold of \$T errors.:\$A	10	5	1	60	R
routerMsgTimeouts	191	\$\$SAE Router Driver (\$juniSaeRouterClientId):During the last \$Ps, \$D router timeouts occurred. This \$L the threshold of \$T timeouts.:\$A	10	5	1	60	R
routerAvgJobQTime	192	\$\$SAE Router Driver (\$juniSaeRouterClientId):During the last \$Ps, the average time that incoming router messages waited to be processed is \$Dms. This \$L the threshold of \$Tms.:\$A	500	250	100	60	R
routerJobQLength	193	\$\$SAE Router Driver (\$juniSaeRouterClientId):The number of unprocessed incoming router messages is \$D. This \$L the threshold of \$T messages.:\$A	2500	500	100	60	AV

Table 12: Performance Traps—Router Drivers (continued)

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
routerJobQAge	194	\$\$SAE Router Driver (\$juniSaeRouterClientId):The oldest unprocessed router message has been waiting for \$Dms. This \$L the threshold of \$Tms.:\$A	30000	10000	5000	60	AV
routerAvgAddTime	195	\$\$SAE Router Driver (\$juniSaeRouterClientId): During the last \$Ps, the average time (in milliseconds) this router driver spent handling 'object added' notifications is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	100	60	R
routerAvgChgTime	196	\$\$SAE Router Driver (\$juniSaeRouterClientId): During the last polling interval, the average time (in milliseconds) this router driver spent handling 'object changed' notifications is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	100	60	R
routerAvgDelTime	197	\$\$SAE Router Driver (\$juniSaeRouterClientId): During the last polling interval, the average time (in milliseconds) this router driver spent handling 'object deleted' notifications is \$Dms. This \$L the threshold of \$Tms.:\$A	1000	500	100	60	R

System Management Performance Traps

Table 13 on page 64 lists the performance traps for system management event.

Table 13: Performance Traps—System Management Event

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
agentLdapLimitReached	113	\$\$: Ldap: The Ldap Limit has been reached: \$D entries, during the last \$Ps. This \$L the threshold of \$T entries.:\$A.	100 % of MAX	95 % of MAX	90 % of MAX	30	AV

Policy Engine Performance Traps

Table 14 on page 65 lists the performance traps for policy engine.

Table 14: Performance Traps–Policy Engine

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
penAvgPGModProcTime	150	\$\$:Policy Engine:The average policy group modification processing time is \$D ms. This \$L the threshold of \$T ms.:\$A	200	500	1000	60	AV
penAvgICMModProcTime	151	\$\$:Policy Engine:The average interface classifier modification processing time is \$D ms. This \$L the threshold of \$T ms.:\$A	200	500	1000	60	AV
pdpErrors	152	\$\$:Policy Decision Point:During the last \$Ps, \$D errors occurred. This \$L the threshold of \$T PDP errors.:\$A	10	5	1	30	R

SRC Redirector Performance Traps

Table 15 on page 65 lists the performance traps for SRC redirector.

Table 15: Performance Traps–SRC Redirector

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
redirGBLimitReached	170	\$\$:SDX Redirector:During the last \$Ps, the global bucket limit has been reached for \$D times. This \$L the threshold of \$T times.:\$A	3	2	1	900	R

SRC-ACP Performance Traps

Table 16 on page 66 lists the performance traps for the SRC-Admission Control Plug-In (SRC-ACP) application.

Table 16: Performance Traps—SRC-ACP

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
acpHeapUsed	280	\$S:ACP:\$D % of Java VM heap is in use. This \$L the threshold of \$T %.: \$A	95 %	90 %	80 %	60	AV

JPS Performance Traps

Table 17 on page 66 lists the performance traps for the Juniper Policy Server (JPS).

Table 17: Performance Traps—JPS

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
jpsHeapUsed	250	\$\$:JPS:\$D % of Java VM heap is in use. This \$L the threshold of \$T %.: \$A	95 %	90 %	80 %	60	AV
jpsCmtsAvgSyncTime	251	\$\$:JPS:During the last \$Ps, the average time this JPS spent on CMTS synchronizations is \$Dms. This \$L the threshold of \$Tms.: \$A	900s	600s	200s	60	R
jpsCmtsAvgDecTime	252	\$\$:JPS:During the last \$Ps, the average time the CMTS connection spent on successfully completed DEC/RPT transactions is \$Dms. This \$L the threshold of \$Tms.: \$A	3s	2s	1s	60	R
jpsMsgHdlrProcTime	253	\$\$:JPS:During the last \$Ps, the average time the JPS message handler spent on message handling is \$Dms. This \$L the threshold of \$Tms.: \$A	10s	5s	2s	60	R
jpsMsgFlowProcTime	254	\$\$:JPS:During the last \$Ps, the average time the JPS message flow spent on message handling is \$Dms. This \$L the threshold of \$Tms.: \$A	30s	15s	6s	60	R
jpsMsgFlowDroppedMsgs	255	\$\$:JPS:During the last \$Ps, the number of messages dropped by a JPS message flow is \$D. This \$L the threshold of \$T.: \$A	1000	100	1	60	R

Chassis Performance Traps

Table 18 on page 67 lists the performance traps for chassis events.

Table 18: Performance Traps—Chassis

			Alarm Threshold Levels (default values)				
Trap Event	Trap ID	Text Displayed	Critical	Major	Minor	Interval(sec)	R/AV
diskUsage	302	\$\$:diskUsage: directory (juniSdxDiskPath) uses up to (juniSdxDiskUsedPercentage) of disk space. This exceeded (THRESHOLD).:RAISE	95 % of MAX	90 % of MAX	80 % of MAX	60	AV

Event Traps

Table 19 on page 67 lists the event traps.

Table 19: Event Traps

Trap Event	Trap ID	Text Displayed
saeLicenseNetworkCapacity	9	\$\$:SAE:The total number of sum-weighted line cards allocated in this SRC network is \$LINE_CARD_NUMBER (\$THRESHOLD_PERCENTAGE) % . This \$L the network ERX capacity threshold of \$T sum-weighted line cards.: \$A
saeServiceSessionLicense	11	\$\$:LICENSE SERVER:\$SERVICE_SESSIONS (\$SERVICES_PERCENTAGE %) of the available licensed service sessions are in use.: \$A
routerConnClosed	211	When juniSaeRouterUseFailOver is FALSE: <ul style="list-style-type: none"> ■ INFORMATION:SAE Router Driver:The router connection to \$juniSaeRouterClientId has been closed.:RAISE When juniSaeRouterUseFailOver is TRUE: <ul style="list-style-type: none"> ■ INFORMATION:SAE Router Driver:The router connection to \$juniSaeRouterClientId has been closed and redirected to \$juniSaeRouterFailOverIp:\$juniSaeRouterFailOverPort:RAISE
routerConnDown	212	INFORMATION:SAE Router Driver:The router connection to \$juniSaeRouterClientId went down.:RAISE
routerConnRejected	213	INFORMATION:SAE Router Driver:The router connection from \$juniSaeRouterClientId has been rejected.:RAISE
routerConnUp	210	INFORMATION:SAE Router Driver:A new router connection was established with \$juniSaeRouterClientId.:RAISE
routerConfOutOfSynch	214	When the trap is raised, the text displayed is: <ul style="list-style-type: none"> ■ INFORMATION:SAE Router Driver: The configured state of router \$juniSaeRouterClientId is out of synch with SAE. The configured action to be taken by SAE is \$configuredAction.:RAISE When the trap is cleared, the text displayed is: <ul style="list-style-type: none"> ■ INFORMATION:SAE Router Driver: The configured state of router \$juniSaeRouterClientId is successfully resynchronized with SAE.:CLEAR

Table 19: Event Traps (continued)

Trap Event	Trap ID	Text Displayed
agentStarted	110	INFORMATION:Agent:The agent has started.:RAISE
agentRestartFailed	111	CRITICAL: Agent: The agent has failed to restart after \$ATTEMPTS attempts:RAISE
agentShutdown	112	INFORMATION:Agent:The agent has shutdown.:RAISE
componentUp	114	INFORMATION:\$I: This component is up.:RAISE
componentDown	115	INFORMATION:\$I: This component is down:RAISE
dirConnected	130	INFORMATION:\$I:The directory connection has been established with \$LDAP_HOST on port \$LDAP_PORT, and has a type of \$CONNECTION_TYPE.:RAISE
dirConnectionFailure	131	CRITICAL:\$I:The directory connection with \$LDAP_HOST has failed.:RAISE
dirNotAvail	132	CRITICAL:\$I:A directory connection is not available.:RAISE
nicHostRedundStateSwitched	240	INFORMATION:NIC Host:The redundancy state of the NIC Host has switched to \$juniNicHostRedundState.:RAISE
nicHostMisconfigured	241	INFORMATION:NIC Host: The NIC Host failed to start due to misconfiguration. The error message is "\$MESSAGE".:RAISE
acpSyncCompleted	290	INFORMATION:ACP State Sync:ACP finished state sync with SAE for \$juniAcpVirtualRouterName.:RAISE
acpRedundStateSwitched	291	INFORMATION:ACP Host:The redundancy state of the ACP Host has switched to \$juniAcpRedundState.:RAISE
jpsAmConnUp	260	INFORMATION:JPS:A new application manager connection was established.:RAISE
jpsAmConnDown	261	INFORMATION:JPS:The application manager connection went down.:RAISE
jpsCmtsConnUp	262	INFORMATION:JPS:A new CMTS connection was established.:RAISE
jpsCmtsConnDown	263	INFORMATION:JPS:A CMTS connection went down.:RAISE
jdbReplicationFailure	292	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION:jdbReplicationFailure:Failed to replicate LDAP data {juniSdxjdbReplicationDirection} neighbor {juniSdxjdbNeighbor}.The latest JDB replicaion status is:{juniSdxjdbLastStatus }:RAISE <p>When the trap is cleared, the text displayed is:</p> <ul style="list-style-type: none"> INFORMATION: jdbReplicationFailure:Community directory server {juniSdxjdbNeighbor} latest update status error:CLEAR

Table 19: Event Traps (continued)

Trap Event	Trap ID	Text Displayed
systemOperatingFailure	300	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> ■ INFORMATION:System:hardware failure is found with \$juniSdxOperatingSensor on system \$juniSdxOperatingLocation:RAISE <p>When the trap is cleared, the text displayed is:</p> <ul style="list-style-type: none"> ■ INFORMATION:System:hardware failure with \$juniSdxOperatingSensor on system \$juniSdxOperatingLocation is cleared:CLEAR
diskFailure	301	<p>When the trap is raised, the text displayed is:</p> <ul style="list-style-type: none"> ■ INFORMATION:System:disk failure is found:RAISE <p>When the trap is cleared, text displayed is:</p> <ul style="list-style-type: none"> ■ INFORMATION:System:disk failure is cleared:CLEAR

Alarm State Transitions

Table 20 on page 69 lists the alarm state transitions.

Table 20: Alarm State Transitions

Last Data Threshold	Current Data Threshold	Action(s)
NONE	NONE	No action
NONE	MINOR	Raise minor event
NONE	MAJOR	Raise major event
NONE	CRITICAL	Raise critical event
MINOR	NONE	Clear minor event
MINOR	MINOR	No action
MINOR	MAJOR	Raise major event
MINOR	CRITICAL	Raise critical event
MAJOR	NONE	Clear critical event
MAJOR	MINOR	Clear major event Raise minor event
MAJOR	MAJOR	No action
MAJOR	CRITICAL	Raise critical event

Table 20: Alarm State Transitions *(continued)*

Last Data Threshold	Current Data Threshold	Action(s)	
CRITICAL	NONE	Clear critical event	
CRITICAL	MINOR	Clear critical event	Raise minor event
CRITICAL	MAJOR	Clear critical event	Raise major event
CRITICAL	CRITICAL	No action	

Part 5

Monitoring the SRC Software and the C-series Controller with the C-Web Interface and the SRC CLI

- Monitoring the SRC CLI and the C-Web Interface on page 73
- Monitoring the System (SRC CLI) on page 77
- Monitoring the System (C-Web Interface) on page 81
- Monitoring SAE Data (SRC CLI) on page 89
- Monitoring SAE Data (C-Web Interface) on page 109
- Monitoring and Troubleshooting NIC (SRC CLI) on page 133
- Monitoring the NIC (C-Web Interface) on page 143
- Monitoring NTP (SRC CLI) on page 149
- Monitoring NTP (C-Web Interface) on page 151
- Monitoring Redirect Server (SRC CLI) on page 155
- Monitoring the Redirect Server and Filtered Traffic (C-Web Interface) on page 157
- Troubleshooting Network Connectivity (SRC CLI) on page 159
- Monitoring Network Connectivity (C-Web Interface) on page 163

Chapter 11

Monitoring the SRC CLI and the C-Web Interface

- Monitoring with the SRC CLI and the C-Web Interface on page 73
- SRC Monitoring Options on page 73

Monitoring with the SRC CLI and the C-Web Interface

You can use the **show** commands available with the SRC CLI to monitor the operation and configuration of your SRC environment.

The C-Web graphical user interface (GUI) allows you to monitor the operation and configuration of your SRC environment by using a Web browser with Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.

SRC Monitoring Options

Table 21 on page 74 lists and compares the monitoring options for the C-Web interface and the SRC CLI.

Table 21: Comparison of SRC Monitoring Options

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
ACP	Admission Control Plug-In (ACP) data and statistics	<ul style="list-style-type: none"> ■ show acp backbone congestion-point congestion-point-expression ■ show acp backbone congestion-point dn ■ show acp backbone service ■ show acp edge congestion-point dn ■ show acp edge congestion-point subscriber-session-id ■ show acp edge subscriber ■ show acp remote-update congestion-point dn ■ show acp remote-update congestion-point name ■ show acp remote-update subscriber ■ show acp statistics directory ■ show acp statistics general ■ show acp statistics router
CLI	SRC CLI level and authorization data	<ul style="list-style-type: none"> ■ show cli ■ show cli authorization
Component	Installed components	<ul style="list-style-type: none"> ■ show component
Date	System date and time	<ul style="list-style-type: none"> ■ show date
Disk	System disk status	<ul style="list-style-type: none"> ■ show disk status
Interfaces	System interfaces	<ul style="list-style-type: none"> ■ show interfaces
Iptables	Filtered traffic statistics from the iptables Linux tool	<ul style="list-style-type: none"> ■ show iptables
JPS	Juniper Policy Server (JPS) data and statistics	<ul style="list-style-type: none"> ■ show jps statistics ■ show jps statistics am ■ show jps statistics am connections ■ show jps statistics cmts-locator ■ show jps statistics cmts ■ show jps statistics_cmts connections ■ show jps statistics message-handler ■ show jps statistics message-handler message-flow ■ show jps statistics process ■ show jps statistics rks

Table 21: Comparison of SRC Monitoring Options *(continued)*

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
NIC	Network information collector (NIC) component configuration data and statistics, including NIC agents, resolvers, and process	<ul style="list-style-type: none"> ■ show nic data ■ show nic data agent ■ show nic data resolver ■ show nic statistics ■ show nic statistics agent ■ show nic statistics host ■ show nic statistics process ■ show nic statistics resolver ■ show nic slot number data ■ show nic slot number statistics
NTP	Network Time Protocol (NTP) configuration data and statistics	<ul style="list-style-type: none"> ■ show ntp associations ■ show ntp statistics ■ show ntp status
Redirect server	Redirect server statistics	<ul style="list-style-type: none"> ■ show redirect server statistics
Route	Route data from the local system to a remote host	<ul style="list-style-type: none"> ■ show route

Table 21: Comparison of SRC Monitoring Options *(continued)*

C-Web Interface Monitor Option	Information Displayed	Corresponding SRC CLI Commands
SAE	SAE configuration data and statistics	<ul style="list-style-type: none"> ■ show sae interfaces ■ show sae licenses ■ show sae policies ■ show sae registered equipment ■ show sae registered login ■ show sae routers ■ show sae services ■ show sae statistics device ■ show sae statistics device common ■ show sae statistics directory ■ show sae statistics directory connections ■ show sae statistics license client ■ show sae statistics license local ■ show sae statistics license virtual-router ■ show sae statistics policy-management ■ show sae statistics process ■ show sae statistics radius ■ show sae statistics radius client ■ show sae statistics sessions ■ show sae subscribers ■ show sae subscribers dn ■ show sae subscribers ip ■ show sae subscribers login-name ■ show sae subscribers service-name ■ show sae subscribers session-id ■ show sae threads
Security	Security certificate configuration and statistics	<ul style="list-style-type: none"> ■ show security certificate
System	SRC software and C-series controller configuration data	<ul style="list-style-type: none"> ■ show configuration ■ show system boot-messages ■ show system information ■ show system ldap community ■ show system ldap server ■ show system ldap statistics ■ show system users

Chapter 12

Monitoring the System (SRC CLI)

- Viewing Information About a C-series Controller on page 77
- Viewing Information About Components Installed (SRC CLI) on page 78
- Viewing Information About Boot Messages (SRC CLI) on page 78
- Viewing Information About Security Certificates (SRC CLI) on page 80

Viewing Information About a C-series Controller

Purpose View information about a C-series controller.

Action user@host> **show system information**

System Identification

Hostname my-server
Manufacturer Juniper Networks
Product Name C-2000
Version 1.0
Serial Number 0207082006000001
UUID 48384441-5254-0030-4859-0030485977EE
Hostid e30a2e07
Software version SRC-PE Release 7.0 [A.7.0.0-151]

System Time

Current time 2007-01-02 17:29:19 EST
Uptime 15 days, 1:07
Number of active users 3
Load Averages (1m/5m/15m) 0.23/0.22/0.14

Memory

Total 15G
Free 12G

CPU Info

Number of CPU 4
CPU Model Dual Core AMD Opteron(tm) Processor 265
Clock Speed 1804.132 MHz

Disk Information

Mountpoint	Total	Used	Use%
/	2015M	956M	47%
/altroot	2015M	35M	1%
/altvar	29G	75M	0%
/boot	98M	14M	14%
/var	31G	216M	0%

Temperature

System +23 C
 CPU-1 +33 C
 CPU-2 +35 C

Fan speed

Fan-1 9375 RPM
 Fan-2 9375 RPM

Viewing Information About Components Installed (SRC CLI)

Purpose View release and status information for SRC components installed on a system.

Action user@host> **show component**

Installed Components

Name	Version	Status
cli	Release: 7.0 Build: CLI.A.7.0.0.0171	running
acp	Release: 7.0 Build: ACP.A.7.0.0.0174	disabled
jdb	Release: 7.0 Build: DIRXA.A.7.0.0.0176	running
editor	Release: 7.0 Build: EDITOR.A.7.0.0.0176	running
redir	Release: 7.0 Build: REDIR.A.7.0.0.0176	disabled
licSvr	Release: 7.0 Build: LICSVR.A.7.0.0.0179	stopped
nic	Release: 7.0 Build: GATEWAY.A.7.0.0.0170	disabled
sae	Release: 7.0 Build: SAE.A.7.0.0.0166	running
www	Release: 7.0 Build: UMC.A.7.0.0.0169	disabled
jps	Release: 7.0 Build: JPS.A.7.0.0.0172	disabled
agent	Release: 7.0 Build: SYSMAN.A.7.0.0.0174	running
webadm	Release: 7.0 Build: WEBADM.A.7.0.0.0173	disabled

Meaning Table 22 on page 78 describes the output fields for the **show component** command. Output fields are listed in the order in which they appear.

Table 22: Output Fields for show component

Field Name	Field Description
Name	Name of the component
Version	Version of the component
Status	State of the component, running or disabled

Viewing Information About Boot Messages (SRC CLI)

Purpose If you encounter system problems in a C-series controller after you start the system, you can view information about the boot process.
 View messages generated during system boot.

Action user@host> **show system boot-messages**

```

Bootdata ok (command line is ro root=/dev/vg0/root console=tty0 console=ttyS0,96
00)
Linux version 2.6.9-42.0.3.ELsmp (buildcentos@x8664-build.centos.org) (gcc versi
on 3.4.6 20060404 (Red Hat 3.4.6-3)) #1 SMP Fri Oct 6 06:28:26 CDT 2006
BIOS-provided physical RAM map:
  BIOS-e820: 0000000000000000 - 000000000009ac00 (usable)
  BIOS-e820: 000000000009ac00 - 00000000000a0000 (reserved)
  BIOS-e820: 00000000000ea070 - 0000000000100000 (reserved)
  BIOS-e820: 0000000000100000 - 00000000dffc0000 (usable)
  BIOS-e820: 00000000dffc0000 - 00000000dffc0000 (ACPI data)
  BIOS-e820: 00000000dffc0000 - 00000000dfff0000 (ACPI NVS)
  BIOS-e820: 00000000dfff0000 - 00000000e0000000 (reserved)
  BIOS-e820: 00000000fec00000 - 00000000fec86000 (reserved)
  BIOS-e820: 00000000fee00000 - 00000000fee01000 (reserved)
  BIOS-e820: 00000000ffb00000 - 0000000100000000 (reserved)
  BIOS-e820: 0000000100000000 - 0000000220000000 (usable)
ACPI: RSDP (v000 ACPIAM ) @ 0x000000000000f7760
ACPI: RSDT (v001 A M I OEMRSDT 0x03000529 MSFT 0x00000097) @ 0x00000000dffc00
0
ACPI: FADT (v002 A M I OEMFACP 0x03000529 MSFT 0x00000097) @ 0x00000000dffc020
0
ACPI: MADT (v001 A M I OEMAPIC 0x03000529 MSFT 0x00000097) @ 0x00000000dffc039
0
ACPI: OEMB (v001 A M I AMI_OEM 0x03000529 MSFT 0x00000097) @ 0x00000000dffc04
0
ACPI: DSDT (v001 DVLG2 DVLG2007 0x00000007 INTL 0x02002026) @ 0x0000000000000000
0
No NUMA configuration found
Faking a node at 0000000000000000-0000000220000000
Bootmem setup node 0 0000000000000000-0000000220000000
No mptable found.
On node 0 totalpages: 2228224
  DMA zone: 4096 pages, LIFO batch:1
  Normal zone: 2224128 pages, LIFO batch:16
  HighMem zone: 0 pages, LIFO batch:1
DMI 2.3 present.
ACPI: PM-Timer IO Port: 0x408
ACPI: Local APIC address 0xfec00000
ACPI: LAPIC (acpi_id[0x01] lapic_id[0x00] enabled)
Processor #0 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x02] lapic_id[0x06] enabled)
Processor #6 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x03] lapic_id[0x01] enabled)
Processor #1 15:4 APIC version 16
ACPI: LAPIC (acpi_id[0x04] lapic_id[0x07] enabled)
Processor #7 15:4 APIC version 16
Setting APIC routing to flat
ACPI: IOAPIC (id[0x08] address[0xfec00000] gsi_base[0])
IOAPIC[0]: apic_id 8, version 32, address 0xfec00000, GSI 0-23
ACPI: IOAPIC (id[0x09] address[0xfec10000] gsi_base[24])
IOAPIC[1]: apic_id 9, version 32, address 0xfec10000, GSI 24-4
ACPI: INT_SRC_OVR (bus 0 bus_irq 0 global_irq 2 df1 df1)
ACPI: INT_SRC_OVR (bus 0 bus_irq 9 global_irq 9 high level)
ACPI: IRQ0 used by override.
ACPI: IRQ2 used by override.
ACPI: IRQ9 used by override.
Using ACPI (MADT) for SMP configuration information
Allocating PCI resources starting at e2000000 (gap: e0000000:1ec00000)
Checking aperture...
Built 1 zonelists
Kernel command line: ro root=/dev/vg0/root console=tty0 console=ttyS0,9600

```

```

Initializing CPU#0
PID hash table entries: 4096 (order: 12, 131072 bytes)
time.c: Using 3.579545 MHz PM timer.
time.c: Detected 3200.267 MHz processor.
Console: colour VGA+ 80x25
Dentry cache hash table entries: 2097152 (order: 12, 16777216 bytes)
Inode-cache hash table entries: 1048576 (order: 11, 8388608 bytes)
Placing software IO TLB between 0x28c1000 - 0x68c1000
Memory: 8168568k/8912896k available (2106k kernel code, 0k reserved, 1297k data,
    196k init)
Calibrating delay using timer specific routine.. 6406.43 BogoMIPS (1pj=3203218)
Security Scaffold v1.0.0 initialized
SELinux: Initializing.
SELinux: Starting in permissive mode
There is already a security framework initialized, register_security failed.
selinux_register_security: Registering secondary module capability
Capability LSM initialized as secondary
Mount-cache hash table entries: 256 (order: 0, 4096 bytes)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
using mwait in idle threads.
CPU0: Initial APIC ID: 0, Physical Processor ID: 0
Using IO APIC NMI watchdog
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
CPU0: Initial APIC ID: 0, Physical Processor ID: 0
CPU0: Intel(R) Xeon(TM) CPU 3.20GHz stepping 03
per-CPU timeslice cutoff: 705.82 usecs.
task migration cache decay timeout: 1 msecs.
Booting processor 1/6 rip 6000 rsp 10006945f58
Initializing CPU#1
Calibrating delay using timer specific routine.. 6399.38 BogoMIPS (1pj=3199690)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K
CPU1: Initial APIC ID: 6, Physical Processor ID: 3
Intel(R) Xeon(TM) CPU 3.20GHz stepping 03
Booting processor 2/1 rip 6000 rsp 1000697df58
Initializing CPU#2
Calibrating delay using timer specific routine.. 6399.32 BogoMIPS (1pj=3199664)
CPU: Trace cache: 12K uops, L1 D cache: 16K
CPU: L2 cache: 2048K

```

Viewing Information About Security Certificates (SRC CLI)

Purpose	View information about security certificates that reside on the system.
Action	<pre> user@host> show security certificate web subject:CN=myhost CAcert1 subject:CN=myhost </pre>
Meaning	<p>If no security certificates reside on the system, the CLI return a message to that effect:</p> <pre> user@host> show security certificate No entity certificates in key store </pre>

Chapter 13

Monitoring the System (C-Web Interface)

- Viewing Information About the System (C-Web Interface) on page 81
- Viewing the System Date and Time (C-Web Interface) on page 82
- Viewing Information About Components Installed (C-Web Interface) on page 83
- Viewing Information About Boot Messages (C-Web Interface) on page 83
- Viewing Information About Security Certificates (C-Web Interface) on page 84
- Viewing Information About System Disk Status on page 85
- Viewing Information About the Users on the System on page 85
- Viewing Information About the Juniper Networks Database in Community Mode on page 86
- Viewing Statistics for the Juniper Networks Database on page 87
- Viewing Information About the SRC CLI (C-Web Interface) on page 87

Viewing Information About the System (C-Web Interface)

Purpose View system information.

You can view information about the SRC software, including system identification and the system time. You can also view information about the environment of the C-series controller, including memory, temperature, and fan speeds.

Action ■ Click **Monitor > System > Information**.

The Information pane displays the system information.

The screenshot shows the C-Web Interface with the 'Monitor' tab selected. The left sidebar contains a menu with the following items: ACP, CLI, Component, Date, Disk, Interfaces..., Iptables..., JPS, NIC, NTP, Redirect Server, Route..., SAE, Security, and System (highlighted in orange). The main content area displays the 'System Information' pane. The top of the pane has a header with 'System' in orange and 'Information' in black. Below this, the 'System Identification' section contains a table with the following data:

Hostname	gaspode
Manufacturer	Juniper Networks
Product Name	SDX-2000
Version	1.0
Serial Number	0207082006000003
UUID	48384441-5254-0030-4859-003048595D02
Hostid	e30a2f07
Software version	SDX-300 Release . [A.MAIN-110] (January 22, 2007 02:20)

Below the 'System Identification' section is the 'System Time' section, which contains a table with the following data:

Current time	2007-08-24 14:07:16 EDT
Uptime	76 days, 18:35
Number of active users	3
Load Averages (1m/5m/15m)	0.27/0.06/0.02

Below the 'System Time' section is the 'Memory' section, which contains a table with the following data:

Total	15G
Free	13G

Below the 'Memory' section is the 'CPU Info' section, which contains a table with the following data:

Number of CPU	4
CPU Model	Dual Core AMD Opteron(tm) Processor 265

Viewing the System Date and Time (C-Web Interface)

Purpose View the system date and time.

Action Click **Monitor > Date**.

The Date pane displays the date and time of the system.

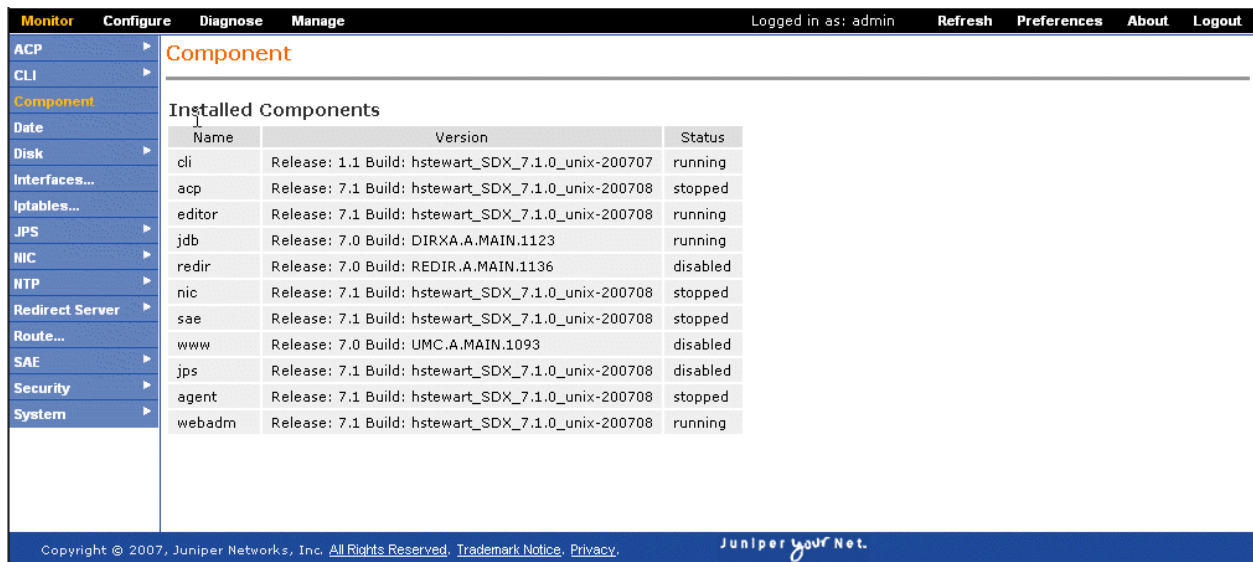


Viewing Information About Components Installed (C-Web Interface)

Purpose View the installed SRC components.

Action Click **Monitor > Component**.

The Component pane displays the status of each installed component.



Viewing Information About Boot Messages (C-Web Interface)

Purpose View messages generated during SRC software startup.

Action Click **Monitor > System > Boot Messages**.

The Boot Messages pane displays the boot messages.

Monitor		Logged in as: admin	About	Refresh	Logout
ACP	System				
CLI	Boot Messages				
Component					
Date	Fri Mar 9 10:17:24 EST 2007				
Disk	Feb 20 19:27:18 buffy genunix: [ID 936769 kern.info] dad0 is /pci@1f,0/ide@d/dad@2,0				
Interfaces...	Feb 20 19:27:18 buffy dada: [ID 365881 kern.info] <ST380011A cyl 38307 alt 2 hd 16 sec 255>				
JPS	Feb 20 19:27:19 buffy swapgeneric: [ID 308332 kern.info] root on /pci@1f,0/ide@d/disk@2,0:a fstype ufs				
NIC	Feb 20 19:27:19 buffy pcipsy: [ID 370704 kern.info] PCI-device: isa@7, ebus0				
NTP	Feb 20 19:27:19 buffy genunix: [ID 936769 kern.info] ebus0 is /pci@1f,0/isa@7				
Redirect Server	Feb 20 19:27:19 buffy ebus: [ID 521012 kern.info] su0 at ebus0: offset 0,3f8				
Route...	Feb 20 19:27:19 buffy genunix: [ID 936769 kern.info] su0 is /pci@1f,0/isa@7/serial@0,3f8				
SAE	Feb 20 19:27:19 buffy ebus: [ID 521012 kern.info] sul at ebus0: offset 0,2e8				
Security	Feb 20 19:27:19 buffy genunix: [ID 936769 kern.info] sul is /pci@1f,0/isa@7/serial@0,2e8				
System	Feb 20 19:27:19 buffy unix: [ID 987524 kern.info] cpu0: SUNW,UltraSPARC-IIe (upaid 0 impl 0x13 ver 0x33 clock 548 MHz)				
	Feb 20 19:27:20 buffy pcipsy: [ID 370704 kern.info] PCI-device: usb@a, ohci0				
	Feb 20 19:27:20 buffy genunix: [ID 936769 kern.info] ohci0 is /pci@1f,0/usb@a				
	Feb 20 19:27:22 buffy gld: [ID 944156 kern.info] dmfe0: Davicom DM9102 (v1.1): type "ether" mac address 00:03:ba:ce:d7:79				
	Feb 20 19:27:22 buffy pcipsy: [ID 370704 kern.info] PCI-device: ethernet@c, dmfe0				
	Feb 20 19:27:22 buffy genunix: [ID 936769 kern.info] dmfe0 is /pci@1f,0/ethernet@c				
	Feb 20 19:27:22 buffy gld: [ID 944156 kern.info] dmfel: Davicom DM9102 (v1.1): type "ether" mac address 00:03:ba:ce:d7:7a				
	Feb 20 19:27:22 buffy pcipsy: [ID 370704 kern.info] PCI-device: ethernet@5, dmfel				
	Feb 20 19:27:22 buffy genunix: [ID 936769 kern.info] dmfel is /pci@1f,0/ethernet@5				
	Feb 20 19:27:23 buffy genunix: [ID 454863 kern.info] dump on /dev/dsk/c0t2d0s1 size 2000 MB				
	Feb 20 19:27:24 buffy dmfe: [ID 426308 kern.info] dmfe0: PHY 1 link up 100 Mbps Full-Duplex				
	Feb 20 19:27:24 buffy dmfe: [ID 247303 kern.notice] NOTICE: dmfel: PHY 1 link down				
	Feb 20 19:27:25 buffy pseudo: [ID 129642 kern.info] pseudo-device: devinfo0				
	Feb 20 19:27:25 buffy genunix: [ID 936769 kern.info] devinfo0 is /pseudo/devinfo@0				
	Feb 20 19:27:26 buffy scsi: [ID 193665 kern.info] sd0 at uata0: target 3 lun 0				
	Feb 20 19:27:26 buffy genunix: [ID 936769 kern.info] sd0 is /pci@1f,0/ide@d/sd@3,0				
	Feb 20 19:27:26 buffy ebus: [ID 521012 kern.info] isadma0 at ebus0: offset 0,0				
	Feb 20 19:27:26 buffy pseudo: [ID 129642 kern.info] pseudo-device: fssnap0				
	Feb 20 19:27:26 buffy genunix: [ID 936769 kern.info] fssnap0 is /pseudo/fssnap@0				
	Feb 20 19:27:26 buffy pseudo: [ID 129642 kern.info] pseudo-device: winlock0				
	Feb 20 19:27:26 buffy genunix: [ID 936769 kern.info] winlock0 is /pseudo/winlock@0				
	Feb 20 19:27:27 buffy pseudo: [ID 129642 kern.info] pseudo-device: lockstat0				

Viewing Information About Security Certificates (C-Web Interface)

Purpose View messages generated during SRC software startup.

Action 1. Click **Monitor > Security > Certificate**.

The Certificate pane appears.

Monitor		Configure	Diagnose	Manage	Logged in as: admin	Refresh	Preferences	About	Logout
ACP	Security								
CLI	Certificate								
Component									
Date	Trusted <input type="checkbox"/>								
Disk	OK Reset								
Interfaces...									
Iptables...									
JPS									
NIC									
NTP									
Redirect Server									
Route...									
SAE									
Security									
System									

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper Your Net.

- To display authority certificates, select the **Trusted** check box.
- Click **OK**.

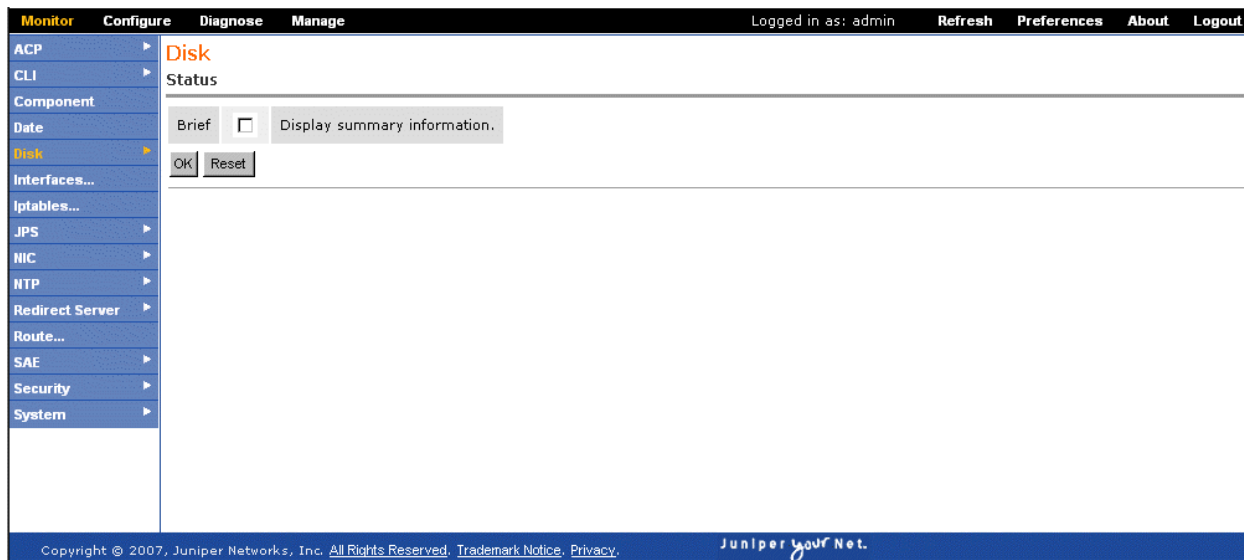
The Certificate pane displays the security certificates.

Viewing Information About System Disk Status

Purpose View information about the system disk status.

Action 1. Click **Monitor > Disk > Status**.

The Status pane appears.



2. To display a summary of the system disk status, select the **Brief** check box.
3. Click **OK**.

The Status pane displays the system disk status.

Viewing Information About the Users on the System

Purpose View information about the users on the system.

Action 1. Click **Monitor > System > Users**.

The Users pane appears.

The screenshot shows the Juniper Networks CLI interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The user is logged in as 'sleswayball'. The 'System' menu is expanded, showing options like ACP, CLI, Component, Date, Disk, Interfaces..., JPS, NIC, NTP, Redirect Server, Route..., SAE, Security, and System. The 'System' option is selected, and the 'Users' pane is displayed. The 'Brief' checkbox is checked, and the 'Use the short format' checkbox is also checked. The 'Do not show the FROM field' checkbox is unchecked. The 'OK' button is highlighted. The 'Users' pane displays a table of users:

Username	Shell	Home Directory	Group	Full Name
root	pts/6	4	telnet	menemsha
root	pts/8	3:40	bash	
root	pts/10	12	python	-0 /opt/UMC/cli/lib/fe/cl
root	pts/3	3:38	telnet	menemsha

The footer of the interface shows the copyright notice: 'Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.' and the Juniper logo.

2. To display a summary of the users, select the **Brief** check box.
3. Click **OK**.

The Users pane displays the information about the users on the system.

Viewing Information About the Juniper Networks Database in Community Mode

Purpose View information about the Juniper Networks database when it runs in community mode.

Action Click **Monitor > System > LDAP > Community**.

The LDAP/Community pane appears and displays information about the Juniper Networks database.

The screenshot shows the Juniper Networks CLI interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The user is logged in as 'sleswayball'. The 'System' menu is expanded, showing options like ACP, CLI, Component, Date, Disk, Interfaces..., JPS, NIC, NTP, Redirect Server, Route..., SAE, Security, and System. The 'System' option is selected, and the 'Ldap / Community' pane is displayed. The pane shows the message: 'JDB is not configured in community mode! There is nothing to be displayed.' The footer of the interface shows the copyright notice: 'Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.' and the Juniper logo.

Viewing Statistics for the Juniper Networks Database

Purpose View statistics for the Juniper Networks database.

Action Click **Monitor > System > LDAP > Statistics**.

The Statistics pane appears and displays local Juniper Networks database statistics.

Monitor	Configure	Diagnose	Manage	Logged in as: sleswayball	Update	Preferences	About	Logout
ACP	System							
CLI	Ldap / Statistics							
Component								
Date	Local JDB statistics							
Disk	Number of Add operations since startup	993						
Interfaces...	Number of Delete operations since startup	0						
JPS	Number of Modify operations since startup	282						
NIC	Number of Rename operations since startup	0						
NTP	Number of Read operations since startup	480933						
Redirect Server	Number of List operations since startup	93821						
Route...	Number of Subtree Search operations since startup	367916						
SAE	Number of Bind operations	18266						
Security	Number of Anonymous Bind operations since startup	18232						
System	Number of Compare operations since startup	0						
	Number of current connections	19						
	Number of all connections since startup	18266						
	Number of bind errors since startup	0						
	Number of all errors since startup	226721						

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.

Juniper your Net.

Viewing Information About the SRC CLI (C-Web Interface)

You can view information about the current user's permissions and editing level for the SRC CLI by:

- Viewing Information About the SRC CLI on page 87
- Viewing Information About SRC CLI User Permissions on page 88

Viewing Information About the SRC CLI

Purpose View information about the current user's command completion setting and editing level for the SRC CLI.

Action Click **Monitor > CLI**.

The CLI pane appears and displays the information about the CLI.

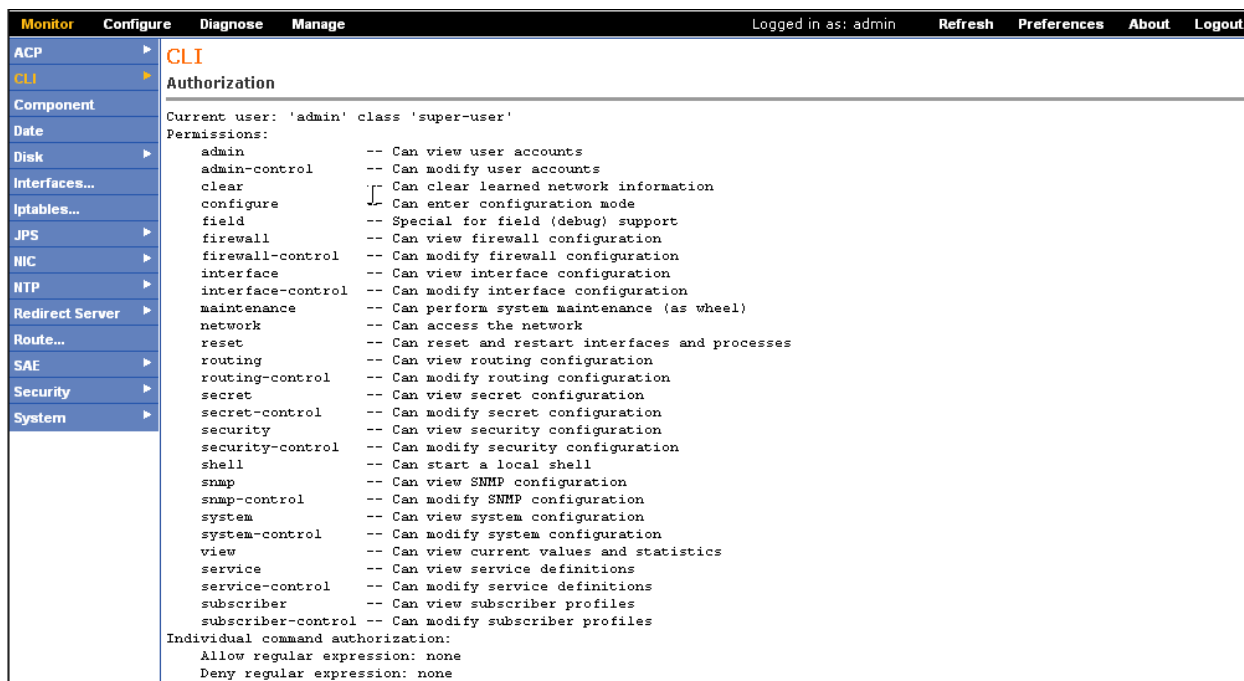


Viewing Information About SRC CLI User Permissions

Purpose To display information about the current user's permissions for the SRC CLI.

Action Click **Monitor > CLI > Authorization**.

The Authorization pane appears and displays the current user's permissions for each SRC CLI option.



Chapter 14

Monitoring SAE Data (SRC CLI)

- Viewing SAE Data with the CLI on page 89
- Viewing Information About Subscriber Sessions with the CLI on page 97
- Viewing SAE SNMP Information with the CLI on page 101

Viewing SAE Data with the CLI

You can view information about the SAE active configuration for data currently stored in the SAE server's memory.

You can view SAE data by:

- Viewing Information About the Directory Blacklist with the CLI on page 89
- Viewing Information About SAE Device Drivers with the CLI on page 89
- Viewing Information About SAE Interfaces with the CLI on page 91
- Viewing Information About SAE Licenses with the CLI on page 91
- Viewing Information About Policies on the SAE with the CLI on page 92
- Viewing Login Registrations with the CLI on page 93
- Viewing Equipment Registrations with the CLI on page 93
- Viewing Information About Services with the CLI on page 94
- Viewing Information About Threads with the CLI on page 96

Viewing Information About the Directory Blacklist with the CLI

Purpose View information about the directory blacklist configured on the SAE.

Action `user@host> show sae directory-black-list`

Viewing Information About SAE Device Drivers with the CLI

Purpose View information about SAE device drivers. Each device driver manages one logical router instance.

Action To view information about the state of SAE device drivers:

```

user@host> show sae drivers
JUNOSe Driver
Device name                default@dryad
Device type                junose
Device IP                  10.227.7.244
Local IP                   10.227.7.172
TransportRouter            default@dryad
Device version             7.2.0
Start time                 Tue Feb 13 14:18:44 EST 2007
Number of notifications    20
Number of processed added  14
Number of processed changed 0
Number of processed deleted 6
Number of provisioning attempt 30
Number of provisioning attempt failed 0
Number of outstanding decisions 0
Number of SAP              7
Number of PAP              1
  Job Queue
    Size                    0
    Age (ms)                1
    Total enqueued          28
    Total dequeued          28
    Average job time (ms) 426
  State Synchronization
    Number recovered subscriber sessions 0
    Number recovered service sessions    0
    Number recovered interface sessions   0
    Number invalid subscriber sessions    0
    Number invalid service sessions       0
    Number invalid interface sessions     0
    Background restoration start time      Tue Feb 13 14:18:49 EST 2007

    Background restoration end time        Tue Feb 13 14:18:49 EST 2007

    Number subscriber sessions restored in background 0
    Number of provisioning objects left to collect    0
    Total number of provisioning objects to collect   11
    Start time                                         Tue Feb 13 14:18:45 EST 2007

    End time                                           Tue Feb 13 14:18:47 EST 2007

    Number of synched contexts 7
    Number of post-sync jobs   6

```

To view information about the state of a particular device driver, specify all or part of the virtual router name. For JUNOS router drivers and PCMM drivers, use the format `default@routerName`.

```
user@host> show sae drivers device-name device-name
```

To view only the virtual router names for the device driver:

```
user@host> show sae drivers brief
```

```

Router Drivers
Router Name      Router Type
default@simJunos junos

```

To restrict the number of displayed results:

```
user@host> show sae drivers maximum-results maximum-results
```

Viewing Information About SAE Interfaces with the CLI

Purpose View information about SAE interfaces.

We recommend that you do not enter the **show sae interfaces** command without specifying an interface, virtual router, brief, or maximum results to filter the results. Entering the **show sae interfaces** command can generate a large quantity of results, and processing these results can place a load on the C-series controller.

Action To view information about the router interfaces:

```
user@host> show sae interfaces
```

To view information about particular router interfaces, specify all or part of the interface name.

```
user@host> show sae interfaces interface-name interface-name
```

To view information about interfaces for a particular virtual router, specify all or part of the VR name.

```
user@host> show sae interfaces virtual-router-name virtual-router-name
```

To view only the interface names:

```
user@host> show sae interfaces brief
```

To restrict the number of displayed results:

```
user@host> show sae interfaces maximum-results maximum-results
```

Viewing Information About SAE Licenses with the CLI

Purpose View the installed licenses.

Action

```
user@host> show sae licenses
SSC License Key Checker V3.0
Type of license: Pilot. Status: OK.
The following valid licenses are found:
License: cn=83ced779,ou=Licenses,o=Management,o=UMC
license.val.component = 1
license.val.customer = buffy
license.val.expiry = 2007-02-23
license.val.nodeid = 83ced779
license.val.release = 7.*
```

```
license.val.seqnum = 00555
license.val.type = pilot
license.val.userSessions = 100
```

Viewing Information About Policies on the SAE with the CLI

Purpose View policy information.

Action To view information about the policies available on the SAE:

```
user@host> show sae policies
```

To view information about particular policies, specify all or part of the policy list name:

```
user@host> show sae policies filter filter
```

For example, if you wanted to view the policy called brickwall:

```
user@host> show sae policies filter brickwall
```

Policy Group

```
Policy Group Name brickwall
Absolute ID      policyGroupName=brickwall,ou=entjunos,o=Policies,o=UMC
```

Policy Object

```
applicability both
Name          both
policyRoles   JUNOS
accountingRule false
Name          block
priority      601
ruleType      JUNOS ASP
matchDirection both
Name          all
Name          drop
Name          packet
```

To view only the policy list names for the policies:

```
user@host> show sae policies brief
```

Policies

```
ADSL-Basic
basicBod
BestEffort64
block
bod
bodVpn
both_fwr_filter
both_fwr_fwd
both_fwr_reject
brickwall
brickwall
content-provider
content-provider-tiered
```

```

custom_policer
default
default
DHCP
DocsisParameter
DownStream
dynsrcnat
eglimit
emailweb
emailweb
EntDefault
filter
More results available. Display has reached the maximum number of results.
Number of skipped results: 43

```

To restrict the number of displayed results:

```
user@host> show sae policies maximum-results maximum-results
```

Viewing Login Registrations with the CLI

Purpose View information about registered logins. You can view all login registrations, or you can view a specific registration.

Action To view information about all login registrations:

```
user@host> show sae registered login
```

To view a specific registration, specify the media access control (MAC) address for the registration that you want to display:

```
user@host> show sae registered login mac-address mac-address
```

To view only the MAC address of the registrations:

```
user@host> show sae registered login brief
```

To restrict the number of displayed results:

```
user@host> show sae registered login maximum-results maximum-results
```

Related Topics ■ For information about login registrations, see the *SRC-PE Sample Applications Guide*.

Viewing Equipment Registrations with the CLI

Purpose View information about equipment registrations. You can view all equipment registrations, or you can view a specific registration.

Action To view information about all equipment registrations:

```
user@host> show sae registered equipment
```

To view a specific registration, specify the media access control (MAC) address for the registration that you want to display:

```
user@host> show sae registered equipment mac-address mac-address
```

To view only the MAC address of the registrations:

```
user@host> show sae registered equipment brief
```

To restrict the number of displayed results:

```
user@host> show sae registered equipment maximum-results maximum-results
```

Related Topics For information about equipment registrations, see the *SRC-PE Sample Applications Guide*.

Viewing Information About Services with the CLI

Purpose View information about services available on the SAE. You can view information about all services, or about specific services.

Action To view information about the services available on the SAE:

```
user@host> show sae services
```

To view information about particular services, specify all or part of the service name:

```
user@host> show sae services filter filter
```

For example, if you wanted to view the service called BrickWall:

```
user@host> show sae services filter brickwall
```

```
Service
available      true
description    This firewall blocks all incoming and outgoing traffic.
location       l=entjunos,o=scopes,o=umc
policygroupref policyGroupName=brickwall,ou=entjunos,o=Policies,o=UMC
servicename    BrickWall
servicetype    7
sspcategory    basicFirewall
ssptype        Normal
status         2
available      true
description    This firewall blocks all incoming and outgoing traffic.
location       l=entjunosstatelessfw,o=scopes,o=umc
policygroupref policyGroupName=brickwall,ou=entjunos_statelessfw,o=Policies,o=UMC
servicename    BrickWall
servicetype    7
sspcategory    basicFirewall
ssptype        Normal
status         2
```

To view all the hidden services:

```
user@host> show sae services secret

Service
available      true
description    This firewall blocks all incoming traffic and allows only
                outgoing email and web traffic.
location       l=entjunos,o=scopes,o=umc
policygroupref policyGroupName=emailweb,ou=entjunos,o=Policies,o=UMC
servicename    EmailAndWeb
servicetype    7
sspcategory    basicFirewall
sspradiusclass EmailAndWeb
ssptype        Normal
status         2
available      true
description    This firewall blocks all incoming traffic and allows only
                outgoing email and web traffic.
location       l=entjunosstatelessfw,o=scopes,o=umc
policygroupref policyGroupName=emailweb,ou=entjunos_statelessfw,o=Policies,o=UMC
servicename    EmailAndWeb
servicetype    7
sspcategory    basicFirewall
sspradiusclass EmailAndWeb
ssptype        Normal
status         2
Service
available      true
description    This service is activated automatically when the
                subscriber is the source or destination of a network
                attack
location       l=idp-subscriber,o=scopes,o=umc
parametersubstitution captiveAddress=66.13.2.11
policygroupref policyGroupName=quarantine,ou=idp,o=Policies,o=UMC
servicename    Quarantine
servicetype    7
sspradiusclass Quarantine
ssptype        Normal
status         2
```

To view only the service names for the services:

```
user@host> show sae services brief
```

```
Services
EmailAndWeb
Quarantine
Audio-Silver
Internet-Gold
Internet-Silver
DynSrcNat
FWR_Filter_Out
StaticDestNat
PingDoSProtect
MirrorFragment
SubrIntfFragment
BrickWall
Audio-Bronze
Internet-Bronze
Limit500kbs
```

```

News
Gold_VPN
Limit1Mbs
Video-Silver
Audio-Gold
RouterFragment
1.0 Mbps
DynSrcNat
FWR_Filter_Out
StaticDestNat
PingDoSProtect
MirrorFragment
SubrIntfFragment
BrickWall
Audio-Bronze
Internet-Bronze
Limit500kbs
News
Gold_VPN
Limit1Mbs
Video-Silver
Audio-Gold
RouterFragment
1.0 Mbps
FWR_Rej_In
MirrorAggregate
Video-Bronze
More results available. Display has reached the maximum number of results.
Number of skipped results: 26

```

To restrict the number of displayed results:

```
user@host> show sae services maximum-results maximum-results
```

Viewing Information About Threads with the CLI

Purpose View information about the threads and their priority on the SAE.

Action user@host> **show sae threads**

```

Thread Group
Thread group name system
Active threads      112
Active groups       11
Max priority         10

  Thread name      Priority Daemon thread
  Reference Handler    10      true
  Finalizer            8      true
  Signal Dispatcher    9      true
  ...

Thread Group
Thread group name RKSTrackingQueue
Active threads      5
Active groups       0
Max priority         10

```

Thread name	Priority	Daemon	thread
RKSTrackingQueue-0	5	true	
RKSTrackingQueue-1	5	true	
RKSTrackingQueue-2	5	true	
RKSTrackingQueue-3	5	true	
RKSTrackingQueue-4	5	true	

Viewing Information About Subscriber Sessions with the CLI

You can list subscriber sessions by:

- Viewing General Information for Subscriber Sessions on page 97
- Viewing Information About Subscriber Sessions by DN with the CLI on page 98
- Viewing Information About Subscriber Sessions by IP Address with the CLI on page 98
- Viewing Information About Subscriber Sessions by Login Name with the CLI on page 99
- Viewing Information About Subscriber Sessions by Service Name with the CLI on page 100
- Viewing Information About Subscriber Sessions by Session ID with the CLI on page 100

Viewing General Information for Subscriber Sessions

Purpose View general information about subscriber sessions. You can view all or restricted information about all subscriber sessions.

Action To view information about all subscriber sessions:

```
user@host> show sae subscribers
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers maximum-results maximum-results
```

Viewing Information About Subscriber Sessions by DN with the CLI

Purpose View information about subscriber sessions by the DN associated with the subscriber session. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions accessible by DN:

```
user@host> show sae subscribers dn
```

To view information about particular subscriber sessions, specify all or part of the DN:

```
user@host> show sae subscribers dn filter filter
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers dn secret
user@host> show sae subscribers dn filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers dn brief
user@host> show sae subscribers dn filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers dn terse
user@host> show sae subscribers dn filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers dn maximum-results maximum-results
user@host> show sae subscribers dn filter filter maximum-results maximum-results
```

Viewing Information About Subscriber Sessions by IP Address with the CLI

Purpose View information about subscriber sessions by the IP address associated with the subscriber session.

You can list subscriber sessions by IP address for Dynamic Host Configuration Protocol (DHCP) subscribers, authenticated Point-to-Point Protocol (PPP) subscribers, and static IP subscribers who have logged in to the portal.

Action To view information about subscriber sessions accessible by IP address:

```
user@host> show sae subscribers ip
```

To view information about particular subscriber sessions, specify the IP address:

```
user@host> show sae subscribers ip filter filter
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers ip secret
user@host> show sae subscribers ip filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers ip brief
user@host> show sae subscribers ip filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers ip terse
user@host> show sae subscribers ip filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers ip maximum-results maximum-results
user@host> show sae subscribers ip filter filter maximum-results maximum-results
```

Viewing Information About Subscriber Sessions by Login Name with the CLI

Purpose View information about subscriber sessions by the subscriber login name. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions accessible by login name:

```
user@host> show sae subscribers login-name
```

To view information about particular subscriber sessions, specify all or part of the login name:

```
user@host> show sae subscribers login-name filter filter
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers login-name secret
user@host> show sae subscribers login-name filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers login-name brief
user@host> show sae subscribers login-name filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers login-name terse
user@host> show sae subscribers login-name filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers login-name maximum-results maximum-results
user@host> show sae subscribers login-name filter filter maximum-results
maximum-results
```

Viewing Information About Subscriber Sessions by Service Name with the CLI

Purpose View information about subscriber sessions that are associated with a specified service. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions activated by a subscription to an active service session:

```
user@host> show sae subscribers service-name
```

To view information about particular subscriber sessions, specify all or part of the service name:

```
user@host> show sae subscribers service-name filter filter
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers service-name secret
user@host> show sae subscribers service-name filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers service-name brief
user@host> show sae subscribers service-name filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers service-name terse
user@host> show sae subscribers service-name filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers service-name maximum-results maximum-results
user@host> show sae subscribers service-name filter filter maximum-results
maximum-results
```

Viewing Information About Subscriber Sessions by Session ID with the CLI

Purpose View information about subscriber sessions by the session ID associated with the subscriber session. You can view all or restricted information about all associated subscriber sessions.

Action To view information about subscriber sessions by session ID:

```
user@host> show sae subscribers session-id
```

To view information about particular subscriber sessions, specify all or part of the subscriber session ID:

```
user@host> show sae subscribers session-id filter filter
```

To view the subscriptions and service sessions from hidden services:

```
user@host> show sae subscribers session-id secret
user@host> show sae subscribers session-id filter filter secret
```

To view only the subscriber session information without service sessions:

```
user@host> show sae subscribers session-id brief
user@host> show sae subscribers session-id filter filter brief
```

To view the subscriber session ID, login name, and IP address:

```
user@host> show sae subscribers session-id terse
user@host> show sae subscribers session-id filter filter terse
```

To restrict the number of displayed results:

```
user@host> show sae subscribers session-id maximum-results maximum-results
user@host> show sae subscribers session-id filter filter maximum-results
maximum-results
```

Viewing SAE SNMP Information with the CLI

You can view state information that is also available through SNMP, including information about counters that describe the SAE history of activity. This information is the same as the information you can view from the SAE SNMP interface. You can monitor SNMP by:

- Viewing Statistics About the Directory with the CLI on page 102
- Viewing Statistics for Directory Connections with the CLI on page 102
- Viewing SNMP Information for Client Licenses with the CLI on page 103
- Viewing SNMP Information for Local Licenses with the CLI on page 103
- Viewing SNMP Information for Licenses on Virtual Routers with the CLI on page 104
- Viewing SNMP Information for Policies with the CLI on page 104
- Viewing SNMP Information for the SAE Server Process with the CLI on page 104
- Viewing Statistics for RADIUS Clients with the CLI on page 105
- Viewing SNMP Information for RADIUS Clients with the CLI on page 105
- Viewing SNMP Information for Routers and Devices with the CLI on page 105

- Viewing Statistics for Device Drivers with the CLI on page 106
- Viewing Statistics for Specific Device Drivers with the CLI on page 107
- Viewing Statistics for Subscriber and Service Sessions with the CLI on page 107

Viewing Statistics About the Directory with the CLI

Purpose View statistics about the directory.

Action user@host> **show sae statistics directory**

```
SNMP Statistics
Services read      51
Services written   0
Subscriptions read 0
Subscriptions written 0
Users read         0
Users written      0
```

Viewing Statistics for Directory Connections with the CLI

Purpose View information for all or specific directory connections.

Action To view statistics for directory connections:

user@host> **show sae statistics directory connections**

```
DES connection
Connection ID      FEEDBACK_DATA_MANAGER
Number of read     93
Number of write    93
Number of events sent 0
Number of events dropped 0
Average read time  2
Average write time 23
Directory host     127.0.0.1
Directory port     389
Directory type     primary
Primary restore time 83218
Event queue length 0
...

DES connection
Connection ID      ldapAuth-LdapAuthenticator
Number of read     0
Number of write    0
Number of events sent 0
Number of events dropped 0
Average read time  0
Average write time 0
Directory host     127.0.0.1
Directory port     389
Directory type     primary
Primary restore time 83200
Event queue length 0
```

To view information about particular directory connections, specify all or part of the connection ID.

```
user@host> show sae statistics directory connections filter filter
```

For example, if you wanted to view the directory connection that contained ldap in its connection ID:

```
user@host> show sae statistics directory connections filter ldap
```

DES connection	
Connection ID	ldapAuth-LdapAuthenticator
Number of read	0
Number of write	0
Number of events sent	0
Number of events dropped	0
Average read time	0
Average write time	0
Directory host	127.0.0.1
Directory port	389
Directory type	primary
Primary restore time	83608
Event queue length	0

To view only the directory connection IDs:

```
user@host> show sae statistics directory connections brief
```

Directory Connections	
FEEDBACK_DATA_MANAGER	
EQUIPMENT_DATA_MANAGER	
POM_Engine	
LICENSE_MANAGER	
SAE_ConfigMgr	
adminLdap-LdapAuthenticator	
SERVICE_DATA_MANAGER	
USER_DATA_MANAGER	
SAE_ConfigMgr(dynamicProps)	
ldapAuth-LdapAuthenticator	

Viewing SNMP Information for Client Licenses with the CLI

Purpose View SNMP information about the state of client licenses.

Action user@host> show sae statistics license client

Viewing SNMP Information for Local Licenses with the CLI

Purpose View SNMP information about the state of local licenses.

Action user@host> show sae statistics license local

Client License State	
Mode	Pilot

```

Number of licensed users 100
Number of current users  0
Expiry                   2007-02-23

```

Viewing SNMP Information for Licenses on Virtual Routers with the CLI

Purpose View SAE license information for the SRC software.

Action To view SNMP information about the state of licenses on specified virtual routers:

```
user@host> show sae statistics license virtual-router
```

To view information about the state of licenses for a particular virtual router, specify all or part of the VR name. For JUNOS router drivers and PCMM drivers, use the format `default@routerName`.

```
user@host> show sae statistics license virtual-router filter filter
```

To view only the virtual router names:

```
user@host> show sae statistics license virtual-router brief
```

Viewing SNMP Information for Policies with the CLI

Purpose View SNMP information for the policy engine, policy decision point, and the shared object repository where the policy objects are stored:

Action `user@host> show sae statistics policy-management`

```

SNMP Statistics
Average time for processing interface classifier modification 0
Average time for processing policy group modification 0
Current total number of policy groups loaded 68
Total number of default policy decisions 0
Total number of errors 0
Total number of interface classifier modifications 0
Total number of policy group modifications 0
Total number of service policy decisions 0
Up time 81107 seconds since Tue Jan 23 19:52:53
EST 2007

```

Viewing SNMP Information for the SAE Server Process with the CLI

Purpose View SNMP information for the SAE server process.

Action `user@host> show sae statistics process`

```
SNMP Statistics
```

```

Heap in use 19211 kilo bytes (2%)
Heap limit 910016 kilo bytes
Threads    96
Up time    80877 seconds since Tue Jan 23 19:51:42 EST 2007

```

Viewing Statistics for RADIUS Clients with the CLI

Purpose View SNMP statistics for RADIUS clients.

Action user@host> **show sae statistics radius**

```

SNMP Statistics
Accounting ACKs from unrecognized IP    0
Authentication ACKs from unrecognized IP 0
Radius client ID                        SAE.buffy

```

Viewing SNMP Information for RADIUS Clients with the CLI

Purpose View SNMP information for RADIUS clients. You can view information for all accounting or authentication clients, or by IP address, UDP port number, or IP address and UDP port.

Action To view SNMP information for RADIUS accounting clients:

```
user@host> show sae statistics radius client accounting
```

To view SNMP information for RADIUS authentication clients:

```
user@host> show sae statistics radius client authentication
```

To view information for a particular RADIUS client by IP address:

```

user@host> show sae statistics radius client ip-address ip-address
user@host> show sae statistics radius client accounting ip-address ip-address
user@host> show sae statistics radius client authentication ip-address ip-address

```

To view information for a particular RADIUS client by UDP port number:

```

user@host> show sae statistics radius client udp-port udp-port
user@host> show sae statistics radius client accounting udp-port udp-port
user@host> show sae statistics radius client authentication udp-port udp-port

```

To view only the RADIUS clients that were accessible by IP address and port number:

```

user@host> show sae statistics radius client brief
user@host> show sae statistics radius client accounting brief
user@host> show sae statistics radius client authentication brief

```

Viewing SNMP Information for Routers and Devices with the CLI

Purpose View SNMP information for routers and devices that the SAE manages. You can view information for all routers and devices, or for specific ones.

Action To view SNMP information for routers and devices that the SAE is managing:

```
user@host> show sae statistics device
```

To view information for a particular router, specify all or part of the VR name. For JUNOS router drivers and PCMM drivers, use the format default@routerName.

```
user@host> show sae statistics device filter filter
```

To view only the RADIUS clients that were accessible by IP address and port number:

```
user@host> show sae statistics device brief
```

Viewing Statistics for Device Drivers with the CLI

Purpose View SNMP statistics for all device drivers.

Action user@host> show sae statistics device common

SNMP Statistics

Driver type	JUNOSE COPS
Number of close requests	0
Number of connections accepted	0
Number of current connections	0
Number of open requests	0
Server address	0.0.0.0
Server port	3288
Time since last redirect	0

SNMP Statistics

Driver type	PACKETCABLE COPS
Number of close requests	0
Number of connections accepted	0
Number of current connections	0
Number of open requests	0
Server address	0.0.0.0
Server port	0
Time since last redirect	0

SNMP Statistics

Driver type	JUNOS
Number of close requests	0
Number of connections accepted	0
Number of current connections	0
Number of open requests	0
Server address	0.0.0.0
Server port	3333
Time since last redirect	0

The value of the server address can be either an IPv4 or IPv6 address, depending on the platform.

Viewing Statistics for Specific Device Drivers with the CLI

Purpose View statistics for specific router drivers or device drivers.

Action To view SNMP statistics for JUNOS router drivers:

```
user@host> show sae statistics device common junos
```

To view SNMP statistics for JUNOSe router drivers:

```
user@host> show sae statistics device common junose-cops
```

To view SNMP statistics for PCMM device drivers:

```
user@host> show sae statistics device common packetcable-cops
```

To view SNMP statistics for third-party device drivers:

```
user@host> show sae statistics device common proxy
```

For example, to view SNMP statistics for JUNOS router drivers:

```
user@host> show sae statistics device common junos
```

SNMP Statistics

Driver type	JUNOS
Number of close requests	0
Number of connections accepted	0
Number of current connections	0
Number of open requests	0
Server address	0.0.0.0
Server port	3333
Time since last redirect	0

Viewing Statistics for Subscriber and Service Sessions with the CLI

Purpose View SNMP statistics for subscriber and service sessions.

Action user@host> show sae statistics sessions

SNMP Statistics

Current service sessions	0
Current user sessions	0
Logins (includes sync. and static IP portal logins)	0
Logouts	0
Service session idle timeouts	0
Service sessions started	0
Service sessions stopped	0
Service session timeouts	0

Chapter 15

Monitoring SAE Data (C-Web Interface)

- Viewing SAE Data (C-Web Interface) on page 109
- Viewing Information About Subscriber Sessions (C-Web Interface) on page 117
- Viewing SNMP Information (C-Web Interface) on page 122

Viewing SAE Data (C-Web Interface)

You can view data currently stored in the SAE server's memory by:

- Viewing Information About the Directory Blacklist on page 109
- Viewing Information About Services on page 110
- Viewing Information About Licenses on page 111
- Viewing Information About Policies on page 111
- Viewing Information About Device Drivers on page 112
- Viewing Information About Interfaces on page 113
- Viewing Equipment Registrations on page 114
- Viewing Login Registrations on page 115
- Viewing Information About Threads on page 116

Viewing Information About the Directory Blacklist

Purpose View information about the directory blacklist configured on the SAE.

Action 1. Click **Monitor > SAE > Directory Blacklist**.

The Directory Blacklist pane appears.

Monitor Configure Diagnose Manage Logged in as: admin Refresh Preferences About Logout

ACP CLI Component Date Disk Interfaces... Iptables... JPS NIC NTP Redirect Server Route... **SAE** Security System

SAE
Directory Blacklist

Slot Display SAE information for a specified slot.
Value: Currently the chassis has only one slot. The valid value is 0.
Default: 0

OK Reset

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper your Net.

- In the Slot box, enter the number of the slot for which you want to display directory blacklist information.

The Directory Blacklist pane displays the directory blacklist information.

Viewing Information About Services

Purpose View information about the services available on the SAE.

Action 1. Click **Monitor > SAE > Services**.

The Services pane appears.

Monitor Configure Diagnose Manage Logged in as: admin Refresh Preferences About Logout

ACP CLI Component Date Disk Interfaces... Iptables... JPS NIC NTP Redirect Server Route... **SAE** Security System

SAE
Services

Maximum Results	<input type="text"/>	Number of results to be displayed. Legal range: 1..INF Default: 25
Service Name	<input type="text"/>	Name of service. Value: All or part of the service name Default: No value
Secret	<input type="checkbox"/>	Display subscriber sessions and service sessions for hidden services. Default: Disabled
Slot	<input type="text"/>	Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0. Default: 0
Style	<input type="text"/>	Output style Choices: brief: Display only service names Default: Detail

OK Reset

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper your Net.

- In the Maximum Results box, enter the maximum number of results that you want to receive.

3. In the Service Name box, enter a full or partial service name for which you want to display information, or leave the box blank to display all services.
4. Select the **Secret** check box to set a flag indicating that secret services are displayed.
5. In the Slot box, enter the number of the slot for which you want to display services information.
6. Select an output style from the Style list.
7. Click **OK**.

The Services pane displays the status of the services running on the SAE.

Viewing Information About Licenses

Purpose View information about licenses.

Action 1. Click **Monitor > SAE > Licenses**.

The Licenses pane appears.

The screenshot shows the Juniper C-Web Interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The 'Monitor' tab is selected. On the left, a sidebar menu shows 'ACP', 'CLI', 'Component', 'Date', 'Disk', 'Interfaces...', 'Iptables...', 'JPS', 'NIC', 'NTP', 'Redirect Server', 'Route...', 'SAE' (highlighted), 'Security', and 'System'. The main content area is titled 'SAE Licenses'. It features a 'Slot' input field with the value '0'. To the right of the input field, a text box states: 'Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0. Default: 0'. Below the input field are 'OK' and 'Reset' buttons. The footer contains copyright information for Juniper Networks, Inc. (© 2007) and the Juniper logo.

2. In the Slot box, enter the number of the slot for which you want to display license information.
3. Click **OK**.

The Licenses pane displays license information.

Viewing Information About Policies

Purpose View information about the policies available on the SAE.

Action 1. Click **Monitor > SAE > Policies**.

The Policies pane appears.

The screenshot shows the 'SAE Policies' configuration pane. On the left is a navigation menu with items: ACP, CLI, Component, Date, Disk, Interfaces..., Iptables..., JPS, NIC, NTP, Redirect Server, Route..., SAE (highlighted), Security, and System. The main area is titled 'SAE Policies' and contains four configuration rows:

Policy Group	<input type="text"/>	Name of a policy group. <i>Value:</i> All or part of the policy group name <i>Default:</i> No value
Maximum Results	<input type="text"/>	Number of results to be displayed. <i>Legal range:</i> 1..INF <i>Default:</i> 25
Slot	<input type="text"/>	Display SAE information for a specified slot. <i>Value:</i> Currently the chassis has only one slot. The valid value is 0. <i>Default:</i> 0
Style	<input type="text" value="detail"/>	Output style. <i>Choices:</i> brief: Display only policy group names <i>Default value:</i> detail

At the bottom of the configuration area are 'OK' and 'Reset' buttons. The footer of the interface includes copyright information for Juniper Networks, Inc. (2007) and the slogan 'Juniper your Net.'

2. In the Policy Group box, enter a full or partial policy name for which you want to display information, or leave the box blank to display all policies.
3. In the Maximum Results box, enter the maximum number of results that you want to receive.
4. In the Slot box, enter the number of the slot for which you want to display policy information.
5. Select an output style from the Style list.
6. Click **OK**.

The Policies pane displays the status of the policies configured on the SAE.

Viewing Information About Device Drivers

Purpose View information about the device drivers available on the SAE.

- Action** 1. Click **Monitor > SAE > Drivers**.

The Drivers pane appears.

2. In the Device Name box, enter a full or partial device driver name for which you want to display information, or leave the box blank to display all devices.

For JUNOSe router drivers, use the format:

< virtual router name > @ < router name >

For JUNOS router drivers and PCMM drivers, use the format:

default@<router name>

3. In the Maximum Results box, enter the maximum number of results that you want to receive.
4. In the Slot box, enter the number of the slot for which you want to display device information.
5. Select an output style from the Style list.
6. Click **OK**.

The Drivers pane displays the status of the devices running on the SAE.

Viewing Information About Interfaces

Purpose View information about the interfaces available on the router.

Action 1. Click **Monitor > SAE > Interfaces**.

The Interfaces pane appears.

Field	Description	Value	Legal range	Default
Interface Name	Name of router interface.	All or part of the interface name		No value
Maximum Results	Number of results to be displayed.		1..INF	25
Slot	Display SAE information for a specified slot.	Currently the chassis has only one slot. The valid value is 0.		0
Style	Output style.	Choices: brief: Display only interface names		Detail
Virtual Router	Name of virtual router.	All or part of the virtual router name		No value

- In the Interface Name box, enter the name of the router interface for which you want to display information. or leave the box blank to display information about all router interfaces.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- In the Slot box, enter the number of the slot for which you want to display interface information.
- Select an output style from the Style list.
- In the Virtual Router box, enter the name of the virtual router for which you want to display interfaces, or leave the box blank to display information for all virtual routers.
- Click **OK**.

The Interfaces pane displays the interfaces available on the router.

Viewing Equipment Registrations

Purpose You can view all equipment registrations, or you can view a specific registration.

Action To view information about equipment registrations.

1. Click **Monitor > SAE > Registered > Equipment**.

The Registered/Equipment pane appears.

Monitor		Configure	Diagnose	Manage	Logged in as: admin	Refresh	Preferences	About	Logout					
ACP	CLI	Component	Date	Disk	Interfaces...	Iptables...	JPS	NIC	NTP	Redirect Server	Route...	SAE	Security	System
SAE Registered / Equipment														
Mac Address		<input type="text"/>			MAC address of equipment registrations. <i>Value:</i> MAC address in the format xx:xx:xx:xx:xx:xx <i>Default:</i> No value									
Maximum Results		<input type="text"/>			Number of results to be displayed. <i>Legal range:</i> 1..INF <i>Default:</i> 25									
Slot		<input type="text"/>			Display SAE information for a specified slot. <i>Value:</i> Currently the chassis has only one slot. The valid value is 0. <i>Default:</i> 0									
Style		<input type="text"/>			Output style. <i>Choices:</i> brief: Display only MAC address of registered equipment <i>Default:</i> Detail									
OK		Reset												

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper Your Net.

2. In the MAC Address box, enter a MAC address that specifies the equipment registrations that you want to display.

Use the format:

xx:xx:xx:xx:xx:xx

3. In the Maximum Results box, enter the maximum number of results that you want to receive.
4. In the Slot box, enter the number of the slot for which you want to display equipment registration information.
5. Select an output style from the Style list.
6. Click **OK**.

The Registered/Equipment pane displays information about the equipment registrations.

Related Topics ■ For information about login and equipment registrations, see the *SRC-PE Sample Applications Guide*.

Viewing Login Registrations

Purpose You can view all login registrations, or you can view a specific registration.

Action To view information about login registrations:

1. Click **Monitor > SAE > Registered > Login**.

The Registered/Login pane appears.

Field	Description	Value	Legal range	Default
Mac Address	MAC address of login registrations.	MAC address in the format xx:xx:xx:xx:xx:xx		No value
Maximum Results	Number of results to be displayed.		1..INF	25
Slot	Display SAE information for a specified slot.	Currently the chassis has only one slot. The valid value is 0.		0
Style	Output style	Choices: brief: Display only MAC address of login registrations		Detail

2. In the MAC Address box, enter a MAC address that specifies the login registrations that you want to display.

Use the format:

xx:xx:xx:xx:xx:xx

3. In the Maximum Results box, enter the maximum number of results that you want to receive.
4. In the Slot box, enter the number of the slot for which you want to display login registration information.
5. Select an output style from the Style list.
6. Click **OK**.

The Registered/Login pane displays information about the login registrations.

Related Topics ■ For information about login and equipment registrations, see the *SRC-PE Sample Applications Guide*.

Viewing Information About Threads

Purpose View information about the threads and their priority on the SAE.

- Action**
1. Click **Monitor > SAE > Threads**.

The Threads pane appears.

2. In the Slot box, enter the number of the slot for which you want to display thread information.
3. Click **OK**.

The Threads pane displays information about threads.

Viewing Information About Subscriber Sessions (C-Web Interface)

You can list subscriber sessions by the distinguished name (DN) of the subscriber entry in the directory, by login name, or by session ID. You can also list subscriber sessions by IP address for Dynamic Host Configuration Protocol (DHCP) subscribers, authenticated Point-to-Point Protocol (PPP) subscribers, and static IP subscribers who are being managed by the SAE.

You can list subscriber sessions by:

- Viewing Information About Subscriber Sessions by DN on page 117
- Viewing Information About Subscribers by IP Address on page 118
- Viewing Information About Subscriber Sessions by Login Name on page 119
- Viewing Information About Subscriber Sessions by Service Name on page 120
- Viewing Information About Subscriber Sessions by Session ID on page 121

Viewing Information About Subscriber Sessions by DN

Purpose View information about subscriber sessions by DN.

Action 1. Click **Monitor > SAE > Subscribers > DN**.

The Subscribers/DN pane appears.

Field	Description	Value	Legal range	Default
Subscriber DN	DN of the subscribers.	All or part of the subscriber DN		No value
Maximum Results	Number of results to be displayed.		1..INF	25
Secret	Display subscriber sessions and service sessions for hidden services.	<input type="checkbox"/>		Disabled
Slot	Display SAE information for a specified slot.			0
Style	Output style			Detail

Choices:
 brief: Display only subscriber sessions
 terse: Display subscriber session ID, login name, and IP address
 Default: Detail

- In the Subscriber DN box, enter a full or partial subscriber DN for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/DN pane displays information about subscriber sessions.

Viewing Information About Subscribers by IP Address

Purpose View information about subscriber sessions by IP address.

Action 1. Click **Monitor > SAE > Subscribers > IP**.

The Subscribers/IP pane appears.

Monitor		Configure	Diagnose	Manage	Logged in as: admin	Refresh	Preferences	About	Logout
ACP	SAE								
CLI	Subscribers / IP								
Component									
Date	IP Address	<input type="text"/>	IP address of subscriber sessions. <i>Value:</i> All or part of the subscriber IP address <i>Default:</i> No value						
Disk	Maximum Results	<input type="text"/>	Number of results to be displayed. <i>Legal range:</i> 1..INF <i>Default:</i> 25						
Interfaces...	Secret	<input type="checkbox"/>	Display subscriber sessions and service sessions for hidden services. <i>Default:</i> Disabled						
Iptables...	Slot	<input type="text"/>	Display SAE information for a specified slot. <i>Value:</i> Currently the chassis has only one slot. The valid value is 0. <i>Default:</i> 0						
JPS	Style	<input type="text" value="Detail"/>	Output style <i>Choices:</i> brief: Display only subscriber sessions terse: Display subscriber session ID, login name, and IP address <i>Default:</i> Detail						
NIC	<input type="button" value="OK"/> <input type="button" value="Reset"/>								
NTP									
Redirect Server									
Route...									
SAE									
Security									
System									

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice](#), [Privacy](#).

Juniper Your Net.

- In the IP Address box, enter a full or partial IP address for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/IP pane displays information about subscriber sessions.

Viewing Information About Subscriber Sessions by Login Name

Purpose View information about subscriber sessions by login name.

Action 1. Click **Monitor > SAE > Subscribers > Login Name**.

The Subscribers/Login Name pane appears.

Field	Description	Value	Legal range	Default
Login Name	Login name of subscriber sessions.	All or part of the subscriber login name		No value
Maximum Results	Number of results to be displayed.		1..INF	25
Secret	Display subscriber sessions and service sessions for hidden services.	<input type="checkbox"/>		Disabled
Slot	Display SAE information for a specified slot.			0
Style	Output style			Detail

Choices:
 brief: Display only subscriber sessions
 terse: Display subscriber session ID, login name, and IP address
 Default: Detail

- In the Login Name box, enter a full or partial login name for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/Login Name pane displays information about subscriber sessions.

Viewing Information About Subscriber Sessions by Service Name

Purpose View information about subscriber sessions by service name.

Action 1. Click **Monitor > SAE > Subscribers > Service Name**.

The Subscribers/Service Name pane appears.

Component	Configuration	Description
Service Name	<input type="text"/>	Service name of subscriber sessions. <i>Value:</i> All or part of the service name <i>Default:</i> No value
Maximum Results	<input type="text"/>	Number of results to be displayed. <i>Legal range:</i> 1..INF <i>Default:</i> 25
Secret	<input type="checkbox"/>	Display subscriber sessions and service sessions for hidden services. <i>Default:</i> Disabled
Slot	<input type="text"/>	Display SAE information for a specified slot. <i>Value:</i> Currently the chassis has only one slot. The valid value is 0. <i>Default:</i> 0
Style	<input type="text"/>	Output style <i>Choices:</i> brief: Display only subscriber sessions terse: Display subscriber session ID, login name, and IP address <i>Default:</i> Detail

OK Reset

- In the Service Name box, enter a full or partial service name for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/Service Name pane displays information about subscriber sessions.

Viewing Information About Subscriber Sessions by Session ID

Purpose View information about subscriber sessions by session ID.

Action 1. Click **Monitor > SAE > Subscribers > Session ID**.

The Subscribers/Session ID pane appears.

Field	Description	Value	Legal range	Default
Session ID	ID of subscriber sessions.	All or part of the subscriber session ID		No value
Maximum Results	Number of results to be displayed.		1..INF	25
Secret	Display subscriber sessions and service sessions for hidden services.	<input type="checkbox"/>		Disabled
Slot	Display SAE information for a specified slot.			0
Style	Output style			Detail

- In the Session ID box, enter a full or partial session ID name for which you want to display information, or leave the box blank to display all subscriber sessions.
- In the Maximum Results box, enter the maximum number of results that you want to receive.
- Select the **Secret** check box to set a flag indicating that subscriptions and service sessions from hidden services are displayed.
- In the Slot box, enter the number of the slot for which you want to display subscriber session information.
- Select an output style from the Style list.
- Click **OK**.

The Subscribers/Session ID pane displays information about subscriber sessions.

Viewing SNMP Information (C-Web Interface)

You can use the C-Web interface to view SNMP statistics for the SAE configuration by:

- Viewing SNMP Statistics for the Directory on page 123
- Viewing SNMP Statistics for Directory Connections on page 123
- Viewing SNMP Statistics for Client Licenses on page 124
- Viewing SNMP Statistics for Licenses by Device on page 125
- Viewing SNMP Statistics for Local Licenses on page 126
- Viewing SNMP Statistics About Policies on page 127

- Viewing SNMP Statistics About Server Processes on page 128
- Viewing SNMP Statistics About RADIUS on page 128
- Viewing SNMP Statistics About RADIUS Clients on page 129
- Viewing SNMP Statistics for Devices on page 130
- Viewing SNMP Statistics for Specific Devices on page 131
- Viewing SNMP Statistics for Subscriber Sessions and Service Sessions on page 131

Viewing SNMP Statistics for the Directory

Purpose View SNMP statistics for the directory.

Action 1. Click **Monitor > SAE > Statistics > Directory**.

The Statistics/Directory pane appears.

2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for the directory.
3. Click **OK**.

The Statistics/Directory pane displays statistics for the directory.

Viewing SNMP Statistics for Directory Connections

Purpose View SNMP statistics for directory connections.

Action 1. Click **Monitor > SAE > Statistics > Directory > Connections**.

The Statistics/Directory/Connections pane appears.

2. In the Connection ID box, enter a full or partial connection ID for which you want to display information, or leave the box blank to display all SNMP statistics for all directory connections.
3. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for directory connections.
4. Select an output style from the Style list.
5. Click **OK**.

The Statistics/Connections pane displays statistics for directory connections.

Viewing SNMP Statistics for Client Licenses

Purpose View SNMP statistics for client licenses.

Action 1. Click **Monitor > SAE > Statistics > License > Client**.

The Statistics/License/Client pane appears.

Monitor Configure Diagnose Manage Logged in as: admin Refresh Preferences About Logout

ACP CLI Component Date Disk Interfaces... Iptables... JPS NIC NTP Redirect Server Route... **SAE** Security System

Statistics / License / Client

Slot Display SAE information for a specified slot.
Value: Currently the chassis has only one slot. The valid value is 0.
Default: 0

OK Reset

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper your Net.

2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for client licenses.
3. Click **OK**.

The Statistics/License/Client pane displays statistics for client licenses.

Viewing SNMP Statistics for Licenses by Device

Purpose View SNMP statistics for licenses by device.

Action 1. Click **Monitor > SAE > Statistics > License > Device**.

The Statistics/License/Device pane appears.

Monitor **Configure** **Diagnose** **Manage** Logged in as: admin **Refresh** **Preferences** **About** **Logout**

ACP **CLI** **Component** **Date** **Disk** **Interfaces...** **Iptables...** **JPS** **NIC** **NTP** **Redirect Server** **Route...** **SAE** **Security** **System**

SAE
Statistics / License / Device

Device Name

Slot

Style

OK Reset

Name of a device.
Value: All or part of the device name.

- For JUNOS router drivers, use the format virtualRouterName@routerName.
- For JUNOS router drivers and PCMM drivers, use the format default@routerName.

Default: No value

Display SAE information for a specified slot.
Value: Currently the chassis has only one slot. The valid value is 0.
Default: 0

Output style
Choices:
brief: Display only device names
Default: Detail

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper Your Net.

- In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display SNMP statistics for all devices.

For JUNOS router drivers, use the format:

<virtual router name>@<router name>

For JUNOS router drivers and PCMM drivers, use the format:

default@<router name>

- In the Slot box, enter the number of the slot for which you want to display SNMP statistics for device licenses.
- Select an output style from the Style list.
- Click **OK**.

The Statistics/License/Device pane displays statistics for virtual router licenses.

Viewing SNMP Statistics for Local Licenses

Purpose View SNMP statistics for local licenses.

Action 1. Click **Monitor > SAE > Statistics > License > Local**.

The Statistics/License/Local pane appears.

The screenshot shows the Juniper C-Web Interface with the 'Monitor' tab selected. The left sidebar contains a tree view with 'SAE' highlighted. The main content area displays the 'Statistics / License / Local' pane. At the top, there is a 'Slot' input box with a value of '0'. To the right of the input box, a text box contains the following information: 'Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0. Default: 0'. Below the input box are 'OK' and 'Reset' buttons. The footer of the interface shows the copyright notice 'Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.' and the Juniper logo.

2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for local licenses.
3. Click **OK**.

The Statistics/License/Local pane displays statistics for local licenses.

Viewing SNMP Statistics About Policies

Purpose View SNMP statistics about policies.

Action Click **Monitor > SAE > Statistics > Policy Management**.

The Statistics/Policy Management pane appears.

The screenshot shows the Juniper C-Web Interface with the 'Monitor' tab selected. The left sidebar contains a tree view with 'SAE' highlighted. The main content area displays the 'Statistics / Policy Management' pane. At the top, there is a 'Slot' input box with a value of '0'. To the right of the input box, a text box contains the following information: 'Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0. Default: 0'. Below the input box are 'OK' and 'Reset' buttons. The footer of the interface shows the copyright notice 'Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.' and the Juniper logo.

1. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for policies.
2. Click **OK**.

The Statistics/Policy Management pane displays statistics for policies.

Viewing SNMP Statistics About Server Processes

Purpose View SNMP statistics about server processes.

Action 1. Click **Monitor > SAE > Statistics > Process**.

The Statistics/Process pane appears.

The screenshot shows the Juniper Networks GUI. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The user is logged in as 'admin'. There are links for 'Refresh', 'Preferences', 'About', and 'Logout'. The left sidebar lists various components: ACP, CLI, Component, Date, Disk, Interfaces..., Iptables..., JPS, NIC, NTP, Redirect Server, Route..., SAE, Security, and System. The main pane is titled 'SAE Statistics / Process'. It contains a 'Slot' input box with a value of 0 and an 'OK' button. A tooltip explains that the valid value is 0 and the default is 0. The bottom of the page shows the copyright notice for Juniper Networks, Inc. and the Juniper logo.

2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for server processes.
3. Click **OK**.

The Statistics/Process pane displays statistics for server processes.

Viewing SNMP Statistics About RADIUS

Purpose View SNMP statistics about RADIUS.

Action 1. Click **Monitor > SAE > Statistics > RADIUS**.

The Statistics/RADIUS pane appears.

2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for RADIUS.
3. Click **OK**.

The Statistics/RADIUS pane displays statistics for RADIUS.

Viewing SNMP Statistics About RADIUS Clients

Purpose View SNMP statistics about RADIUS clients.

Action 1. Click **Monitor > SAE > Statistics > RADIUS > Client**.

The Statistics/RADIUS/Client pane appears.

2. Select a client type from the Client Type list:

- accounting—Displays RADIUS accounting information
 - authentication—Displays RADIUS client authentication information
3. In the IP Address box, enter the client IP address to display SNMP information for a specific RADIUS client, or leave the box blank to display SNMP information for all RADIUS clients.
 4. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for RADIUS clients.
 5. Select an output style from the Style list.
 6. In the UDP Port box, enter a port number to display SNMP information for a specific RADIUS client, or leave the box blank to display SNMP information for all RADIUS clients.
 7. Click **OK**.

The Statistics/RADIUS/Client pane displays statistics for RADIUS clients.

Viewing SNMP Statistics for Devices

Purpose View SNMP statistics about devices.

Action 1. Click **Monitor > SAE > Statistics > Device**.

The Statistics/Device pane appears.

Monitor **Configure** **Diagnose** **Manage** Logged in as: admin **Refresh** **Preferences** **About** **Logout**

ACP **CLI** **Component** **Date** **Disk** **Interfaces...** **Iptables...** **JPS** **NIC** **NTP** **Redirect Server** **Route...** **SAE** **Security** **System**

SAE
Statistics / Device

Device Name Name of a device.
Value: All or part of the device name.

- For JUNOS router drivers, use the format virtualRouterName@routerName.
- For JUNOS router drivers and PCMM drivers, use the format default@routerName.

Slot Display SAE information for a specified slot.
Value: Currently the chassis has only one slot. The valid value is 0.
Default: 0

Style Output style
Choices:
brief: Display only device names
Default: Detail

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. [Trademark Notice](#). [Privacy](#). **Juniper your Net.**

2. In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display all devices.
3. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for devices.
4. Select an output style from the Style list.
5. Click **OK**.

The Statistics/Device pane displays statistics for all devices.

Viewing SNMP Statistics for Specific Devices

Purpose View SNMP statistics about specific devices.

Action 1. Click **Monitor > SAE > Statistics > Device > Common**.

The Statistics/Device/Common pane appears.

Monitor Configure Diagnose Manage Logged in as: admin Refresh Preferences About Logout

ACP CLI Component Date Disk Interfaces... Iptables... JPS NIC NTP Redirect Server Route... **SAE** Security System

SAE
Statistics / Device / Common

Device Name	<input type="text"/>	<p>Name of a device. <i>Value:</i> All or part of the device name.</p> <ul style="list-style-type: none"> For JUNOS router drivers, use the format <code>virtualRouterName@routerName</code>. For JUNOS router drivers and PCMM drivers, use the format <code>default@routerName</code>. <p><i>Default:</i> No value</p>
Slot	<input type="text"/>	<p>Display SAE information for a specified slot. <i>Value:</i> Currently the chassis has only one slot. The valid value is 0. <i>Default:</i> 0</p>
Type	<input type="text"/>	<p>Display SNMP statistics for a specified device driver type. <i>Choices:</i> junos: Display SNMP statistics for JUNOS router drivers junose-cops: Display SNMP statistics for JUNOS router drivers packetcable-cops: Display SNMP statistics for PCMM device drivers proxy: Display SNMP statistics for third-party drivers <i>Default:</i> No value</p>

OK Reset

Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy. Juniper your Net.

- In the Device Name box, enter a full or partial device name for which you want to display information, or leave the box blank to display all devices.
- In the Slot box, enter the number of the slot for which you want to display SNMP statistics for specific devices.
- Select a device type from the Type list:
 - junos—Displays SNMP statistics for JUNOS router drivers
 - junose-cops—Displays SNMP statistics for JUNOS router drivers
 - packetcable-COPS—Displays SNMP statistics for PCMM device drivers
 - proxy—Displays SNMP statistics for third-party drivers
- Click **OK**.

The Statistics/Device/Common pane displays statistics for the specified device.

Viewing SNMP Statistics for Subscriber Sessions and Service Sessions

Purpose View SNMP statistics about subscriber sessions and service sessions.

Action 1. Click **Monitor > SAE > Statistics > Sessions**.

The Statistics/Sessions pane displays statistics for subscriber sessions and service sessions.

The screenshot shows the Juniper SRC 3.0.x web interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The user is logged in as 'admin'. The main content area is titled 'SAE Statistics / Sessions'. On the left is a sidebar menu with options: ACP, CLI, Component, Date, Disk, Interfaces..., Iptables..., JPS, NIC, NTP, Redirect Server, Route..., SAE (highlighted), Security, and System. The main pane contains a 'Slot' input box with a text description: 'Display SAE information for a specified slot. Value: Currently the chassis has only one slot. The valid value is 0. Default: 0'. Below the input box are 'OK' and 'Reset' buttons. The footer shows the copyright notice for Juniper Networks, Inc. and the Juniper logo.

2. In the Slot box, enter the number of the slot for which you want to display SNMP statistics for specific devices.
3. Click **OK**.

The Statistics/Sessions pane displays statistics for subscriber sessions and service sessions.

Chapter 16

Monitoring and Troubleshooting NIC (SRC CLI)

- SRC CLI Commands to View Statistics About NIC Operations on page 133
- Viewing Statistics for the NIC Process on page 134
- Viewing Statistics for a NIC Host on page 134
- Viewing Statistics for NIC Resolvers on page 135
- Viewing Statistics for NIC Agents on page 136
- SRC CLI Commands to View NIC Resolution Data on page 137
- Viewing Data for NIC Resolvers on page 137
- Viewing Data for NIC Agents on page 138
- Troubleshooting NIC Data Resolution on page 140

SRC CLI Commands to View Statistics About NIC Operations

You can view statistics for the NIC process and for various NIC components. Table 23 on page 133 lists the commands you use to view NIC statistics.

Table 23: Commands to Display NIC Statistics

Command	Output Displayed
<code>show nic statistics</code>	All NIC statistics. The output for this command includes the output for the other <code>show nic statistics</code> commands.
<code>show nic statistics agen t</code>	NIC statistics for agents.
<code>show nic statistics hos t</code>	NIC statistics for a NIC host.
<code>show nic statistics proces s</code>	NIC statistics for the NIC process.
<code>show nic statistics resolver</code>	NIC statistics for resolvers.
<code>show nic statistics slot</code>	All NIC statistics for a specified slot. The output for this command includes the output for the <code>show nic statistics agent</code> , <code>show nic statistics host</code> , <code>show nic statistics process</code> , and <code>show nic statistics resolver</code> commands.

Viewing Statistics for the NIC Process

Purpose View statistics for the NIC process.

Action `user@host> show nic statistics process`

Component Statistics

```
Component Name process
Heap in use    456194 bytes (87%)
Heap limit     524288 bytes
Threads       42
Up time       747848 seconds since Wed Jan 31 19:35:57 EST 2007
```

Meaning Table 24 on page 134 describes the output fields for the `show nic statistics process` command. Output fields are listed in the order in which they appear.

Table 24: Output Fields for `show nic statistics process`

Field Name	Field Description
Component name	Name of component—process indicates the NIC process.
Heap in use	Heap size allocated by the Java Virtual Machine. The percentage indicates the percentage of the heap in use. We recommend that if the percent in use is more than 90 % additional heap be allocated for the NIC.
Heap limit	Size of Java heap configured for the NIC.
Threads	Number of threads in use.
Up time	Length of time NIC has been running on the system. Includes the date and time at which NIC was last started.

Viewing Statistics for a NIC Host

Purpose View statistics for a NIC host.

Action `user@host> show nic statistics host`

Component Statistics

```
Component Name /hosts
Number of Components Restart 0
Number of No Match Resolutions 0
Number of Resolution Errors 0
Number of Resolutions 0
```

Meaning Table 25 on page 135 describes the output fields for the `show nic statistics host` command. Output fields are listed in the order in which they appear.

Table 25: Output Fields for show nic statistics test

Field Name	Field Description
Component name	Name of component—/hosts indicates NIC host. A specific host has the format /hosts/ <i>hostname</i> .
Number of Components Restart	Number of NIC resolvers and agents that have restarted in the host.
Number of No Match Resolutions	Number of resolution requests that did not return data.
Number of Resolution Errors	Number of errors encountered when processing resolutions requests.
Number of Resolutions	Number of successful data resolutions; for example, the SAE reference for a specified IP address, the login name for a specified IP address, or the SAE reference for a specified login name.

Viewing Statistics for NIC Resolvers

Purpose View statistics for NIC resolvers.

To interpret the statistics for NIC resolvers, make sure that you have a good understanding of the NIC resolutions process.

See Overview of the NIC Resolution Process.

Action user@host> **show nic statistics resolver**

Component Statistics

```
Component Name      /realms/login/A1
Number of Data Sources  0
Resolver Size       0
```

Component Statistics

```
Component Name      /realms/login/B1
Number of Data Sources  1
Resolver Size       0
```

Component Statistics

```
Component Name      /realms/login/C1
Number of Data Sources  1
Resolver Size      2140
```

Component Statistics

```
Component Name      /realms/login/D1
Number of Data Sources  2
Resolver Size       0
```

Meaning Table 26 on page 136 describes the output fields for the **show nic statistics resolver** command. Output fields are listed in the order in which they appear.

Table 26: Output Fields for show nic statistics resolver

Field Name	Field Description
Component name	Name of a resolver. Resolver names have the format <i>/realms/ realm-name/resolver name</i> .
Number of Data Sources	The number of sources from which the resolver obtains data. A data source can be an agent or another resolver.
Resolver Size	The number of keys (or number of mappings) required to perform this resolution.

Viewing Statistics for NIC Agents

Purpose To interpret the statistics for NIC agents, make sure that you have a good understanding of the NIC agents.

See Mapping Subscribers to a Managing SAE.

View statistics for NIC agents.

Action user@host> **show nic statistics agent**

Component Statistics

```
Component Name      /agents/LoginNameVr
Agent Type          Passive
Connection to Data Source Up
Data Size           262141
```

Component Statistics

```
Component Name      /agents/VrSaeId
Agent Type          Active
Connection to Data Source Up
Data Size           2212
```

Component Statistics

```
Component Name      /agents/IpLoginName
Agent Type          Passive
Connection to Data Source Up
Data Size           262141
```

Component Statistics

```
Component Name      /agents/Pool
Agent Type          Active
Connection to Data Source Up
Data Size           3
```

Meaning Table 27 on page 137 describes the output fields for the **show nic statistics agent** command. Output fields are listed in the order in which they appear.

Table 27: Output Fields for show nic statistics agent

Field Name	Field Description
Component name	Name of an agent. Agent names have the format <code>/agents/ agent-name</code> .
Agent Type	Type of agent—active or passive. Active agents publish data whether or not a resolver requests the data. Passive agents provide information only when a resolver requests it.
Connection to Data Source	Whether or not the agent has a connection to its data source; for example, a directory agent to the directory, or an SAE plug-in agent to the CORBA naming server.
Data Size	Number of key to value mappings for the agent.

SRC CLI Commands to View NIC Resolution Data

You can view the data that NIC uses during a resolution. You can view all resolution data, or data for a specified NIC component. Table 28 on page 137 lists the commands you use to view NIC resolution information.

Table 28: Commands to Display NIC Data

Command	Output Displayed
<code>show nic data</code>	All NIC data. The output for this command includes the output for the other <code>show nic data</code> commands.
<code>show nic data maximum-results</code>	All or a specified quantity of NIC resolution data.
<code>show nic data agent</code>	NIC resolution data for a specified agent.
<code>show nic data resolver</code>	NIC resolution data for a specified resolver.
<code>show nic data slot</code>	All NIC data for a specified slot. The output for this command includes the output for the <code>show nic data agent</code> and <code>show nic data resolver</code> commands.

Viewing Data for NIC Resolvers

Purpose To interpret the data for resolvers, make sure that you have a good understanding of the NIC resolution process.

See Overview of the NIC Resolution Process.

View all NIC resolver data.

Action `user@host> show nic data resolver`
 Component name
 /realms/login/C1

```

Key
Type
Vr
String
default@dw2
Value
Type
SaeId
String
IOR:
000000000000003549444C3A736D67742E6A756E697065722E6E65742F7361652F5365727...
41637469766174696F6E456E67696E653A312E30000000000000020000000000000780...
0000000C31302E3232372E362E34330022610000000000226761726B6269742E6B616E6C6...
6E70722E6E65742F736165504F412F5341450000000000200000000000008000000004...
000000010000001C000000000001000100000001050100010001010900000001050100010...
0000002C0000000000000001000000010000001C000000000001000100000001050100010...
0000000105010001...
Key
Type
Vr
String
vr1495@marvin
Value
Type
SaeId
String
...

```

Meaning Table 29 on page 138 describes the output fields for the `show nic data` resolver command. Output fields are listed in the order in which they appear.

Table 29: Output Fields for show nic data resolver

Field Name	Field Description
Component name	Name of a resolver. Resolver names have the format <code>/realms/<i>realm-name</i>/resolver name</code> .
Key	Data type and value of a NIC key. The value is the actual value of the NIC key, not the NIC value to which the key maps.
Value	Data type and value of the NIC value that maps to the associated NIC key.

Viewing Data for NIC Agents

Purpose To interpret the data for agents, make sure that you have a good understanding of the NIC resolution process.

See Overview of the NIC Resolution Process.

View all NIC resolver data.

Action `user@host> show nic data agent`

```

Component name
/agents/LoginNameVr
Key
  Type
Ip
  String
192.170.179.0
Value
  Type
Vr
  String
vorbis-13@prsim
Key
  Type
Ip
  String
192.170.179.3
Value
  Type
Vr
  String
vorbis-13@prsim
...
Key
  Type
Vr
  String
default@sys1
Value
  Type
SaeId
  String
IOR:
0000000000000003549444C3A736D67742E6A756E697065722E6E65742F7361652F53657276696365
41637469766174696F6E456E67696E653A312E300000000000000200000000000007800010200
0000000C31302E3232372E362E34330022610000000000226761726B6269742E6B616E6C61622E6A
6E70722E6E65742F736165504F412F5341450000000000200000000000008000000004A414300
000000010000001C0000000000010001000000010501000100010109000000010501000100000001
0000002C0000000000000001000000010000001C0000000000010001000000010501000100010109
0000000105010001

```

Meaning Table 30 on page 139 describes the output fields for the `show nic data agent` command. Output fields are listed in the order in which they appear.

Table 30: Output Fields for show nic data agent

Field Name	Field Description
Component name	Name of an agent. Agent names have the format <code>/agents/ agent-name</code> .
Key	Data type and value of a NIC key. The value is the actual value of the NIC key, not the NIC value to which the key maps.
Value	Data type and value of the NIC value that maps to the associated NIC key.

Troubleshooting NIC Data Resolution

Problem The NIC does not resolve a request.

Solution Troubleshooting NIC data resolution is a complex task that requires a good understanding of how NIC operates, how it resolves resolution requests, and how the NIC configuration scenario that you are using performs resolutions.

This topic provides high-level troubleshooting information. For further assistance troubleshooting NIC operation and NIC resolutions, contact the Juniper Technical Support Center.

Troubleshoot NIC operation:

1. Make sure that the heap size configured for NIC is adequate and that the process is up:

```
user@host> show nic statistics process
```

```
Component Statistics
Component Name process
Heap in use      456194 bytes (87%)
Heap limit      524288 bytes
Threads         42
Up time         747848 seconds since Wed Jan 31 19:35:57 EST 2007
```

2. Determine whether there are any NIC resolution errors and whether NIC successfully completed any resolution requests:

```
user@host> show nic statistics host
```

```
Component Statistics
Component Name           /hosts
Number of Components Restart 0
Number of No Match Resolutions 0
Number of Resolution Errors 0
Number of Resolutions      0
```

3. Test the resolution process by using the **test nic resolve** command.

See Configuring the NIC (SRC CLI).

If you are unsure whether NIC is resolving resolution requests, view data about those requests to see whether NIC is receiving data.

1. Verify that NIC is receiving data by running the **show nic data resolver** command.

See Viewing Data for NIC Resolvers .

For each resolver, which is identified by a component name such as `/realms/login/C1`, the output should show a value, such as `default@sys1` for the key `Vr`, and the NIC value for that key such as the IOR that identifies an SAE.

2. If NIC is not receiving data, determine which agent or agents are not receiving data by running the `show nic data agent` command.

See Viewing Data for NIC Agents .

3. Review your NIC configuration to make sure that NIC is configured correctly by running the `show` command for the NIC configuration scenario. For example:

```
[edit shared nic scenario OnePop]
user@host# show
```

- Related Topics**
- Configuring the NIC (SRC CLI)
 - Overview of the NIC Resolution Process
 - NIC Configuration Scenarios

Chapter 17

Monitoring the NIC (C-Web Interface)

- Viewing Hosts (C-Web Interface) on page 143
- Viewing Resolvers (C-Web Interface) on page 144
- Viewing Agents (C-Web Interface) on page 146

Viewing Hosts (C-Web Interface)

You can view statistics for hosts and the host process by:

- Viewing Host Statistics on page 143
- Viewing Host Process Statistics on page 144

Viewing Host Statistics

Purpose View NIC host statistics.

Action 1. Click **Monitor > NIC > Statistics > Host**.

The Statistics/Host pane appears.



2. In the Slot box, enter the number of the slot for which you want to display host statistics.

3. Click **OK**.

The Statistics/Host pane displays the properties for the host.

Viewing Host Process Statistics

Purpose View NIC host process statistics.

- Action**
1. Click **Monitor > NIC > Statistics > Process**.

The Statistics/Process pane appears.



2. In the Slot box, enter the number of the slot for which you want to display host process statistics.
3. Click **OK**.

The Statistics/Process pane displays the statistics for the host process.

Viewing Resolvers (C-Web Interface)

You can view resolvers and monitor resolver statistics (C-Web Interface) by:

- Viewing Resolvers on page 144
- Viewing Resolver Statistics on page 145

Viewing Resolvers

Purpose View information about a resolver.

Action 1. Click **Monitor > NIC > Data > Resolver**.

The Data/Resolver pane appears.

The screenshot shows the Juniper C-Web Interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The left sidebar lists various components, with 'NIC' highlighted. The main area is titled 'NIC Data / Resolver' and contains three input fields: 'Maximum Results', 'Name', and 'Slot' (with '0' entered). Below these fields are 'OK' and 'Reset' buttons. The footer shows copyright information for Juniper Networks, Inc. and the slogan 'Juniper your Net.'

2. In the Maximum Results box, enter the maximum number of results that you want to receive.
3. In the Name box, enter the name of the resolver for which you want to view data.
4. In the Slot box, enter the number of the slot for which you want to display resolver data.
5. Click **OK**.

The Data/Resolver pane displays the properties for the resolver.

Viewing Resolver Statistics

Purpose View statistics about resolvers.

Action 1. Click **Monitor > NIC > Statistics > Resolver**.

The Statistics/Resolver pane appears.

2. In the Name box, enter the name of the resolver for which you want to view statistics.
3. In the Slot box, enter the number of the slot for which you want to display resolver statistics.
4. Click **OK**.

The Statistics/Resolver pane displays the statistics for the resolver.

Viewing Agents (C-Web Interface)

You can view agent properties or agent statistics with the C-Web interface by:

- Viewing Agents on page 146
- Viewing Agent Statistics on page 147

Viewing Agents

Purpose View information about an agent.

Action 1. Click **Monitor > NIC > Data > Agent**.

The Data/Agent pane appears.

The screenshot shows the Juniper C-Web Interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The 'Monitor' tab is active, and the left sidebar shows a tree view with 'NIC' selected. The main content area is titled 'Data / Agent' and contains three input fields: 'Maximum Results' (with a value of 10), 'Name' (with a value of 'agent'), and 'Slot' (with a value of 0). Below these fields are 'OK' and 'Reset' buttons. The footer of the interface displays the copyright notice 'Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.' and the Juniper logo.

2. In the Maximum Results box, enter the maximum number of results that you want to receive.
3. In the Name box, enter the name of the agent for which you want to view data.
4. In the Slot box, enter the number of the slot for which you want to display agent data.
5. Click **OK**.

The Data/Agent pane displays the properties for the agent.

Viewing Agent Statistics

Purpose View statistics for an agent.

Action 1. Click **Monitor > NIC > Statistics > Agent**.

The Statistics/Agent pane appears.

The screenshot shows the Juniper Networks SRC 3.0.x web interface. The left sidebar has a menu with the following items: ACP, CLI, Component, Date, Disk, Interfaces..., Iptables..., JPS, NIC (highlighted), NTP, Redirect Server, Route..., SAE, Security, and System. The main content area is titled "Statistics / Agent" and contains two input fields: "Name" and "Slot" (with a value of 0). Below these fields are "OK" and "Reset" buttons. The top navigation bar includes "Monitor", "Configure", "Diagnose", and "Manage". The top right shows "Logged in as: admin", "Refresh", "Preferences", "About", and "Logout". The bottom footer contains copyright information and the Juniper logo.

2. In the Name box, enter the name of the agent for which you want to view statistics.
3. In the Slot box, enter the number of the slot for which you want to display agent statistics.
4. Click **OK**.

The Statistics/Agent pane displays the properties for the agent.

Chapter 18

Monitoring NTP (SRC CLI)

- Viewing NTP Peers (SRC CLI) on page 149
- Viewing Statistics for NTP (SRC CLI) on page 149
- Viewing Internal Variables for NTP (SRC CLI) on page 150

Viewing NTP Peers (SRC CLI)

Purpose View a list of NTP peers with the SRC CLI.

Action user@host> **show ntp associations**

remote	local	st	poll	reach	delay	offset	disp
=====							
*myserver.jnpr.n	192.0.7.46	3	1024	377	0.00038	-0.000573	0.12178

Meaning Table 31 on page 149 describes the output fields for the **show ntp associations** command. Output fields are listed in the approximate order in which they appear.

Table 31: Output Fields for show ntp associations command

remote	Address or name of the remote NTP peer
local	Address or name used by NTP on the local system
st	Stratum of the remote peer
poll	Polling interval, in seconds
reach	Reachability register, in octal
delay	Current estimated delay of the peer, in milliseconds
offset	Current estimated offset of the peer, in milliseconds
disp	Current estimated dispersion of the peer, in milliseconds

Viewing Statistics for NTP (SRC CLI)

Purpose View statistics for NTP with the SRC CLI.

Action user@host> **show ntp statistics**

```

time since restart:    2371617
time since reset:     2371617
packets received:     38765
packets processed:    2573
current version:      38761
previous version:     0
bad version:          0
access denied:        36188
bad length or format: 0
bad authentication:   0
rate exceeded:        0

```

Viewing Internal Variables for NTP (SRC CLI)

Purpose View information about internal variables for NTP with the SRC CLI:

Action user@host> **show ntp status**

```

system peer:          menemsha.jnpr.net
system peer mode:     client
leap indicator:       00
stratum:              4
precision:            -20
root distance:        0.02245 s
root dispersion:      0.07689 s
reference ID:         [10.227.2.100]
reference time:       c922b152.86dd0529 Thu, Dec 7 2006 10:27:14.526
system flags:         auth monitor ntp kernel stats
jitter:               0.000183 s
stability:            1.728 ppm
broadcastdelay:       0.003998 s
authdelay:            0.000000 s

```

Chapter 19

Monitoring NTP (C-Web Interface)

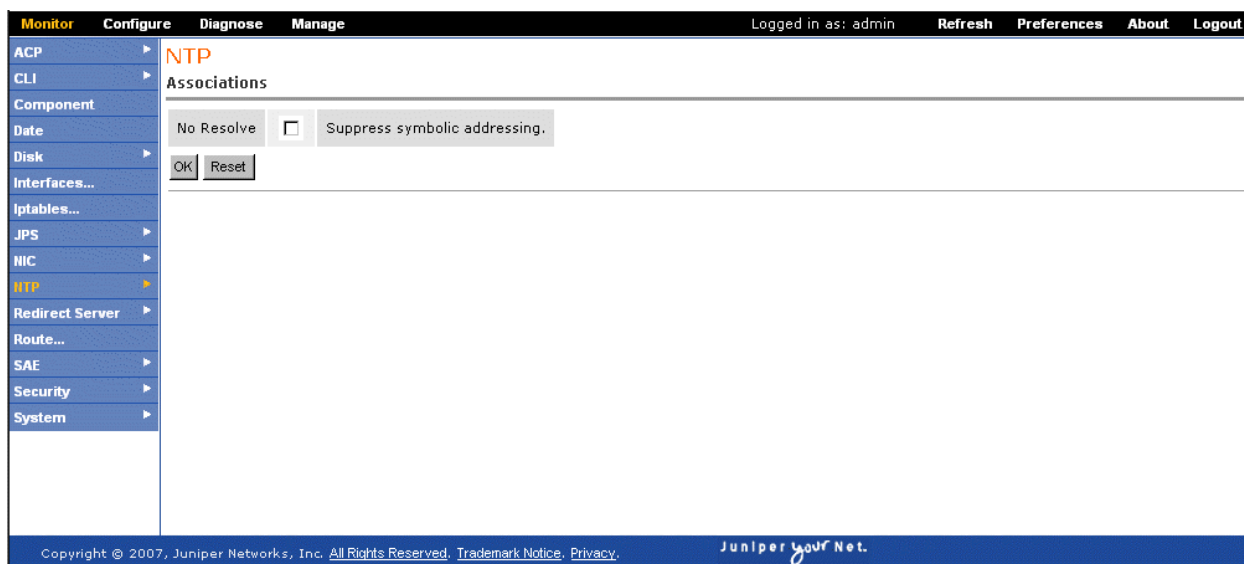
- Viewing NTP Peers (C-Web Interface) on page 151
- Viewing Statistics for NTP (C-Web Interface) on page 151
- Viewing NTP Status (C-Web Interface) on page 152

Viewing NTP Peers (C-Web Interface)

Purpose View a list of NTP peers.

Action 1. Click **Monitor > NTP > Associations**.

The Associations pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

The Associations pane displays the list of NTP peers.

Viewing Statistics for NTP (C-Web Interface)

Purpose Display statistics for NTP.

- Action** 1. Click **Monitor > NTP > Statistics**.

The Statistics pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

The Statistics pane displays statistics for NTP.

Viewing NTP Status (C-Web Interface)

Purpose Display status for NTP.

- Action** 1. Click **Monitor > NTP > Status**.

The Status pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.
3. Click **OK**.

The Status pane displays NTP status.

Chapter 20

Monitoring Redirect Server (SRC CLI)

- Viewing Statistics for the Redirect Server (SRC CLI) on page 155
- Viewing Statistics for Filtered Traffic on page 155

Viewing Statistics for the Redirect Server (SRC CLI)

Purpose View statistics for redirect server.

Action user@host> **show redirect-server statistics**

```
Redirect Server
Uptime: 1270724.713 s
Accepted Requests: 25
Rejected Requests: 0
User limit leaky buckets: 0
User limits reached: 0
Global limits reached: 0
```

- Related Topics**
- Configuring the Redirect Server (SRC CLI)
 - Overview of Traffic Redirection

Viewing Statistics for Filtered Traffic

Purpose You can obtain information about the packets filtered on a C-series controller by accessing statistics for the iptables Linux tool. You can also reset the counters for this tool.

Action To view information about packet filtering on a C-series controller:

```
user@host> show iptables <nat | filter | mangle> <reset-counters>
```

where

- nat—Displays information for the nat table for the iptables tool. The nat table provides rules for rewriting packet addresses.
- filter—Displays information for the filter table for the iptables tool. The filter table provides rules for defining packet filters.
- mangle—Displays information for the mangle table for the iptables tool. The mangle table provides rules for adjusting packet options, such as quality of service.

For example:

```
user@host> show iptables

Chain INPUT (policy ACCEPT 25M packets, 9401M bytes)
 pkts bytes target    prot opt in     out     source
destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source
destination
Chain OUTPUT (policy ACCEPT 24M packets, 4506M bytes)
 pkts bytes target    prot opt in     out     source
destinationreset-counters
```

To reset the values in the output for the `show iptables` command:

```
user@host> show iptables reset counters
```

- Related Topics**
- Overview of Traffic Redirection
 - Configuring the Redirect Server (SRC CLI)

Chapter 21

Monitoring the Redirect Server and Filtered Traffic (C-Web Interface)

- Viewing Statistics for the Redirect Server (C-Web Interface) on page 157
- Viewing Information About Filtered Traffic (C-Web Interface) on page 158

Viewing Statistics for the Redirect Server (C-Web Interface)

Purpose View statistics for the redirect server.

Action 1. Click **Monitor > Redirect Server > Statistics**.

The Statistics pane appears.



2. Select a style from the Output Style list.
3. Click **OK**.

The Statistics pane displays the redirect server statistics.

Viewing Information About Filtered Traffic (C-Web Interface)

Purpose View information about filtered traffic with the **iptables Linux** tool when you are using C-Web to monitor the C-series controller.

Action To view information about the filtered traffic:

1. Click **Monitor > Iptables**.

The Iptables pane appears.



2. Select the type of table that you want to display from the Table list:
 - nat—Displays information for the iptables NAT table
 - filter—Displays information for the iptables filter table
 - mangle—Displays information for the iptables mangle table
3. Select the **Reset Counters** check box to reset the counters of items in the output.
4. Click **OK**.

The Iptables pane displays information about filtered traffic.

Chapter 22

Troubleshooting Network Connectivity (SRC CLI)

- Overview of Commands to Troubleshoot Connections to Remote Hosts on page 159
- Testing Connectivity to Remote Hosts on page 159
- Viewing the Route Information on page 160
- Viewing Routing Table Information on page 160
- Viewing Interface Information on page 161

Overview of Commands to Troubleshoot Connections to Remote Hosts

If you are troubleshooting problems with the SRC software that might be caused by connectivity problems to remote hosts, you can use the following commands:

- `ping`—Test connectivity to a remote host.
- `tracert`—Display the route from the local host to a remote host and back.
- `show interfaces`—Display information about system interfaces.
- `show route`—Display information from the system routing table.

Testing Connectivity to Remote Hosts

Purpose Test connectivity to a remote host.

Action `user@host> ping`
PING 10.227.7.45 (10.227.7.45) 56(84) bytes of data.
64 bytes from 10.227.7.45: icmp_seq=0 ttl=63 time=0.560 ms
64 bytes from 10.227.7.45: icmp_seq=1 ttl=63 time=0.613 ms
64 bytes from 10.227.7.45: icmp_seq=2 ttl=63 time=0.641 ms
64 bytes from 10.227.7.45: icmp_seq=3 ttl=63 time=0.653 ms
64 bytes from 10.227.7.45: icmp_seq=4 ttl=63 time=0.651 ms
64 bytes from 10.227.7.45: icmp_seq=5 ttl=63 time=0.418 ms
64 bytes from 10.227.7.45: icmp_seq=6 ttl=63 time=0.440 ms
64 bytes from 10.227.7.45: icmp_seq=7 ttl=63 time=0.454 ms
64 bytes from 10.227.7.45: icmp_seq=8 ttl=63 time=0.466 ms
64 bytes from 10.227.7.45: icmp_seq=9 ttl=63 time=0.478 ms
64 bytes from 10.227.7.45: icmp_seq=10 ttl=63 time=0.488 ms

Ctrl-C

```

--- 10.227.7.45 ping statistics ---
94 packets transmitted, 94 received, 0% packet loss, time 93038ms
rtt min/avg/max/mdev = 0.418/0.560/0.791/0.089 ms, pipe 2

```

For information about all the options for the ping command, see the *SRC-PE CLI Command Reference*.

Viewing the Route Information

Purpose You can use the `traceroute` command to get information about the hops between the local system and a remote host.

Action To view route information:

```

user@host> traceroute 192.2.7.48
traceroute to 192.2.7.48 (192.2.7.48), 30 hops max, 46 byte packets
 1  host (192.2.7.45)  3000.716 ms !H  3000.733 ms !H  3001.272 ms !H

```

For information about all the options for the `traceroute` command, see the *SRC-PE CLI Command Reference*.

Viewing Routing Table Information

Purpose You can display brief or detailed information about the route from the local system to a remote host.

Action To view brief route information:

```
user@host> show route
```

```

Kernel IP routing table
Destination  Gateway      Genmask      Flags  MSS Window  irtt Iface
192.2.2.0    ' ' ' ' ' ' '*  255.255.255.0  U      0  0      0  0      0 eth0
default      src1ab1.my1ab. 0.0.0.0      UG      0  0      0  0      0 eth0

```

To view detailed route information:

```
user@host> show route detail
```

```

Kernel IP routing table
Destination  Gateway      Genmask      Flags Metric Ref  Use Iface MSS  Window  irtt
192.2.2.0    ' ' ' ' ' ' '*  255.255.255.0  U      0    0      0      0 eth0 ' ' ' ' '0    0
0
default      src1ab1.my1ab. 0.0.0.0      UG      0    0      0      0 eth0 ' ' ' ' '0    0

```

The detailed output includes the additional Metric, Ref, and Use fields.

Viewing Interface Information

Purpose You can view information about all system interfaces, or about a specified interface.

Action To view information about all system interfaces:

```
user@host> show interfaces
eth0      Link encap:Ethernet  HWaddr 00:30:48:55:B6:FC
          inet addr:10.227.6.42  Bcast:10.227.6.255  Mask:255.255.255.0
          inet6 addr: fe80::230:48ff:fe55:b6fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:482467 errors:0 dropped:0 overruns:0 frame:0
          TX packets:57573 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:38147790 (36.3 MiB)  TX bytes:4396018 (4.1 MiB)
          Base address:0xcc00 Memory:fc9c0000-fc9e0000
eth1      Link encap:Ethernet  HWaddr 00:30:48:55:B6:FD
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0xc800 Memory:fc9a0000-fc9c0000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1946394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1946394 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:260604464 (248.5 MiB)  TX bytes:260604464 (248.5 MiB)
lo:1      Link encap:Local Loopback
          inet addr:192.168.254.1  Mask:255.255.255.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```


Chapter 23

Monitoring Network Connectivity (C-Web Interface)

- Viewing Information About the Routing Table (C-Web Interface) on page 163
- Viewing Information About System Interfaces (C-Web Interface) on page 164

Viewing Information About the Routing Table (C-Web Interface)

Purpose View information about the route from the local system to a remote host.

Action 1. Click **Monitor > Route**.

The Route pane appears.



2. To suppress symbolic addressing, select the **No Resolve** box.
3. To display detailed output, select the **Detail** box.
4. Click **OK**.

The Route pane displays the information about the route.

Viewing Information About System Interfaces (C-Web Interface)

Purpose View information about all system interfaces.

Action 1. Click **Monitor > Interfaces**.

The Interfaces pane appears.

The screenshot shows the Juniper C-Web Interface. The top navigation bar includes 'Monitor', 'Configure', 'Diagnose', and 'Manage'. The 'Monitor' tab is selected. On the right side of the top bar, it says 'Logged in as: admin' and provides links for 'Refresh', 'Preferences', 'About', and 'Logout'. On the left side, there is a vertical menu with various system components: ACP, CLI, Component, Date, Disk, Interfaces... (highlighted in orange), Iptables..., JPS, NIC, NTP, Redirect Server, Route..., SAE, Security, and System. The main content area is titled 'Interfaces' in orange. It contains a form with a label 'Interface Name' next to a text input field. Below the input field are 'OK' and 'Reset' buttons. The footer of the page displays 'Copyright © 2007, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.' and the Juniper logo with the tagline 'Juniper your Net.'

2. In the Interface name box, enter the name of the interface for which you want to view data.
3. Click **OK**.

The Interfaces pane displays the information about the interface.

Part 6

Index

- Index on page 167

Index

C

C-series controllers	
boot messages, viewing	
C-Web interface.....	83
SRC CLI.....	78
interface information.....	161
monitoring	
C-Web interface.....	81
system date, viewing.....	82
system information, viewing	
C-Web interface.....	82
SRC CLI.....	77
C-Web interface	
monitoring options.....	76
conventions	
notice icons.....	xvii
text.....	xvii
customer support.....	xxi
contacting JTAC.....	xxi

D

device drivers	
simulated, configuring.....	23
SRC CLI.....	23
viewing on SAE	
C-Web interface.....	112
SRC CLI.....	89
documentation set	
comments on.....	xxi

E

equipment registration	
viewing on SAE	
C-Web interface.....	114
SRC CLI.....	93
event messages. <i>See</i> logging	

F

filtered traffic statistics.....	155, 158
----------------------------------	----------

I

interfaces	
information, viewing	
C-Web interface.....	164
SRC CLI.....	161
iptables Linux tool	
monitoring	
C-Web interface.....	158
SRC CLI.....	155

J

Juniper Networks database, viewing	
C-Web interface.....	86, 87

L

license	
viewing on SAE	
C-Web interface.....	111
SRC CLI.....	91
logging	
configuration statements.....	11
configuring component	
SRC CLI.....	12
file folders	
C-Web interface.....	7
file logging, configuring	
SRC CLI.....	12
log files	
rotation.....	10
messages	
categories.....	8
filters.....	7, 9
format.....	14
severity levels.....	8
overview.....	7
system log, configuring	
SRC CLI.....	13
login registration	
viewing on SAE	
C-Web interface.....	115
SRC CLI.....	93

M

manuals	
comments on.....	xxi
MIBs	
Juniper Networks, list.....	50
monitoring with SNMP agent.....	49
monitoring tools	
C-Web interface.....	73
overview.....	3
SRC CLI.....	73

N

Network Time Protocol. <i>See</i> NTP	
NIC (network information collector)	
agents, viewing	
C-Web interface.....	146
SRC CLI.....	136
hosts, viewing	
C-Web interface.....	143
SRC CLI.....	134
monitoring	
C-Web interface.....	143
SRC CLI.....	133
resolution data, troubleshooting.....	140
resolution data, viewing	
C-Web interface.....	144
SRC CLI.....	137, 138
statistics, viewing	
C-Web interface.....	143
SRC CLI.....	134
notice icons.....	xvii
NTP (Network Time Protocol)	
monitoring	
C-Web interface.....	151
SRC CLI.....	149, 150
statistics, viewing	
C-Web interface.....	151
SRC CLI.....	149

P

policies	
viewing on SAE	
C-Web interface.....	111
SRC CLI.....	92
portals, testing.....	29

R

redirect server	
statistics, viewing	
C-Web interface.....	157
SRC CLI.....	155

router interfaces	
viewing on SAE	
C-Web interface.....	113
SRC CLI.....	91
routing table, viewing	
C-Web interface.....	163
SRC CLI.....	160

S

SAE (service activation engine)	
configuration, viewing	
C-Web interface.....	109
SRC CLI.....	89
directory blacklist, viewing	
C-Web interface.....	109
SRC CLI.....	89
SNMP information, viewing	
C-Web interface.....	122
SRC CLI.....	101
SAE (service activation engine), configuring	
simulated router driver	
C-Web interface.....	27
SRC CLI.....	23
security certificates	
information, viewing	
C-Web interface.....	84
SRC CLI.....	80
services	
viewing on SAE	
C-Web interface.....	110
SRC CLI.....	94
simulated router driver, configuring	
C-Web interface.....	27
SRC CLI.....	23
simulated subscribers	
logging in on SAE.....	30
logging out.....	29
SNMP agent	
MIBs.....	50
See also SNMP traps	55
viewing information on SAE	
C-Web interface.....	122
SRC CLI.....	101
SNMP alarm	
boolean test.....	43
discontinuity check.....	45
existence test.....	44
overview.....	42
threshold test.....	44
SNMP events.....	46, 47

- SNMP monitors
 - alarms.....42
 - boolean test.....43
 - existence test.....44
 - threshold test.....44, 45
 - events.....46, 47
 - overview.....39
 - security name.....46
 - statement hierarchy.....41
- SNMP traps
 - alarm state transitions.....69
 - configuring.....52, 53
 - event traps
 - configuring.....53
 - defined.....51
 - list and description.....67
 - notifications
 - defined.....51
 - overview.....50
 - performance traps
 - accounting.....59
 - authentication.....61
 - chassis.....66
 - configuring.....52
 - defined.....50
 - JPS.....66
 - NIC.....62
 - policy engine.....65
 - redirect server.....65
 - router driver.....63
 - SAE.....58
 - SRC-ACP.....65
 - system management.....64
- SRC CLI, viewing
 - C-Web interface.....87
- SRC components
 - information, viewing
 - C-Web interface.....83
 - SRC CLI.....78
- storing log messages
 - SRC CLI.....12
- subscriber sessions
 - logging in.....30
 - logging out.....33
 - viewing on SAE
 - C-Web interface.....117
 - SRC CLI.....97, 98, 99, 100
- support, technical *See* technical support
- system logging. *See* logging
- T**
- technical support
 - contacting JTAC.....xxi
- testing
 - connection to remote host.....160
- text conventions defined.....xvii
- threads
 - viewing on SAE
 - C-Web interface.....116
 - SRC CLI.....96
- traps. *See* SNMP traps
- troubleshooting
 - tools.....3
 - with log files.....7
- U**
- user permissions, viewing
 - C-Web interface.....88
- users, viewing
 - C-Web interface.....85

