



Cisco Service Control Engine (SCE) CLI Command Reference

Version 3.0
OL-7825-03

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-782503=
Text Part Number: OL-7825-03



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

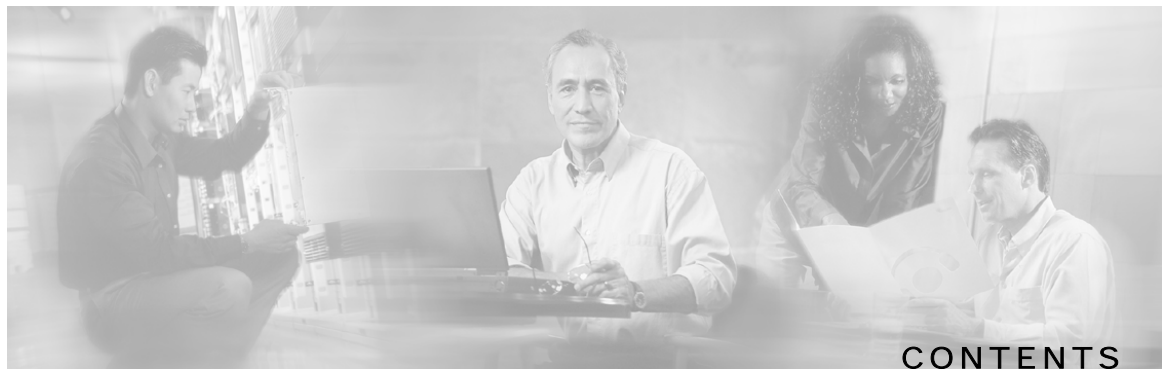
CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Printed in the USA on recycled paper containing 10% postconsumer waste.

Cisco SCE CLI Command Reference

Copyright © 2002-2005 Cisco Systems, Inc.
All rights reserved.



Preface xi

- Document Revision History xi
- Audience xi
- Organization xii
- Related Publications xii
- Conventions xii
- Obtaining Documentation xiii
 - World Wide Web xiii
 - Documentation CD-ROM xiv
 - Ordering Documentation xiv
 - Documentation Feedback xiv
- Obtaining Technical Assistance xiv
 - Cisco.com xv
 - Technical Assistance Center xv

Command-Line Interface 1-1

- Getting Help 1-1
- Authorization and Command Levels (Hierarchy) 1-2
 - CLI Command Hierarchy 1-3
 - CLI Authorization Levels 1-6
 - Prompt Indications 1-7
 - Exiting Modes 1-8
- Navigating Between Configuration Modes 1-9
 - Entering and Exiting Global Configuration Mode 1-9
 - Interface Configuration Modes 1-9
- CLI Help Features 1-14
 - Partial Help 1-14
 - Argument Help 1-14
 - The [no] Prefix 1-15

Navigational and Shortcut Features 1-15

Command History 1-15

Keyboard Shortcuts 1-15

Tab Completion 1-16

FTP User Name and Password 1-17

Managing Command Output 1-17

Scrolling the Screen Display 1-17

Filtering Command Output 1-18

Redirecting Command Output to a File 1-18

CLI Scripts 1-19

CLI Command Reference 2-1

Syntax and Conventions 2-1

CLI Commands 2-2

? 2-2

access-class 2-3

aaa authentication accounting commands 2-4

aaa authentication attempts 2-5

aaa authentication enable default 2-6

access-list 2-7

accelerate-packet-drops 2-9

active-port 2-10

attack-detector default 2-11

aaa authentication login default 2-13

attack-detector 2-14

attack-detector <number> 2-15

attack-detector TCP-port-list|UDP-port-list 2-17

attack-filter (LineCard Interface Configuration) 2-18

attack-filter (Privileged Exec) 2-20

attack-filter subscriber-notification ports 2-22

auto-fail-over 2-23

auto-negotiate (GigabitEthernet only) 2-24

bandwidth 2-25

blink 2-26

boot system 2-27
calendar set 2-28
cd 2-29
clear arp-cache 2-30
clear interface linecard 2-31
clear interface linecard subscriber 2-32
clear interface linecard subscriber db counters 2-33
clear interface linecard 0 VAS-traffic-forwarding VAS all counters health-check 2-34
clear logger 2-35
clear interface linecard traffic-counter 2-37
clear RDR-formatter 2-38
clock read-calendar 2-39
clock set 2-40
clock summertime 2-41
clock timezone 2-44
clock update-calendar 2-45
configure 2-46
connection-mode (SCE 1000 platform) 2-47
connection-mode (SCE 2000 platform) 2-48
copy 2-49
copy ftp:// 2-50
copy-passive 2-51
copy running-config startup-config 2-52
copy source-file ftp:// 2-53
copy source-file startup-config 2-54
copy startup-config destination-file 2-55
default subscriber template all 2-56
delete 2-57
dir 2-58
disable 2-59
do 2-60
duplex 2-61
enable 2-62

- enable password 2-63
- erase startup-config-all 2-64
- exit 2-65
- failure-recovery operation-mode 2-66
- force failure-condition (SCE 2000 only) 2-67
- help 2-68
- history 2-70
- history size 2-71
- hostname 2-72
- interface FastEthernet 2-73
- interface GigabitEthernet 2-74
- interface LineCard 2-75
- interface Mng 2-76
- ip access-class 2-77
- ip address 2-78
- ip advertising 2-79
- ip default-gateway 2-80
- ip domain-lookup 2-81
- ip domain-name 2-82
- ip filter fragment 2-83
- ip filter monitor 2-84
- ip ftp password 2-85
- ip ftp username 2-86
- ip host 2-87
- ip name-server 2-88
- ip route 2-89
- ip rpc-adapter 2-90
- ip rpc-adapter port 2-91
- ip ssh 2-92
- ip ssh access-class 2-93
- ip ssh key 2-94
- ip-tunnel L2TP skip 2-95
- L2TP identify-by 2-96
- line vty 2-97

link failure-reflection 2-98
link mode 2-99
logger add-user-message 2-101
logger device User-File-Log 2-102
logger device User-File-Log max-file-size 2-103
logger get support-file 2-104
logger get user-log file-name 2-105
logout 2-106
management-agent access-class 2-107
management-agent sce-api logging 2-108
management-agent sce-api timeout 2-110
management-agent system 2-111
mkdir 2-112
more 2-113
more user-log 2-114
MPLS 2-115
no subscriber 2-116
no subscriber anonymous-group 2-117
no subscriber mappings included-in 2-118
ping 2-119
pqi install file 2-120
pqi rollback file 2-121
pqi uninstall file 2-122
pqi upgrade file 2-123
pwd 2-124
queue 2-125
RDR-formatter category-number 2-126
RDR-formatter destination 2-127
RDR-formatter forwarding-mode 2-129
RDR-formatter history-size 2-130
RDR-formatter protocol 2-131
RDR-formatter protocol RDRv2 connection-timeout 2-132
RDR-formatter rdr-mapping 2-133
reload 2-134

- reload shutdown 2-135
- rename 2-136
- rmdir 2-137
- script capture 2-138
- script print 2-139
- script run 2-140
- script stop 2-141
- service password-encryption 2-142
- service RDR-formatter 2-143
- service telnetd 2-144
- setup 2-145
- show access-lists 2-149
- show blink 2-150
- show calendar 2-151
- show clock 2-152
- show failure-recovery operation-mode 2-153
- show hostname 2-154
- show hosts 2-155
- show interface FastEthernet 2-156
- show interface GigabitEthernet 2-159
- show interface Mng 2-160
- show interface LineCard 2-161
- show interface LineCard application 2-162
- show interface LineCard attack-detector 2-163
- show interface LineCard attack-filter 2-164
- show interface LineCard connection-mode 2-166
- show interface LineCard counters 2-167
- show interface LineCard link mode 2-168
- show interface LineCard link-bypass (SCE 1000 only) 2-169
- show interface LineCard physically-connected-links (SCE 2000 only) 2-170
- show interface LineCard silent 2-171
- show interface LineCard subscriber 2-172
- show interface LineCard subscriber aging 2-173
- show interface LineCard subscriber anonymous 2-174

show interface LineCard subscriber anonymous-group 2-175

show interface LineCard subscriber db counters 2-176

show interface LineCard subscriber mapping 2-178

show interface LineCard subscriber name 2-179

show interface LineCard subscriber properties 2-180

show interface LineCard subscriber TP-mappings statistics 2-181

show interface LineCard subscriber TP-IP-range 2-182

show interface LineCard subscriber mapping included-in TP-IP-range 2-183

show interface LineCard tos-marking mode 2-184

show interface LineCard tos-marking table 2-185

show interface LineCard traffic-counter 2-186

show interface LineCard traffic-rule 2-187

show interface linecard VAS-traffic-forwarding 2-188

show interface LineCard [VLAN|L2TP|IP-tunnel] 2-191

show interface LineCard vlan translation 2-192

show ip access-class 2-193

show ip advertising 2-194

show ip filter 2-195

show ip default-gateway 2-196

show ip route 2-197

show ip rpc-adapter 2-198

show ip ssh 2-199

show line vty 2-200

show logger device User-File-Log 2-201

show logger device User-File-Log counters 2-202

show logger device User-File-Log max-file-size 2-202

show logger device User-File-Log status 2-204

show logger device User-File-Log nv-counters 2-205

show management-agent sce-api 2-206

show pqj file 2-207

show pqj last-installed 2-208

show RDR-formatter 2-209

show RDR-formatter connection-status 2-210

show RDR-formatter counters 2-211

show RDR-formatter destination 2-212
show RDR-formatter enabled 2-213
show RDR-formatter forwarding-mode 2-214
show RDR-formatter statistics 2-215
show running-config 2-216
show snmp 2-218
show snmp community 2-220
show snmp contact 2-221
show snmp enabled 2-222
show snmp host 2-223
show snmp location 2-224
show snmp MIB 2-225
show snmp traps 2-226
show snmp 2-227
show startup-config 2-228
show system operation-status 2-229
show system-uptime 2-230
show tacacs 2-231
show telnet sessions 2-232
show telnet status 2-233
show timezone 2-234
show users 2-235
show version 2-236
show version all 2-238
show version software 2-241
silent 2-242
snmp-server 2-243
snmp-server community 2-244
snmp-server contact 2-245
snmp-server enable traps 2-246
snmp-server host 2-248
snmp-server location 2-249
snmp server 2-250
snmp broadcast client 2-251

snmp update-interval 2-252
speed 2-253
subscriber aging 2-254
subscriber anonymous-group export csv-file 2-255
subscriber anonymous-group import csv-file 2-256
subscriber export csv-file 2-257
subscriber import csv-file 2-258
subscriber sm-connection-failure 2-259
subscriber template export csv-file 2-260
subscriber template import csv-file 2-261
subscriber TP-IP-range name IP-range target-TP 2-262
subscriber TP-mappings 2-263
subscriber TP-IP-range 2-264
tacacs-server host 2-265
tacacs-server key 2-266
tacacs-server timeout 2-267
telnet 2-268
timeout 2-269
tos-marking mode 2-270
tos-marking reset-table 2-271
tos-marking set-table-entry 2-272
tracert 2-273
traffic-counter 2-274
traffic-rule 2-275
unzip 2-278
username 2-279
username privilege 2-281
VAS-traffic-forwarding 2-282
VAS-traffic-forwarding VAS server-id health-check 2-284
VAS-traffic-forwarding VAS server-group 2-286
VAS-traffic-forwarding VAS server-group failure 2-288
VAS-traffic-forwarding VAS server-id 2-290
VAS-traffic-forwarding server-id VLAN 2-292
VAS-traffic-forwarding traffic-link 2-293

VLAN 2-294

vlan translation 2-295

wap 2-296

Index I-1



Preface

This guide contains Command-Line Interface (CLI) commands to maintain the SCE Platform. This guide assumes a basic familiarity with telecommunications equipment and installation procedures.

Throughout the book, the procedures shown are examples of how to perform typical SCE platform management functions. Because of the large number of functions available, not every possible procedure is documented in the instructional chapters. The *CLI Command Reference* (on page 2-1) provides a complete listing of all possible commands. The other chapters provide examples of how to implement the most common of these commands, general information on the interrelationships between the commands and the conceptual background of how to use them.

Document Revision History

Cisco Service Control Release	Part Number	Publication Date
Release 3.0	OL-7825-03	December, 2005

DESCRIPTION OF CHANGES

Added CLI commands related to the following new features:

- Value Added Services traffic forwarding
- TACACS+ authentication, authorization and accounting
- Management port redundancy

Release 2.5.7	OL-7825-02	August, 2005
---------------	------------	--------------

Audience

This guide is intended for the networking or computer technician responsible for configuring and maintaining the SCE Platform on-site. It is also intended for the operator who manages the SCE Platform(s). This guide does not cover high-level technical support procedures available to Root administrators and Cisco technical support personnel.

Organization

This guide covers the following topics:

Chapter	Title	Description
Chapter 1	<i>Command-Line Interface</i> (on page 1-1)	Describes how to use the SCE Platform Command-Line Interface (CLI), its hierarchical structure, authorization levels and its help features.
Chapter 2	<i>CLI Command Reference</i> (on page 2-1)	Provides an alphabetical list of the available CLI commands that you can use to configure the <i>SCE</i> .

Related Publications

This *Cisco Service Control Engine (SCE) CLI Command Reference* should be used in conjunction with the following SCE platform manuals to provide a detailed explanation of the commands:

- *SCE 2000 4xGBE Installation and Configuration Guide*
- *SCE 2000 4/8xFBE Installation and Configuration Guide*
- *SCE 1000 2xGBE Installation and Configuration Guide*
- *Cisco Service Control Engine (SCE) Software Configuration Guide*

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands and keywords are in boldface .
<i>italic font</i>	Arguments for which you supply values are in <i>italics</i> .
[]	Elements in square brackets are optional.
{x y z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
screen font	Terminal sessions and information the system displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font .

<i>italic screen font</i>	Arguments for which you supply values are in <i>italic screen font</i> .
→	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
<>	Nonprinting characters, such as passwords, are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Cautions use the following conventions:



Caution

Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Warnings use the following conventions:



Warning

Means *reader be warned*. You are capable of doing something that might result in bodily injury.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the networking Products Marketplace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/pcgi-bin/marketplace/welcome.pl>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can email your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides [Cisco.com](http://www.cisco.com) (on page [xv](#)) as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for *Cisco.com* (on page xv), go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

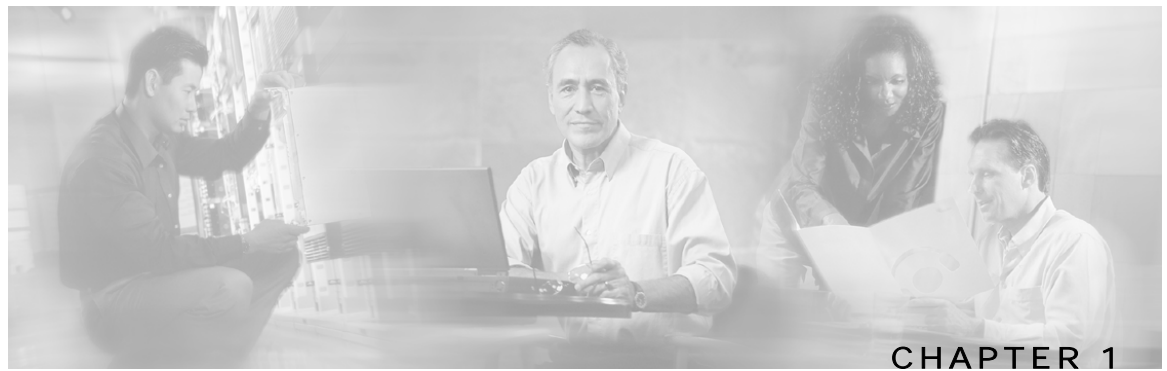
Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.



Command-Line Interface

This chapter describes how to use the SCE Platform Command-Line Interface (CLI), its hierarchical structure, authorization levels and its help features. The Command-Line Interface is one of the *SCE* platform management interfaces.

The CLI is accessed through a Telnet session or directly via the console port on the front panel of the SCE Platform. When you enter a Telnet session, you enter as the simplest level of user, in the User Exec mode.

The SCE Platform supports up to six concurrent CLI sessions; five sessions initiated by Telnet connection, and one session on the console port.

This chapter contains the following sections:

- [Getting Help](#) 1-1
- [Authorization and Command Levels \(Hierarchy\)](#) 1-2
- [Navigating Between Configuration Modes](#) 1-9
- [CLI Help Features](#) 1-14
- [Navigational and Shortcut Features](#) 1-15
- [Managing Command Output](#) 1-17
- [CLI Scripts](#) 1-19

Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark (?) at the system prompt. You also can obtain a list of keywords and arguments associated with any command using the context-sensitive help feature.

The following table lists commands you can enter to get help that is specific to a command mode, a command, a keyword, or an argument.

Table 1-1 Getting Help

Command	Purpose
abbreviated-command-entry?	Obtain a list of commands that begin with a particular character string. (Do not leave a space between the command and question mark.)
abbreviated-command-entry<Tab>	Complete a partial command name.
?	List all commands available for a particular command mode.
command ?	List the keywords associated with the specified command. Leave a space between the command and question mark.
command keyword ?	List the arguments associated with the specified keyword. Leave a space between the keyword and question mark.

Authorization and Command Levels (Hierarchy)

When using the CLI there are two important concepts that you must understand in order to navigate:

- **Authorization Level** — Indicates the level of commands you can execute. A user with a simple authorization level can only view some information in the system, while a higher level administrator can actually make changes to configuration.

This manual documents commands at the User, Viewer, and Admin authorization level. See CLI Command Hierarchy.

- **Command Hierarchy Level** — Provides you with a context for initiating commands. Commands are broken down into categories and you can only execute each command within the context of its category. For example, in order to configure parameters related to the Line Card, you need to be within the LineCard Interface Configuration Mode. See CLI Command Hierarchy.

The following sections describe the available Authorization and Command Hierarchy Levels and how to maneuver within them.

The on-screen prompt indicates both your authorization level and your command hierarchy level, as well as the assigned host name. See *Prompt Indications* (on page 1-7).



Note Throughout the manual, *SCE* is used as the sample host name.

CLI Command Hierarchy

The set of all CLI commands is grouped in hierarchical order, according to the type of the commands. The first three levels in the hierarchy are the User Exec, Viewer, and Privileged Exec modes. These are non-configuration modes in which the set of available commands enables the monitoring of the SCE Platform, file system operations, and other operations that cannot alter the configuration of the SCE Platform.

The next levels in the hierarchy are the Global and Interface configuration modes, which hold a set of commands that control the global configuration of the SCE Platform and its interfaces. Any of the parameters set by the commands in these modes should be saved in the startup configuration, such that in the case of a reboot, the SCE Platform restores the saved configuration.

The following table shows the available CLI modes.

Table 1-2 CLI Modes

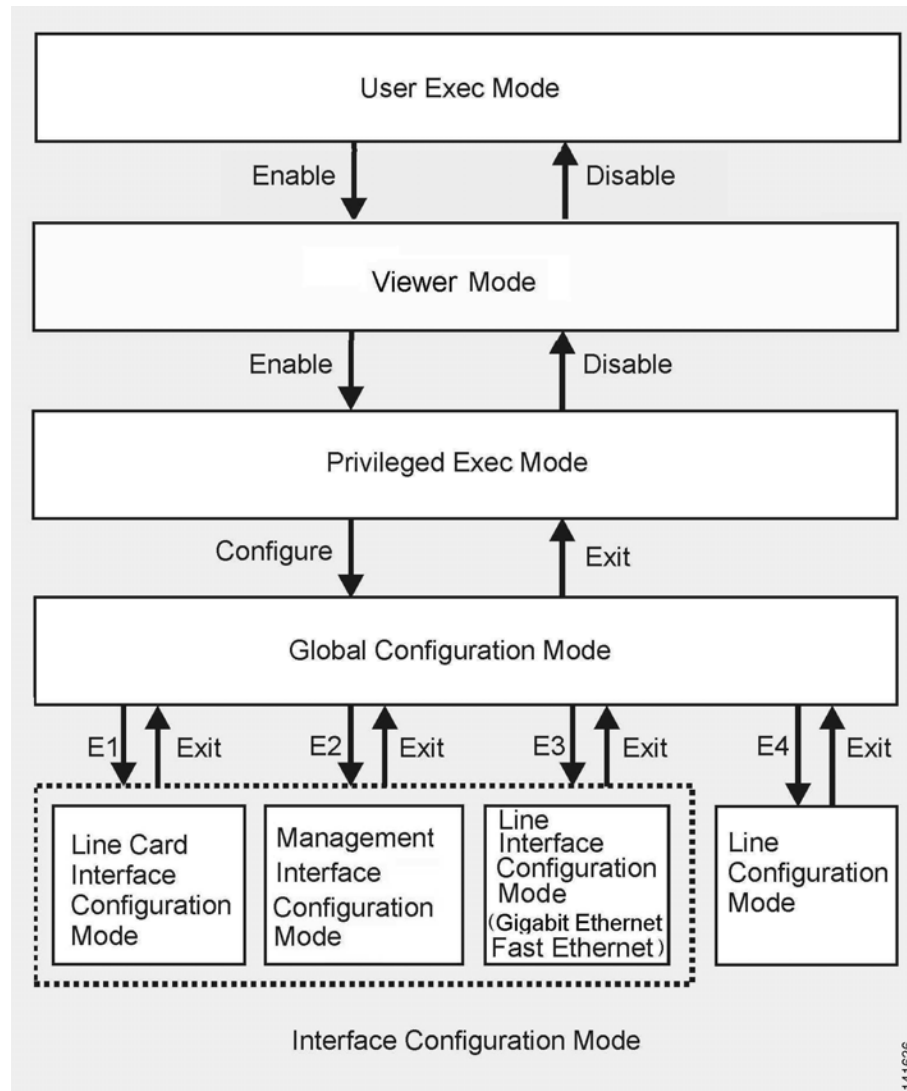
Mode	Description	Level	Prompt indication
User Exec	Initial mode with very limited functionality.	User	<i>SCE</i> >
Viewer	Monitoring (show commands).	Viewer	<i>SCE</i> >
Privileged Exec	General administration; file system manipulations and control of basic parameters that do not change the configuration of the SCE Platform.	Admin	<i>SCE</i> #
Global Configuration	Configuration of general system parameters, such as DNS, host name, and time zone.	Admin	<i>SCE</i> (config)#
Management Interface Configuration	Configuration of management interface parameters, such as the Ethernet interface properties and selection of the active port.	Admin	<i>SCE</i> (config if)#
Interface Configuration	Configuration of specific system interface parameters, such as the Line Card, and the Ethernet interfaces.	Admin	<i>SCE</i> (config if)#
Line Configuration	Configuration of Telnet lines, such as an access-list.	Admin	<i>SCE</i> (config-line)#

When you login to the system, you have the User authorization level and enter User Exec mode. Changing the authorization level to Viewer automatically moves you to Viewer mode. In order to move to any of the configuration modes, you must enter commands specific to that mode.

The list of available commands in each mode can be viewed using the question mark '?' at the end of the prompt.

The figure below, illustrates the hierarchical structure of the CLI modes, and the CLI commands used to enter and exit a mode.

Figure 1-1: CLI Command Hierarchy



The following commands are used to enter the different configure interface modes and the Line Configuration Mode:

- E1 **interface LineCard 0**
- E2 **interface Mng 0/1** or **0/2** (management port, all platforms)
- E3 **interface GigabitEthernet 0/1** or **0/2** (line ports, SCE 1000 platform)
- E3 **interface GigabitEthernet 0/1, 0/2, 0/3, or 0/4** (line ports, SCE 2000 4xGBE platform)
- E3 **interface FastEthernet 0/1, 0/2, 0/3, or 0/4** (line ports, SCE 2000 4/8xFE platform)

- E4 **line vty 0**

**Note**

Although the system supports up to five concurrent Telnet connections, you cannot configure them separately. This means that any number you enter in the **line vty** command (**0, 1, 2, 3** or **4**) will act as a **0** and configure all five connections together.

**Note**

In order for the auto-completion feature to work, when you move from one interface configuration mode to another, you must first exit the current interface configuration mode (as illustrated in the above figure).

EXAMPLE:

This example illustrates moving into and out of configuration modes as follows:

- Enter global configuration mode
- Configure the SCE Platform time zone
- Enter Mng Interface configuration mode for Mng port 1
- Configure the speed of the management interface
- Exit the Mng Interface configuration mode to the global configuration mode
- Enter the LineCard Interface configuration
- Define the link mode.
- Exit LineCard Interface configuration mode to the global configuration mode
- Exit global configuration mode

```
SCE#configure
SCE(config)#clock timezone PST -10
SCE(config)#interface Mng 0/1
SCE(config if)#speed 100
SCE(config if)#exit
SCE(config)#interface LineCard 0
SCE(config if)#link-mode all-links forwarding
SCE(config if)#exit
SCE(config)#exit
SCE#
```

CLI Authorization Levels

The SCE Platform system has four authorization levels, which represent the user access permissions. When you initially connect to the SCE Platform, you automatically have the most basic authorization level, that is User, which allows minimum functionality.

In order to monitor the system, you must have Viewer authorization, while in order to perform administrative functions on the SCE Platform, you must have Admin or Root authorization. A higher level of authorization is accessed by logging in with appropriate password, as described in the procedures below.

In each authorization level, all the commands of the lower authorization layers are available in addition to commands that are authorized only to the current level.



Note This manual covers the functions that can be performed by the Admin level user, unless otherwise noted.

The following CLI commands are related to authorization levels:

- enable
- disable

Each authorization level has a value (number) corresponding to it. When using the CLI commands, use the values, not the name of the level, as shown in the following table.

Table 1-3 Authorization Levels

Level	Description	Value	Prompt
User	Password required. This level enables basic operational functionality.	0	>
Viewer	Password required. This level enables monitoring functionality. All show commands are available to the Viewer authorization level, with the exception of those that display password information.	5	>
Admin	Password required. For use by general administrators, the Admin authorization level enables configuration and management of the SCE Platform.	10	#
Root	Password required. For use by technical field engineers, the Root authorization level enables configuration of all advanced settings, such as debug and disaster recovery. The Root level is used by technical engineers only and is not documented in this manual.	15	#>

To change from User to Viewer level authorization:

Step 1 From the *SCE>* prompt, type **enable 5** and press **Enter**.

The system prompts for a password by showing the prompt *Password*:

Step 2 Type in the password for the Viewer level and press **Enter**.

Note that the password is an access-level authorization setting, not an individual user password.

The system prompt *SCE>* does not change when you move from User to Viewer level.

A telnet session begins with a request for password, and will not continue until the proper user password is supplied. This enhances the security of the system by not revealing its identity to unauthorized people.

To log in with Admin level authorization:

Step 1 Initiate a telnet connection.

Step 2 A `Password:` prompt appears. Type in the user level password and press **Enter**.

The *SCE>* prompt appears.

You now have user level authorization.

Step 3 From the *SCE>* prompt, type **enable 10** and press **Enter**.

The system prompts for a password by showing the prompt `Password:`:

Step 4 Type in the password for the Admin level and press **Enter**.

Note that the password is an access-level authorization setting, not an individual user password.

The system prompt changes to *SCE#* to show you are now in Admin level.

EXAMPLE:

The following example illustrates how to change the authorization level from User to Admin, and then revert back to Viewer. No password is required for moving to a lower authorization level.

```
SCE>enable 10
Password: cisco
SCE#disable
SCE>
```

Prompt Indications

The on-screen prompt indicates your authorization level, your command hierarchy level, and the assigned host name. The structure of the prompt is:

```
<hostname>(mode-indication)level-indication>
```

Authorization levels are indicated as follows:

This prompt...	Indicates this...
>	indicates User and Viewer levels
#	indicates Admin level
#>	indicates Root level

Command hierarchy levels are indicated as follows:

This command hierarchy...	Is indicated as...
User Exec	<i>SCE</i> >
Privileged Exec	<i>SCE</i> #
Global Configuration	<i>SCE</i> (config)#
Interface Configuration	<i>SCE</i> (config if)#
Line Configuration	<i>SCE</i> (config-line)#

EXAMPLE:

The prompt *MySCE*(config if)# indicates:

- The name of the *SCE* platform is *MySCE*
- The current CLI mode is Interface configuration mode
- The user has Admin authorization level

Exiting Modes

This section describes how to revert to a previous mode.

- To exit from one authorization level to the previous one, use the **disable** command.
- To exit from one mode to another with the Admin authorization level (these are the various configuration modes), use the **exit** command.

To exit from the Privileged Exec mode and revert to the Viewer mode:

At the *SCE*# prompt, type **disable**, and press **Enter**.

The *SCE*> prompt for the Viewer and User Exec mode appears.

To exit from the Global Configuration Mode:

At the *SCE*(config)# prompt, type **exit**, and press **Enter**.

The appropriate prompt for the previous level appears.

EXAMPLE:

The following example shows the system response when you exit the Interface Configuration mode.

```
SCE(config if)#exit
SCE(config)#
```

Navigating Between Configuration Modes

Entering and Exiting Global Configuration Mode

To enter the Global Configuration Mode:

At the *SCE#* prompt, type **configure**, and press **Enter**.

The *SCE(config)#* prompt appears.

To exit the Global Configuration Mode:

At the *SCE(config)#* prompt, type **exit** and press **Enter**.

The *SCE#* prompt appears.

Interface Configuration Modes

The components that are configured by the Interface Configuration Modes are:

- Card
 - LineCard — **Interface LineCard 0**
The LineCard interface configures the main functionality of viewing and handling traffic on the line.
- Ports
 - See [Configuring the Physical Ports](#) (on page 1-9)
- Telnet
 - Line Configuration Mode — **Line vty 0**
The Line Configuration Mode enables you to configure Telnet parameters.

Configuring the Physical Ports

The SCE Platform system contains the following physical port interfaces:

- Management:

Interface Mng 0/1 or 0/2

The Management Interface mode configures the settings for the interface to a remote management console. The two management ports support management interface redundancy.

The following commands are used to configure the management port:

- *ip address* (on page 2-78)
- *duplex* ("speed" on page 2-253)
- *speed* (on page 2-253)
- active-port (SCE 2000 platform only)
- fail-over
- Fast Ethernet (SCE 2000 4/8xFE):

Interface FastEthernet 0/1, 0/2, 0/3, or 0/4

The FastEthernet Interface mode configures the settings for the FastEthernet interface to the Internet traffic on the wire. Each of the four ports can be set individually.

The following commands are used to configure the Fast Ethernet line ports:

- *bandwidth* ("speed" on page 2-253)
- *duplex* (on page 2-61)
- *queue* ("speed" on page 2-253)
- *speed* (on page 2-253)
- Gigabit Ethernet (SCE 1000 platform):

Interface GigabitEthernet 0/1, or 0/2

The GigabitEthernet Interface mode configures the settings for the GigabitEthernet interface to the Internet traffic on the wire. Each of the two ports can be set individually.

- Gigabit Ethernet (SCE 2000 4xGBE platform):

Interface GigabitEthernet 0/1, 0/2, 0/3, or 0/4

The GigabitEthernet Interface mode configures the settings for the GigabitEthernet interface to the Internet traffic on the wire. Each of the four ports can be set individually.

The following commands are used to configure the Gigabit Ethernet line ports:

- *auto-negotiate* (*GigabitEthernet only*) (on page 2-24)
- *bandwidth* ("queue" on page 2-125)
- *queue* (on page 2-125)



Note

You must specify the slot number/interface number when referencing any interface. The slot number is always 0, and the interfaces are numbered as follows:

Management Interface: **1,2**

Ethernet Line Interfaces:

SCE 1000 platform: **1,2**

SCE 2000 platform: **1,2,3,4**

Entering Management Interface Configuration Mode

Before you can configure the parameters for the management interface, you must be in the Mng Interface Configuration Mode.

To enter Mng Interface Configuration Mode, perform the following steps:

Step 1 To enter Global Configuration Mode, type **configure** and press **Enter**.

The *SCE(config)#* prompt appears.

Step 2 Type **interface Mng [0/1|0/2]** and press **Enter**.

The *SCE(config if)#* prompt appears.

The system prompt changes to reflect the higher level mode.

To return to the Global Configuration mode, use the following command:

Type **exit**.

Entering LineCard Interface Configuration Mode

The following procedure is for entering Line Card Interface Configuration mode. The procedures for entering the other interfaces are the same except for the interface command as described above and in [CLI Command Reference](#) (on page 2-1).

To enter LineCard Interface Configuration mode:

Step 1 To enter Global Configuration Mode, at the *SCE#* prompt, type **configure**, and press **Enter**.

The *SCE(config)#* prompt appears.

Step 2 Type **interface LineCard 0**, and press **Enter**.

The *SCE(config if)#* prompt appears.

Step 3 To return to Global Configuration Mode, type **exit** and press **Enter**.

The *SCE(config)#* prompt appears.

Step 4 To exit Global Configuration Mode, type **exit** and press **Enter**.

The *SCE#* prompt appears.

Entering Ethernet Line Interface Configuration Mode

Entering the Fast Ethernet Line Interface Configuration Mode

To enter the FastEthernet Interface Configuration Mode:

Step 1 To enter Global Configuration Mode, type **configure** and press **Enter**.

The *SCE(config)#* prompt appears.

Step 2 For the SCE 2000, type **interface FastEthernet [0/1|0/2|0/3|0/4]** and press **Enter**.

The *SCE(config if)#* prompt appears.

EXAMPLE:

The following example shows how to enter Configuration Mode for the FastEthernet Interface number 3.

```
SCE(config)#interface FastEthernet 0/3
SCE(config if)#
```

Entering the Gigabit Ethernet Line Interface Configuration Mode

To enter the GigabitEthernet Interface Configuration Mode:

Step 1 To enter Global Configuration Mode, type **configure** and press **Enter**.

The *SCE(config)#* prompt appears.

Step 2 For the SCE 1000, type **interface GigabitEthernet [0/1|0/2]** and press **Enter**.

Step 3 For the SCE 2000, type **interface GigabitEthernet [0/1|0/2|0/3|0/4]** and press **Enter**.

The *SCE(config if)#* prompt appears.

EXAMPLE:

The following example shows how to enter Configuration Mode for the GigabitEthernet Interface number 2.

```
SCE(config)#interface GigabitEthernet 0/2
SCE(config if)#
```

Navigating between the Interface Configuration Modes

To navigate from one Interface Configuration Mode to another:

Step 1 Type **exit**.

You are returned to the Global Configuration Mode.

Step 2 Type the appropriate command to enter a different Interface Configuration Mode.

The "do" Command: Executing Commands Without Exiting

There are four configuration command modes:

- Global configuration mode
- Management interface configuration mode
- Interface configuration mode
- Line configuration mode

When you are in one of these configuration modes, it is possible to execute an EXEC mode command (such as a show command) or a privileged EXEC (such as **show running-config**) without exiting to the relevant command mode. Use the 'do' command for this purpose.

To execute an exec mode command from a configuration command mode, use the following command:

At the *SCE*config# (or *SCE*config if#) prompt, type **do <command>**.

The specified command executes without exiting to the appropriate exec command mode.

EXAMPLE

The following example shows how to display the running configuration while in interface configuration mode.

```
SCEconfig if# do show running-config
```

CLI Help Features

CLI provides context sensitive help. Two types of context sensitive help are supported:

- Partial help
- Argument help

Partial Help

To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called partial help, because it lists only the keywords or arguments that begin with the abbreviation you entered.

EXAMPLE:

The following example illustrates how typing `c?` displays all available arguments that start with the letter c.

```
SCE(config)#snmp-server c?
Community                contact
SCE(config)#snmp-server c
```

Argument Help

To obtain a list of command's associated keywords or parameters, type a question mark (?) in place of a keyword or parameter on the command line.

Note that if `<Enter>` is acceptable input, the symbol `<cr>` represents the **Enter** key.

EXAMPLE:

The following example illustrates how to get a list of all arguments or keywords expected after the command `snmp-server`.

```
SCE(config)#snmp-server ?
Community      Define community string
Contact        Set system contact
Enable         Enable the SNMP agent
Host           Set traps destination
Location       Set system location
SCE(config)# snmp-server
```

When asking for help on particular parameter, the system informs you of the type of data that is an accepted legal value. The types of parameters supported are:

- | | |
|---------|---|
| STRING | When a String is expected, you can enter any set of characters or digits. If the string has a space as one of its characters, use double-quote (") marks to enclose the string. |
| DECIMAL | Any decimal number. Positive number is assumed, for negative numbers use the "-" symbol. |
| HEX | A hexadecimal number; must start with either 0x or 0X. |

EXAMPLE:

The following example illustrates the use of `?` to get help on commands syntax. In this example, you can enter either the word **running-config**, or any name of a file, after the word **copy**.

```
SCE#copy ?
      running-config      Copy running configuration file
      STRING              Source file name
SCE#copy
```

The [no] Prefix

Many CLI commands offer the option of adding the word **no** before the command to disable the feature controlled by the command or revert it to its default configuration. This notation is shown in the *CLI Command Reference* (on page 2-1) as **[no]** to denote it is optional.

For example, **no service telnetd** disables the telnet server. Enabling the telnet server is done by typing **service telnetd**.

Navigational and Shortcut Features

Command History

CLI maintains a history buffer of the most recent commands you used in the current CLI session for quick retrieval. Using the keyboard, you can navigate through your last commands, one by one, or all commands that start with a given prefix. By default, the system saves the last 30 commands you typed. You can change the number of commands remembered using the **history size** command.

To use the history functions, use the keys shown in the following table.

Table 1-4 Keyboard Shortcuts for History Functions

Arrow	Shortcut	Description
Up arrow	Ctrl-P	Moves cursor to the previous command with the same prefix.
Down arrow	Ctrl-N	Moves cursor to the next command with the same prefix as original.
	Ctrl-L Ctrl-R	Re-display the current command line.

Keyboard Shortcuts

The SCE Platform has a number of keyboard shortcuts that make it easier to navigate and use the system. The following table shows the keyboard shortcuts available.

You can get a display the keyboard shortcuts at any time by typing **help bindings**.

Table 1-5 Keyboard Shortcuts

Description	Shortcut Key
Navigational shortcuts	
Move cursor one character to the right.	CTRL-F /->
Move cursor one character to the left.	CTRL-B /<-
Move cursor one word to the right (forward).	ESC-F
Move cursor one word to the left (backward).	ESC-B
Move cursor to the start of the line.	CTRL-A
Move cursor to the end of the line.	CTRL-E
Editing shortcuts	
Delete the character where the cursor is located.	CTRL-D
Delete from the cursor position to the end of the word.	ESC-d
Delete the character before the current location of the cursor.	Backspace
Delete the character before the current location of the cursor.	CTRL-H
Deletes from the cursor position to the end of the line	CTRL-K
Deletes all characters from the cursor to the beginning of the line	CTRL-U
Deletes all characters from the cursor to the beginning of the line. (Same functionality as CTRL-U.)	CTRL-X
Delete the word to the left of the cursor.	CTRL-W
Recall the last item deleted.	CTRL-Y
Completes the word when there is only one possible completion.	<Tab>
Completes the word when there is only one possible completion. (Same functionality as <Tab>.)	CTRL-I

Tab Completion

The CLI interface features tab completion. When you type in the first letters of a command and type **<Tab>**, the system automatically fills in the rest of the command or keyword. This feature works only when there is one possible command that could be possible using the starting letters.

EXAMPLE:

The letters **snm** followed by **<Tab>** will be completed to the command **snmp-server**.

```
SCE (config) #snm<Tab>
SCE (config) #snmp-server
```

If you type **<Enter>** instead of **<Tab>**, and there is no ambiguity, the system actually carries out the command which would be filled in by the rest of the word.

EXAMPLE:

The following example displays how the system completes a partial (unique) command for the **enable** command. Because **enable** does not require any parameters, the system simply carries out the **enable** command when the user presses **Enter**.

```
SCE>en<Enter>
Password:
SCE#
```

FTP User Name and Password

CLI enables saving ftp user name and password to be used in FTP operations—download and upload, per session.

These settings are effective during the current CLI session.

EXAMPLE:

The following example illustrates how to set FTP password and user name and the use in these settings for getting a file named *config.tmp* from a remote station using FTP protocol.

```
SCE#ip ftp password vk
SCE#ip ftp username vk
SCE#copy ftp://@10.1.1.253/h:/config.tmp myconf.txt
connecting 10.1.1.253 (user name vk password vk) to retrieve
config.tmp
SCE#
```

Managing Command Output

Some commands, such as many **show** commands, may have many lines of output. There are several ways of managing the command output:

- Scrolling options — When the command output is too large to be displayed all at once, you can control whether the display scrolls line by line or refreshes the entire screen.
- Filtering options — You can filter the output so that output lines are displayed only if they include or exclude a specified expression.
- Redirecting to a file — You can send the output to a specified file

Scrolling the Screen Display

The output of some **show** and **dir** commands is quite lengthy and cannot all be displayed on the screen at one time. Commands with many lines of output are displayed in chunks of 24 lines. You can choose to scroll the display line by line or refresh the entire screen. At the prompt after any line, you can type one of the following keys for the desired action:

- **<Enter>**— show one more line
- **<Space>** – show 24 more lines (a new chunk)
- **<g>** – Stop prompting for more
- **<?>** – Display a help string showing possible options

- Any other key – quit showing the file

Filtering Command Output

You can filter the output of certain commands, such as **show**, **more**, and **dir**, so that output lines are displayed only if they include or exclude a specified expression. The filtering options are as follows:

- **include** — Shows all lines that include the specified text.
- **exclude** — Does not show any lines that include the specified text.
- **begin** — Finds the first line that includes the specified text, and shows all lines starting from that line. All previous lines are excluded.

The syntax of filtered commands is as follows:

- `<command> | include <expression>`
- `<command> | exclude <expression>`
- `<command> | begin <expression>`

The `<expression>` in these commands is case sensitive.

EXAMPLE

Following is an example of how to filter the **show version** command to display only the last part of the output, beginning with the version information.

```
SCE# show version begin revision
```

Redirecting Command Output to a File

You can redirect the output of commands, such as **show**, **more**, and **dir**, to a file. When writing the output of these commands to a file, you can specify either of the following options:

- **redirect** — The new output of the command will overwrite the existing contents of the file.
- **append** — The new output of the command will be appended to the existing contents of the file.

The syntax of redirection commands is as follows:

- `<command> | redirect <file-name>`
- `<command> | append <file-name>`

EXAMPLE

Following is an example of how to do the following:

- Filter the **more** command to display from a *csv* subscriber file only the gold package subscribers.
- Redirect that output to a file named *current_gold_subscribers*. The output should not overwrite existing entries in the file, but should be appended to the end of the file.

```
SCE# more subscribers_10.10.2004 include gold append
current_gold_subscribers
```

CLI Scripts

The CLI scripts feature allows you to record several CLI commands together as a script and play it back. This is useful for saving repeatable sequence of commands, such as software upgrade. For example, if you are configuring a group of SCE Platforms and you want to run the same configuration commands on each platform, you could create a script on one platform and run it on all the other SCE Platforms.

The available script commands are:

- `script capture`
- `script stop`
- `script print`
- `script run`

To create a script:

Step 1 At the `SCE#` prompt, type `script capture sample1.scr` where `sample1.scr` is the name of the script.

Step 2 Perform the actions you want to be included in the script.

Step 3 Type `script stop`.

The system saves the script.

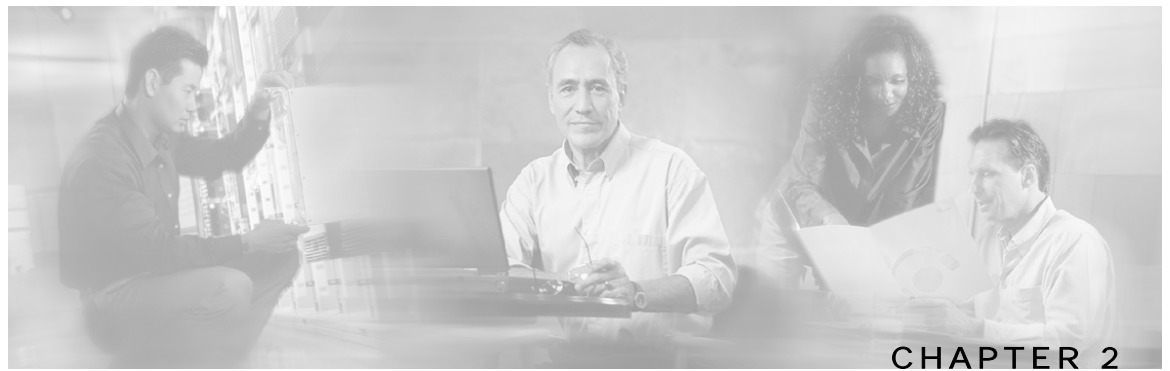
EXAMPLE:

The following is an example of recording a script for upgrading software.

```
SCE#script capture upgrade.scr
SCE#configure
SCE(config)#boot system new.pkg
Verifying package file...
Package file verified OK.
SCE(config)#exit
SCE#copy running-config startup-config
Writing general configuration file to temporary location...
Extracting files from '/tffs0/images/new.pkg'...
Verifying package file...
Package file verified OK.
Device '/tffs0/' has 81154048 bytes free, 21447973 bytes are
needed for extraction, all is well.
Extracting files to temp locations...
Renaming temp files...
Extracted OK.
Backing-up general configuration file...
Copy temporary file to final location...
SCE#script stop
```

To run the script recorded above, type:

```
SCE#script run upgrade.scr
```

CLI Command Reference

This chapter contains all the CLI commands available on the SCE platform.

This chapter contains the following sections:

- [Syntax and Conventions](#) 2-1
- [CLI Commands](#) 2-2

Each command description is broken down into the following sub-sections:

Command syntax	The general format of the command.
Description	Description of what the command does.
Default	If relevant, the default setting for the command.
Authorization	The level of user authorization required for using the command.
Mode	The mode (command line) from which the command can be invoked.
Parameters	Description of parameters and switches for the command.
Usage guidelines	Information about when to invoke the command and additional details.
Example	An illustration of how the command looks when invoked. Because the interface is straightforward, some of the examples are obvious, but they are included for clarity.

Syntax and Conventions

The CLI commands are written in the following format:

command *required-parameter* [*optional-parameter*]

[no] is an optional parameter that may appear before the command name.

- When typing commands, you may enclose parameters in double-quote marks, and you *must* do so when there is a space within a parameter name.
- Examples are shown in courier style. **Bold courier** is used to show the commands as you type them and regular courier is used for system prompts and responses.

CLI Commands

?

Lists all of the commands available for the current command mode. You can also use the ? command to get specific information on a keyword or parameter.

To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called partial help, because it lists only the keywords or arguments that begin with the abbreviation you entered.

Syntax Description

This command has no arguments or keywords

Defaults

This command has no default settings

Command Modes

All

Usage Guidelines

To list a command's associated keywords or arguments, enter a question mark (?) in place of a keyword or parameter on the command line. This form of help is called argument help because it lists the keywords or arguments that apply based on the command, keywords, and arguments you have already entered.

Authorization: User

Examples

The following example shows ways of requesting help using the ? wildcard.

```
SCE(config)#ip ?
default-gateway  Sets the default gateway
domain-lookup    Enables the IP DNS-based host name-to-address
translation
domain-name      Define a default domain name
host              Add a host to the host table
name-server      Specify the address of one or more name servers
to use for name and address resolution
route            Add IP routing entry
SCE(config)#ip d?
default-gateway  domain-lookup  domain-name
SCE(config)#ip de?
default-gateway
SCE(config)#ip de
```

Related Commands

access-class

Restricts Telnet server access to those addresses listed in the specified access list. Use the [no] form of this command to set the Telnet server to accept access from any address.

```
access-class number in
no access-class number in
```

Syntax Description

number An access-list number (1–99).

Defaults

No access list

Command Modes

Line Configuration Mode

Usage Guidelines

Authorization: admin

Examples

The following are examples of the access-class command:

EXAMPLE 1

The following example configures an access class for all Telnet lines.

```
SCE(config-line)#access-class 1 in
SCE(config-line)#
```

EXAMPLE 2

The following example removes an access class for Telnet lines.

```
SCE(config-line)#no access-class in
SCE(config-line)#
```

Related Commands

aaa authentication accounting commands

Enables TACACS+ accounting.

Use the **no** form of the command to disable TACACS+ accounting.

aaa authentication accounting commands *level* **default stop-start group tacacs+**

no aaa authentication accounting commands *level* **default**

Syntax Description	<i>level</i>	The privilege level for which to enable the TACACS+ accounting 0: User 5: Viewer 10: Admin 15: Root
Defaults	By default, TACACS+ accounting is disabled.	
Command Modes	Global Configuration	
Usage Guidelines	<p>If TACACS+ accounting is enabled, the SCE platform sends an accounting message to the TACACS+ server after every command execution. The accounting message is logged in the TACACS+ server for the use of the network administrator.</p> <p>The start-stop keyword (required) indicates that the accounting message is sent at the beginning and the end (if the command was successfully executed) of the execution of a CLI command.</p> <p>Authorization: admin</p>	
Examples	<p>The following example enables TACACS+ accounting for the admin privilege level (10).</p> <pre>SCE(config)# aaa authentication accounting commands 10 default stop-start group tacacs+</pre>	
Related Commands		

aaa authentication attempts

Sets the maximum number of login attempts that will be permitted before a Telnet session is terminated.

aaa authentication attempts login *number-of-attempts*

Syntax Description

number-of-attempts the maximum number of login attempts that will be permitted before the telnet session is terminated

Defaults

Default *number-of-attempts* = 3

Command Modes

Global Configuration

Usage Guidelines

The maximum number of login attempts is relevant only for Telnet sessions. From the local console, the number of re-tries is unlimited.

Authorization: admin

Examples

The following example shows how to set the maximum number of logon attempts to five.

```
product>(config)# aaa authentication attempts login 5
```

Related Commands

aaa authentication enable default

Specifies which privilege level authentication methods are to be used, and in what order of preference.

Use the no form of the command to delete the privilege level authentication methods list.

aaa authentication enable default *method1* [*method2...*]

no aaa authentication enable default

Syntax Description

method the privilege level authentication methods to be used. You may specify up to four different methods, in the order in which they are to be used

Defaults

Default privilege level authentication method = **enable** only

Command Modes

Global Configuration

Usage Guidelines

Use this command to configure "backup" privilege level authentication methods to be used in the event of failure of the primary privilege level authentication method.

The following method options are available:

- **group tacacs+**: Use TACACS+ authentication.
- **local**: Use the local username database for authentication.
- **enable** (default): Use the "**enable**" password for authentication
- **none**: Use no authentication.

If the privilege level authentication methods list is deleted, the default privilege level authentication method only (**enable** password) will be used. TACACS+ authentication will not be used.

Authorization: admin

Example

This example shows how to configure privilege level authentication methods,
SCE(config)# aaa authentication enable default group tacacs+ enable none

Related Commands

[aaa authentication login default](#) (on page 2-13)

access-list

Adds an entry to the bottom of the specified access list.

Use the **no** form of the command to remove an entry from the specified access list.

access-list *number permission address*

no access-list *number*

Syntax Description

<i>number</i>	An access-list number (1–99).
<i>permission</i>	Indicates whether the IP address should be allowed or denied access permission as described in the Valid Permission Values table in the Usage Guidelines..
<i>address</i>	Addresses to be matched by this entry as described in the Valid Address Values table in the Usage Guidelines.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The *SCE* platform can be configured with Access Control Lists (ACLs), which are used to permit or deny incoming connections on any of the management interfaces. An access list is an ordered list of entries, each consisting of an IP address and an optional wildcard “mask” defining an IP address range, and a permit/deny field.

The order of the entries in the list is important. The default action of the first entry that matches the connection is used. If no entry in the Access List matches the connection, or if the Access List is empty, the default action is **deny**.

Table 2-1 Valid Permission Values

<i>deny</i>	Deny access to list member
<i>permit</i>	Permit access to list member.

Table 2-2 Valid Address Values

<i>any</i>	All IP addresses are matched by this entry. This is equivalent to specifying the address 0.0.0.0 255.255.255.255
<i>ip-address</i>	The IP address or range of IP addresses, matched by this entry. This can be one address in the x.x.x.x format or a range of addresses in the format x.x.x.x y.y.y.y where x.x.x.x specifies the prefix bits common to all IP addresses in the range, and y.y.y.y is a mask specifying the bits that are ignored. In this notation, ‘1’ means bits to ignore. For example, the address 0.0.0.0 255.255.255.255 means any IP address. The address 10.0.0.0 0.1.255.255 means IP addresses from 10.0.0.0 to 10.1.255.255. The address 1.2.3.4 0.0.0.255 means IP addresses from 1.2.3.0 to 1.2.3.255 (A more natural way of expressing the same range is 1.2.3.0 0.0.0.255).

Authorization: admin

Examples

The following example adds entries to the bottom of access-list 1. The first entry permits access to 10.1.1.0 through 10.1.1.255. The second entry denies access to any address. Together this list allows access only to addresses 10.1.1.*.

```
SCE(config)#access-list 1 permit 10.1.1.0 0.0.0.255  
SCE(config)#access-list 1 deny any  
SCE(config)#
```

The following example defines access list 2, a list that denies access to all IP addresses in the range: 10.1.2.0 to 10.1.2.255, permits access to all other addresses in the range 10.1.0.0 to 10.1.15.255, and denies access to all other IP addresses. Note that since the first range is contained within the second range, the order of entries is important. If they had been entered in the opposite order, the **deny** entry would not have any effect.

```
SCE (config)#access-list 2 deny 10.1.2.0 0.0.0.255  
SCE (config)#access-list 2 permit 10.1.0.0 0.0.15.255  
SCE(config)#
```

Related Commands

accelerate-packet-drops

Enables the drop-red-packets-by-hardware mode. This improves performance, but prevents the application from being able to count all dropped packets.

Use the **no** form to disable the drop-red-packets-by-hardware mode, enabling the software to count all dropped packets (at the expense of some loss of performance).

accelerate-packet-drops

no accelerate-packet-drops

Syntax Description

This command has no arguments or keywords.

Defaults

By default, accelerate-packet-drops (the drop-red-packets-by-hardware mode) is enabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

By default, the SCE platform hardware drops red packets (packets that are marked to be dropped due to BW control criteria). However, this presents a problem for the user who needs to know the number of dropped packets per service.

The user can disable the drop-red-packets-by-hardware mode. The application can then retrieve the number of dropped packets for every flow and provide the user with better visibility into the exact number of dropped packets and their distribution.

Note that counting all dropped packets has a considerable affect on system performance, and therefore, by default, the drop-red-packets-by-hardware mode is enabled.

Authorization: admin

Examples

The following example shows how to disable the drop-red-packets-by-hardware mode so that the application can count all dropped packets.

```
(config if)# no accelerate-packet-drops
```

Related Commands

active-port

Specifies which management port is currently active.

Interface Mng *mng-port* active-port

Syntax Description	<i>mng-port</i> management port that is configured as the currently active management port: 0/1 or 0/2
--------------------	--

Defaults	default Mng port is 0/1.
----------	--------------------------

Command Modes	Mng Interface Configuration
---------------	-----------------------------

Usage Guidelines	The use of this command varies slightly, depending on whether the management interface is configured as a redundant interface (auto fail-over enabled) or not (auto fail-over disabled)
------------------	---

- auto fail-over enabled (automatic mode): the specified port becomes the currently active port, in effect forcing a fail-over action even if a failure has not occurred.
- auto fail-over disabled (manual mode): the specified port should correspond to the cabled Mng port, which is the only functional port and therefore must be and remain the active management port

Authorization: admin

Examples	The following example shows how to use this command to configure Mng port 2 as the currently active management port.
----------	--

```
SCE# Interface Mng 0/2 active-port
```

Related Commands	
------------------	--

attack-detector default

Defines default thresholds and attack handling action. If a specific attack detector is defined for a particular situation (protocol/attack direction/side), it will override these defaults.

Use the **no** version of this command to delete the user-defined defaults. The system defaults will then be used.

attack-detector default protocol *protocol* **attack-direction** *attack-direction* **side** *side* **action** *action* **open-flows** *open-flows* **ddos-suspected-flows** *ddos-suspected-flows* [**notify-subscriber**|**dont-notify-subscriber**] [**alarm**|**no-alarm**]

no attack-detector default protocol *protocol* **attack-direction** *attack-direction* **side** *side* **action** *action* **open-flows** *open-flows* **ddos-suspected-flows** *ddos-suspected-flows*

Syntax Description

protocol **TCP, UDP, ICMP, other**

attack-direction **attack-source, attack-destination, both**

side **subscriber, network, both**

action **report, block**

open-flows Threshold for concurrently open flows

ddos-suspected-flows Threshold for DDoS-suspected flows.

Defaults

The default values for the default attack detector are

- Action — Report
- Thresholds — Varies according to the attack type
- Subscriber notification — Disabled
- Sending an SNMP trap — Disabled

Command Modes

LineCard Interface Configuration

Usage Guidelines

Use the *notify-subscriber* keyword to enable subscriber notification.

Use the *dont-notify-subscriber* keyword to disable subscriber notification.

Use the *alarm* keyword to enable sending an SNMP trap.

Use the *no-alarm* keyword to disable sending an SNMP trap.

Authorization: admin

Examples

The following examples illustrate the use of the **attack-detector default** command:

EXAMPLE 1:

The following example configures a default attack detector for TCP flows from the attack source.

```
SCE(config if)#attack-detector default protocol TCP attack-  
direction attack-source side both action report open-flows 500  
ddos-suspected-flows 75
```

EXAMPLE 2:

The following example enables subscriber notification for the specified situation (protocol/attack direction/side).

```
SCE(config if)#attack-detector default protocol TCP attack-  
direction attack-source side both notify-subscriber
```

Related Commands

[attack-detector <number>](#) (on page 2-15)

aaa authentication login default

Specifies which login authentication methods are to be used, and in what order of preference.

Use the no form of the command to delete the login authentication methods list.

aaa authentication login default *method1* [*method2...*]

no aaa authentication login default

Syntax Description

method the login authentication methods to be used. You may specify up to four different methods, in the order in which they are to be used

Defaults

Default login authentication method = **enable** only

Command Modes

Global Configuration

Usage Guidelines

Use this command to configure "backup" login authentication methods to be used in the event of failure of the primary login authentication method.

The following method options are available:

- **group tacacs+**: Use TACACS+ authentication.
- **local**: Use the local username database for authentication.
- **enable** (default): Use the "**enable**" password for authentication
- **none**: Use no authentication.

If the login authentication methods list is deleted, the default login authentication method only (**enable** password) will be used. TACACS+ authentication will not be used.

Authorization: admin

Example

This example shows how to configure login authentication methods,

```
SCE(config)# aaa authentication login default group tacacs+
enable none
```

Related Commands

[aaa authentication enable default](#) (on page 2-6)

attack-detector

Enables the specified attack detector and assigns an access control list (ACL) to it.

attack-detector <*number*> **access-list** *access-list*

Syntax Description

number The attack detector number.

access-list The number of the ACL containing the IP addresses selected by this detector

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example enables attack detector number "2", and assigns ACL "8".
SCE(config if)# **attack-detector 2 access-list 8**

Related Commands

attack-detector <number>

Configures a specific attack detector for a particular attack type (protocol/attack direction/side) with the assigned number.

Use the **default** form of this command to configure the default attack detector for the specified attack type.

Use the **no** form of this command to delete the specified attack detector.

attack-detector <number> protocol (((TCP|UDP) [dest-port (specific|not-specific|both)]|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) [action (report|block)] [open-flows-rate <number> suspected-flows-rate <number> suspected-flows-ratio <number>] [notify-subscriber|dont-notify-subscriber] [alarm|no-alarm]

no attack-detector <number>

attack-detector default protocol (((TCP|UDP) [dest-port (specific|not-specific|both)]|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both) [action (report|block)] [open-flows-rate <number> suspected-flows-rate <number> suspected-flows-ratio <number>] [notify-subscriber|dont-notify-subscriber] [alarm|no-alarm]

no attack-detector default protocol (((TCP|UDP) [dest-port (specific|not-specific|both)]|ICMP|other|all) attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all) side (subscriber|network|both)

Syntax Description

<i>number</i>	Assigned number for attack-detector
<i>protocol</i>	TCP, UDP, ICMP, other
<i>destination port</i>	{TCP and UDP protocols only}: Defines whether the default attack detector applies to specific (port-based) or not specific (port-less) detections.
<i>attack-direction</i>	<i>single-side-destination single-side-both dual-sided all</i>
<i>side</i>	subscriber, network, both
<i>action</i>	report, block
<i>open-flows-rate</i>	Threshold for rate of open flows
<i>suspected-flows-rate</i>	Threshold for for rate of suspected DDoS flows.
<i>suspected-flows-ratio</i>	Threshold for ratio of suspected flow rate to open flow rate.

Defaults

The default values for the default attack detector are:

- Action: Report
- Thresholds: Varies according to the attack type
- Subscriber notification: Disabled

- Sending an SNMP trap: Disabled

Command Modes

LineCard Interface Configuration

Usage Guidelines

If a specific attack detector is defined for a particular attack type, it will override the configured default attack detector.

Use the appropriate keyword to enable or disable subscriber notification by default:

- **notify-subscriber**: Enable subscriber notification.
- **dont-notify-subscriber**: Disable subscriber notification.

Use the appropriate keyword to enable or disable sending an SNMP trap by default:

- **alarm**: Enable sending an SNMP trap.
- **no-alarm**: Disable sending an SNMP trap.

Authorization: admin

Examples

The following examples illustrate the use of the **attack-detector <number>** command:

EXAMPLE 1:

The following example configures the attack detector number "2".

```
SCE(config if)# attack-detector 2 protocol UDP dest-port not-
specific attack-direction single-side-destination side both
action block open-flows-rate 500 suspected-flows-rate 500
suspected-flows-ratio 50 notify-subscriber alarm
```

EXAMPLE 2:

The following example deletes attack detector number "2".

```
SCE(config if)#no attack-detector 2
```

EXAMPLE 3:

The following example disables subscriber notification for attack detector number "2".

```
SCE(config if)#attack-detector 2 dont-notify-subscriber
```

Related Commands

[attack-detector default](#) (on page 2-11)

attack-detector TCP-port-list|UDP-port-list

Defines the list of destination ports for specific port detections for TCP or UDP protocols.

attack-detector <number> (**TCP-port-list|UDP-port-list**) (*all*|(<port1> [<port2> ...]))

Syntax Description

number number of the attack detector for which this list of specific ports is relevant

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

TCP and UDP protocols may be configured for specified ports only. This is the list of specified destination ports per protocol.

Up to 15 different TCP port numbers and 15 different UDP port numbers can be specified.

Configuring a TCP/UDP port list for a given attack detector affects only attack types that have the same protocol (TCP/UDP) and are port-based (i.e. detect a specific destination port). Settings for other attack types are not affected by the configured port list(s).

Specify either **TCP-port-list** or **UDP-port-list**.

Use the **all** keyword to include all ports in the list.

Authorization: admin

Examples

This example shows how to configure the destination port list for the TCP protocol for attack detector #10.

```
SCE(config if)# attack-detector 10 TCP-port-list 100 101 102 103
```

Related Commands

attack-filter (LineCard Interface Configuration)

Enables specific attack detection for a specified protocol and attack direction.

Use the **no** form of the command to disable attack detection.

attack-filter [protocol (((TCP|UDP) [dest-port (specific|non-specific|both)]|ICMP|other)]
[attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all)]

no attack-filter [protocol (((TCP|UDP) [dest-port (specific|non-specific|both)]|ICMP|other)]
[attack-direction (single-side-source|single-side-destination|single-side-both|dual-sided|all)]

Syntax Description

protocol TCP, UDP, ICMP, or Other

attack direction: defines whether specific IP detection is enabled or disabled for single sided or dual sided attacks.

destination port (TCP and UDP protocols only): Defines whether specific IP detection is enabled or disabled for port-based (specific) or port-less (non-specific) detections.

Defaults

By default, attack-filter is enabled

Default *protocols*: all protocols (no protocol specified)

Default *attack direction*: all directions

Default *destination port*: both port-based or port-less

Command Modes

LineCard Interface Configuration

Usage Guidelines

By default, specific-IP detection is enabled for all attack types. You can configure specific IP detection to be enabled or disabled for a specific, defined situation only, depending on the following options:

- For a selected protocol only.
- For TCP and UDP protocols, for only port-based or only port-less detections.
- For a selected attack direction, either for all protocols or for a selected protocol.

Authorization: admin

EXAMPLE 1

The following example shows how to enable specific, dual-sided attack detection for TCP protocol only.

```
SCE(config if)#attack-filter protocol TCP dest-port specific
attack-direction dual-sided
```

EXAMPLE 2

The following example shows how to enable single-sided attack detection for ICMP protocol only.


```
SCE(config if)# protocol ICMP attack-direction single-side-source
```

EXAMPLE 3

The following example disables attack detection for all non TCP, UDP, or ICMP protocols.

```
SCE(config if)#no attack-filter protocol other attack-direction  
all
```

Related Commands

[*attack-filter \(Privileged Exec\)*](#) (on page 2-20)

attack-filter (Privileged Exec)

The **attack-filter** command prevents attack filtering for a specified IP address/protocol. If filtering is already in process, it will be stopped.

When attack filtering has been stopped, it remains stopped until explicitly restored by another CLI command (either specific or general). Use the **no** form of this command to restore attack filtering.

When using the **force-filter** keyword, it forces attack filtering for a specified IP address/protocol. When attack filtering has been forced, it continues until explicitly stopped by another CLI command (either specific or general). Use the **no** form of this command to stop attack filtering.

attack-filter *slot-number* **ip** *ip-address* **protocol** *protocol* **attack-direction** *attack-direction* **side** *side* [**dont-filter**]

attack-filter *slot-number* **ip** *ip-address* **action** *action* **protocol** *protocol* **attack-direction** *attack-direction* **side** *side* [**force-filter**]

no attack-filter *slot-number* [**dont-filter**] [**all**]

no attack-filter *slot-number* [**force-filter**] [**all**]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

ip-address IP address from which traffic will not be filtered.

action *report, block*

protocol *TCP, UDP, ICMP, other*

attack-direction *attack-source, attack-destination, both*

side *subscriber, network, both*

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

After configuring the attack detectors, the SCE Platform automatically detects attacks and handles them according to the configuration. However, there are scenarios in which a manual intervention is desired, either for debug purposes, or because it is not trivial to reconfigure the SCE attack-detectors properly.

The user can use the CLI attack filtering commands to do the following:

- Prevent/stop filtering of an attack related to a specified IP address
- Force filtering of an attack related to a specified IP address

Attack filtering can be prevented for a specified IP address/protocol by executing a **dont-filter** CLI command. If filtering is already in process, it will be stopped. When attack filtering has been stopped, it remains stopped until explicitly restored by another CLI command (either **force-filter** or **no dont-filter**).

Attack filtering can be forced for a specified IP address/protocol. If filtering is already in process, it will be stopped. Forced attack filtering will continue until undone by an explicit CLI command (either **no force-filter** or **dont-filter**).

Use the **all** keyword to restore or stop all filtering.

Authorization: admin

Examples

The following are examples of the **attack-filter** command:

EXAMPLE 1:

The following example prevents attack filtering for the specified conditions.

```
SCE#attack-filter 0 ip 10.10.10.10 protocol TCP attack-direction  
attack-source side both dont-filter  
SCE#
```

EXAMPLE 2:

The following example restores all attack filtering.

```
SCE#no attack-filter 0 dont-filter all
```

EXAMPLE 3:

The following example forces attack filtering.

```
SCE#attack-filter 0 action block ip 10.10.10.10 protocol TCP  
attack-direction attack-source side both
```

EXAMPLE 4:

The following example stops all forced attack filtering.

```
SCE#no attack-filter 0 force-filter all
```

Related Commands

[attack-filter](#) ("[attack-filter \(LineCard Interface Configuration\)](#)" on page 2-18)

attack-filter subscriber-notification ports

Specifies a port as subscriber notification port. TCP traffic from the subscriber side to this port will never be blocked by the attack filter, leaving it always available for subscriber notification.

Use the **[no]** form of this command to remove the port from the subscriber notification port list.

attack-filter subscriber-notification ports *port*

no attack-filter subscriber-notification ports *port*

Syntax Description	<i>port</i> Port number. One port can be specified as the subscriber notification port.
--------------------	---

Defaults	This command has no default settings.
----------	---------------------------------------

Command Modes	LineCard Interface Configuration
---------------	----------------------------------

Usage Guidelines	
------------------	--

Authorization: admin

Examples	The following example defines adds ports to the subscriber notification port list. SCE(config if)# attack-filter subscriber-notification ports 100
----------	--

Related Commands	
------------------	--

auto-fail-over

Enables automatic fail-over on the Mng ports.

Use the no form of the command to disable automatic fail-over on the Mng ports.

auto-fail-over

no auto-fail-over

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the auto fail-over mode is enabled.

Command Modes

Interface Management Configuration

Usage Guidelines

This parameter can be configured for either management port, and is applied to both ports with one command.

The automatic mode must be enabled to support management interface redundancy. This mode automatically switches to the backup management link when a failure is detected in the currently active management link.

When the automatic fail-over mode is disabled, by default Mng port 1 is the active port. If Mng port 2 will be the active port, it must be explicitly configured as such (see [active-port](#) (on page 2-10))

Authorization: admin

Examples

This example shows how to disable the auto fail-over mode.

```
SCE(config if)# no auto-fail-over
```

Related Commands

[active-port](#) (on page 2-10)

auto-negotiate (GigabitEthernet only)

Configures the GigabitEthernet Interface auto-negotiation mode. Use this command to either enable or disable auto-negotiation. When set to no auto-negotiate, auto-negotiation is always disabled, regardless of the connection mode.

auto-negotiate
no auto-negotiate
default auto-negotiate

Syntax Description

This command has no arguments or keywords.

Defaults

On for active connection mode; Off for passive connection mode

Command Modes

GigabitEthernet Interface Configuration

Usage Guidelines

Note that auto-negotiation does not work when the SCE Platform is connected via an optical splitter.

Authorization: admin

Examples

The following example configures the SCE Platform to perform no auto-negotiation.

```
SCE(config if)#no auto-negotiate
SCE(config if)#
```

Related Commands

bandwidth

Sets Ethernet shaping.

bandwidth *bandwidth* **burst-size** *burstsize*

Syntax Description

bandwidth bandwidth measured in kbps.

burstsize Burst size in bytes.

Defaults

Bandwidth = 100000K (100 Mbps)

burst-size = 5000 (5K bytes)

Command Modes

FastEthernet Interface Configuration
GigabitEthernet Interface Configuration

Usage Guidelines

This command is valid for the FastEthernet and GigabitEthernet line interfaces only.

Interface FastEthernet 0/#
Interface GigabitEthernet 0/#

Authorization: admin

Examples

The following sets bandwidth and burst size.

```
SCE(config-if)#bandwidth 100000 burstsize 5000  
SCE(config-if)#
```

Related Commands

blink

Blinks a slot LED for visual identification. Use the **no** form of this command to stop the slot blinking.

blink slot *slot-number*

no blink slot *slot-number*

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

Not blinking

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example configures the SCE Platform to stop blinking.

```
SCE#no blink slot 0
SCE#
```

Related Commands

[show blink](#) (on page 2-150)

boot system

Specifies a new package file to install. The SCE Platform extracts the actual image file(s) from the specified package file only during the **copy running-config startup-config** command.

boot system *ftp://username[:password]@server-address[:port]/path/source-file destination-file*

no boot system

Syntax Description

ftp://...destination-file The ftp site and path of a package file that contains the new firmware. The filename should end with the .pkg extension.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use this command to upgrade the SCE Platform embedded firmware. The package file is verified for the system and checked that it is not corrupted. The actual upgrade takes place only after executing the **copy running-config startup-config** command and rebooting the SCE Platform.

Authorization: admin

Examples

The following example upgrades the system.

```
SCE(config)#boot system
ftp://vk:vk@10.1.1.230/downloads/SENum.pkg.pkg
Verifying package file...
Package file verified OK.
SCE(config)#exit
SCE#copy running-config startup-config
Backing -up configuration file...
Writing configuration file...
Extracting new system image...

Extracted OK.
```

Related Commands

calendar set

Sets the system calendar. The calendar is a system clock that continues functioning even when the system shuts down.

calendar set *hh:mm:ss day month year*

Syntax Description	
<i>hh:mm:ss</i>	Current local time in hours in 24-hour format, minutes and seconds (HH:MM:SS).
<i>day</i>	Current day (date) in the month.
<i>month</i>	Current month (by three-letter abbreviated name).
<i>year</i>	Current year using a 4-digit number.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Usage Guidelines Always coordinate between the calendar and clock by using the `clock read-calendar` command after setting the calendar.

For further information on setting the clock, see [Setting the Clock](#).

Authorization: admin

Examples The following example sets the calendar to 20 minutes past 10 AM, October 13, 2001, synchronizes the real-time clock to the calendar time, and displays the result.

```
SCE#calendar set 10:20:00 13 oct 2001
SCE#clock read-calendar
SCE#show calendar
10:20:03 UTC THU October 13 2001
SCE#show clock
10:20:05 UTC THU October 13 2001
SCE#
```

Related Commands [show calendar](#) (on page 2-151)
[show clock](#) (on page 2-152)

cd

Changes the path of the current working directory.

cd *new-path*

Syntax Description

new-path The path name of the new directory. This can be either a full path or a relative path.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The new path should already have been created in the local flash file system.

Authorization: admin

Examples

The following example shows the current directory and then changes the directory to the log directory located under the root directory.

```
SCE#pwd  
tffs0  
SCE#cd log  
SCE#pwd  
tffs0:log  
SCE#
```

Related Commands

clear arp-cache

Deletes all dynamic entries from the ARP cache.

The Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses to physical addresses. Dynamic entries are automatically added to and deleted from the cache during normal use. Entries that are not reused age and expire within a short period of time. Entries that are reused have a longer cache life.

clear arp-cache

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example clears the ARP cache.

```
SCE#clear arp-cache
SCE#
```

Related Commands

clear interface linecard

Clears the linecard Interface counters.

clear interface linecard *slot-number* **counters**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example clears the Line-Card 0 counters.
SCE#clear interface linecard 0 counters
SCE#

Related Commands

clear interface linecard subscriber

Clears all anonymous subscribers in the system.

clear interface linecard *slot-number* subscriber anonymous all

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example clears all anonymous subscribers.

```
SCE#clear interface LineCard 0 subscriber anonymous all
```

Related Commands

[no subscriber](#) (on page 2-116)

clear interface linecard subscriber db counters

Clears the “total” and “maximum” subscribers database counters.

clear interface linecard *slot-number* subscriber db counters

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example clears all anonymous subscribers.

```
SCE#clear interface linecard 0 subscriber db counters
```

Related Commands

clear interface linecard 0 VAS-traffic-forwarding VAS all counters health-check

Clears the VAS health check counters.

Use the **all** keyword to clear counters for all VAS servers.

clear interface linecard *slot-number* **VAS-traffic-forwarding VAS server-id** *number*
counters health-check

clear interface linecard *slot-number* **VAS-traffic-forwarding VAS all counters health-check**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

number ID number of the specified VAS server clear the counters.

Defaults

This command has no default settings.

Command Modes

Privilege Exec

Usage Guidelines

Use the **all** keyword to clear counters for all VAS servers.

Authorization: admin

Examples

This example illustrates how to clear the health check counters for all VAS servers.

```
clear interface linecard 0 VAS-traffic-forwarding VAS all  
counters health-check
```

Related Commands

show interface linecard 0 VAS-traffic-forwarding (on page 2-188) (To display the VAS health check counters)

clear logger

Clears SCE Platform logger (user log files). This erases the information stored in the user log files.

When using the **counters** keyword, it clears the counters of the SCE Platform logger (user log files). The counters keep track of the number of info, warning, error and fatal messages.

When using the **nv-counters** keyword, it clears the non-volatile counters for the entire log or only the specified SCE Platform. These counters are not cleared during bootup, and must be cleared explicitly by using this command.

clear logger [**device** *User-File-Log/Line-Attack-File-Log*] [**counters|nv-counters**]

Syntax Description

device The device name to be cleared, either user-file-log or line-attack-file-log

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The users log files have a size limit, with new entries overwriting the oldest entries. Therefore, there is no need to regularly clear the log files. Use this operation when you are certain that the information contained on the logs is irrelevant and might be confusing (For example, when re-installing the system at a new site, whose administrators should not be confused with old information).

Authorization: admin

Examples

The following examples illustrate the use of the **clear logger** command:

EXAMPLE 1:

The following example clears the SCE platform user file logs:

```
SCE#clear logger device User-File-Log
Are you sure?Y
SCE#
```

EXAMPLE 2:

The following example clears the SCE platform user log file counters.

```
SCE#clear logger device User-File-Log counters
Are you sure?Y
SCE#
```

EXAMPLE 3:

The following example clears the user log file non-volatile counters.

```
SCE#clear logger device user-file-log nv-counters  
Are you sure?Y  
SCE#
```

Related Commands [show logger device User-File-Log](#) (on page 2-201)

clear interface linecard traffic-counter

Clears the specified traffic counter.

clear interface linecard *slot-number* **traffic-counter** *name* [**all**]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

name Name of the traffic counter to be cleared.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **all** keyword to clear all traffic counters.

Authorization: admin

Examples

The following example clears the traffic counter name counter1.

```
SCE#clear interface linecard 0 traffic-counter name counter1
```

Related Commands

clear RDR-formatter

Clears the RDR formatter counters.

clear RDR-formatter

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example clears the RDR-formatter counters.

```
SCE#clear RDR-formatter  
SCE#
```

Related Commands

show RDR-formatter (on page 2-209)

clock read-calendar

Synchronizes clocks by setting the system clock from the calendar.

clock read-calendar

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example updates the system clock from the calendar.

```
SCE#clock read-calendar  
SCE#
```

Related Commands

clock set

Manually sets the system clock.

clock set *hh:mm:ss day month year*

Syntax Description	
<i>hh:mm:ss</i>	Current local time in hours in 24-hour format, minutes and seconds (HH:MM:SS).
<i>day</i>	Current day (date) in the month.
<i>month</i>	Current month (by three-letter abbreviated name).
<i>year</i>	Current year using a 4-digit number.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Usage Guidelines Always coordinate between the calendar and clock by using the **clock update-calendar** command after setting the clock.

Authorization: admin

Examples The following example sets the clock to 20 minutes past 10 PM, October 13, 2001.

```
SCE#clock set 22:20:00 13 oct 2001
SCE#clock update-calendar
SCE#show clock
22:21:10 UTC THU October 13 2001
SCE#show calendar
22:21:18 UTC THU October 13 2001
SCE#
```

Related Commands [clock update-calendar](#) (on page 2-45)

[show calendar](#) (on page 2-151)

[show clock](#) (on page 2-152)

clock summertime

Configures the SCE Platform to automatically switch to daylight savings time on a specified date, and also to switch back to standard time. In addition, the three-letter time zone code can be configured to vary with daylight savings time if required. (For instance, in the eastern United States, standard time is designated EST, and daylight savings time is designated EDT).

Use the **no** form of this command to cancel the daylight savings time transitions configuration.

clock summertime

no clock summertime

The format of the command varies somewhat, depending on how the dates for the beginning and end of daylight savings time are determined for the particular location:

- recurring: If daylight savings time always begins and ends on the same day every year, (as in the United States):

Use the **clock summer-time recurring** command

- The *year* parameter is not used
- not recurring: If the start and end of daylight savings time is different every year, (as in Israel):

Use the **clock summer-time** command

- The *year* parameter must be specified

General guidelines for configuring daylight savings time transitions:

- Specify the three letter time zone code for daylight savings time.
- recurring: specify a day of the month (week#|first|last/day of the week/month).
- not recurring: specify a date (month/day of the month/year).
- Define two days:
 - Day1 = beginning of daylight savings time.
 - Day2 = end of daylight savings time.

In the Southern hemisphere, month2 must be before month1, as daylight savings time begins in the fall and ends in the spring.

- Specify the exact time that the transition should occur (24 hour clock).
 - Time of transition into daylight savings time: according to local standard time.
 - Time of transition out of daylight savings time: according to local daylight savings time.

For the **clock summer-time recurring** command, the default values are the United States transition rules:

- Daylight savings time begins: 2:00 (AM) on the first Sunday of April.
- Daylight savings time ends: 2:00 (AM) on the last Sunday of October.

Syntax Description	
<i>zone</i>	The 3-letter code for the time zone for daylight savings.
<i>week1/week2</i>	The week of the month on which daylight savings begins (<i>week1</i>) and ends (<i>week2</i>). A day of the week, such as Monday, must also be specified. The week/day of the week is defined for a recurring configuration only. Default: Not used
<i>day1/day2</i>	The day of the week on which daylight savings begins (<i>day1</i>) and ends (<i>day2</i>). For recurrent configuration: day is a day of the week, such as Sunday. Use the keywords <i>first/last</i> to specify the occurrence of a day of the week in a specified month: For example: last Sunday March. For non-recurrent configuration: day is a day in the month, such as 28. Default: day1 = first Sunday, day2 = last Sunday
<i>month1/month2</i>	The month in which daylight savings begins (<i>month1</i>) and ends (<i>ends2</i>). Default: month1 = April, month2 = October
<i>year1/year2</i>	The year in which daylight savings begins (<i>month1</i>) and ends (<i>ends2</i>). For non-recurring configuration only. Default = not used
<i>time1/time2</i>	The time of day (24-hour clock) at which daylight savings begins (<i>time1</i>) and ends (<i>time2</i>). Required for all configurations. Default: time1/time2 = 2:00
<i>offset</i>	The difference in minutes between standard time and daylight savings time. Default = 60

Defaults

recurring, offset = 60 minutes

- Daylight savings time begins: 2:00 (AM) on the first Sunday of April.
- Daylight savings time ends: 2:00 (AM) on the last Sunday of October.

Command Modes

Global Configuration

Usage Guidelines

Use the **recurring** keyword to enable subscriber notification.

Use the **first/last** keywords to specify the occurrence of a day of the week in a specified month: For example: last Sunday March.

Use a specific date including the year for a not recurring configuration. For example: March 29, 2004.

Use week/day of the week/month (no year) for a recurring configuration:

- Use first/last occurrence of a day of the week in a specified month. For example: last, Sunday, March (the last Sunday in March).
- Use the day of the week in a specific week in a specified month. For example: 4,Sunday, March (the fourth Sunday in March). This would be different from the last Sunday of the month whenever there were five Sundays in the month.

Authorization: admin

Examples

The following examples illustrate the use of the **clock summertime** command:

EXAMPLE 1:

The following example shows how to configure recurring daylight savings time for a time zone designated "DST" as follows:

- Daylight savings time begins: 0:00 on the last Sunday of March.
- Daylight savings time ends: 23:59 on the Saturday of fourth week of November.
- Offset = 1 hour (default)

```
SCE(config)#clock summer-time DST recurring last Sunday March
00:00 4 Saturday November 23:59
```

EXAMPLE 2:

The following example shows how to configure non-recurring daylight savings time for a time zone designated "DST" as follows:

- Daylight savings time begins: 0:00 on April 16, 2005.
- Daylight savings time ends: 23:59 October 23, 2005.
- Offset = 1 hour (default)

```
SCE(config)#clock summer-time DST April 16 2005 00:00 October 23
2005 23:59
```

EXAMPLE 3:

The following example shows how to cancel the daylight savings configuration.

From the **SCE(config)#** prompt, type **no clock summer-time** and press **Enter**.

```
SCE(config)#no clock summer-time
```

Related Commands

clock timezone

Sets the time zone. Use the no version of this command to remove current time zone setting. The purpose of setting the time zone is that the system can correctly interpret time stamps data coming from systems located in other time zones.

clock timezone *zone hours [minutes]*

no clock timezone

Syntax Description		
	<i>zone</i>	The name of the time zone to be displayed.
	<i>hours</i>	The hours offset from GMT (UTC). This must be an integer in the range -23 to 23.
	<i>minutes</i>	The minutes offset from GMT (UTC). This must be an integer in the range of 0 to 59. Use this parameter to specify an additional offset in minutes when the offset is not measured in whole hours.

Defaults GMT (hours = 0)

Command Modes Global Configuration

Usage Guidelines

Authorization: admin

Examples The following example sets the time zone to Pacific Standard Time with an offset of 10 hours behind GMT.

```
SCE(config)#clock timezone PST -10
SCE(config)#
```

Related Commands

clock update-calendar

Synchronizes clocks by setting the calendar from the system clock.

clock update-calendar

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example updates the calendar according to the clock.

```
SCE#clock update-calendar  
SCE#
```

Related Commands

[clock set](#) (on page 2-40)

[show calendar](#) (on page 2-151)

[show clock](#) (on page 2-152)

configure

Enables the user to move from Privileged Exec Mode to Configuration Mode.

configure

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

After the user enters the **configure** command, the system prompt changes from <host-name># to <host-name> (config)#, indicating that the system is in Global Configuration Mode. To leave Global Configuration Mode and return to the Privileged Exec Mode prompt, type **exit**.

Authorization: admin

Examples

The following example enters the Global Configuration Mode.

```
SCE#configure
SCE(config)#
```

Related Commands

[exit](#) (on page 2-65)

connection-mode (SCE 1000 platform)

Sets the connection mode to either inline (on the wire) or receive-only (using beam splitter or switch).

connection-mode *connection-mode* **on-failure** *on-failure*

Syntax Description

connection-mode inline or receive-only setting.

inline SCE Platform is connected in a bump-in-the-wire topology.

receive-only SCE Platform is connected in a out of the line topology using a beam splitter or switch.

On-failure determines system behavior on failure of the SCE Platform. (inline topologies only)

Bypass

cutoff

Defaults

connection mode = inline

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example sets the connection-mode to inline and the on-failure mode to cutoff.

```
SCE(config if)#connection-mode inline on-failure cutoff
```

Related Commands

connection-mode (SCE 2000 platform)

Sets the connection mode parameters.

connection-mode *connection-mode* **physically-connected-links** *physically-connected-links*
Priority *Priority* **On-failure** *On-failure*

Syntax Description

connection mode **inline**: single SCE Platform inline
receive-only: single SCE Platform receive-only
inline-cascade: two SCE Platforms inline
receive-only-cascade: two SCE Platforms receive-only

physically-connected-links The number of the link connected to the SCE Platform. (two SCE Platform topology only)
link 0
link 1

Priority Defines which is the primary SCE Platform.(two SCE Platform topologies only).
primary
secondary

On-failure Determines system behavior on failure of the SCE Platform. (inline topologies only)
Bypass
cutoff

Defaults

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example show how to configure the primary SCE Platform in a two-SCE Platform inline topology. Link "0" is connected to this SCE Platform, and the behavior of the SCE Platform if a failure occurs is "bypass".

```
SCE(config if)#connection-mode inline-cascade physically-connected-links link-0 priority primary on-failure bypass
SCE(config if)#
```

Related Commands

copy

Copies any file from a source directory to a destination directory on the local flash file system.

copy *source-file destination-file*

Syntax Description

source-file The name of the original file.

destination-file The name of the new destination file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Both file names should be in 8.3 format, that is, there are a maximum of 8 characters before the period and three characters following it.

Authorization: admin

Examples

The following example copies the local analysis.sli file located in the root directory to the applications directory.

```
SCE#copy analysis.sli applications/analysis.sli  
SCE#
```

Related Commands

copy ftp://

Downloads a file from a remote station to the local flash file system, using FTP.

copy ftp://username[:password]@server-address[:port]/path/source-file destination-file

Syntax Description

username The username known by the FTP server.

password The password of the given username.

server-address The dotted decimal IP address of the FTP server.

Port Optional port number on the FTP server.

source-file The name of the source file located in the on the server.

destination-file The name of the file to be saved in the local flash file system. The file should be in 8.3 format, that is 8 digits, dot, then 3 digits.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the following syntax for remote upload/download using FTP:

ftp://username[:password]@server-address[:port]/path/file

You can configure keyword shortcuts for the **copy** command using the following commands:

- **IP ftp password** to configure a password shortcut.
- **IP ftp username** to configure a username shortcut.

Authorization: admin

Examples

The following example downloads the ftp.sli file from the host 10.1.1.105 with user name “vk” and password “vk”.

```
SCE#copy ftp://vk:vk@10.1.1.105/p:/applications/ftp.sli
SCE#
```

Related Commands

copy-passive

Uploads or downloads a file using passive FTP.

copy-passive *source-file* **ftp://username[:password]@server-address[:port]/path/destination-file**
[overwrite]

Syntax Description

source-file The name of the source file located in the local flash file system.
username The username known by the FTP server.
password The password of the given username.
server-address The dotted decimal IP address.
port Optional port number on the FTP server.
destination-file The name of the file to be created in the FTP server.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the following format for remote upload/download using FTP:

ftp://username[:password]@serveraddress[:port]/path/file

Use the **overwrite** keyword to permit the command to overwrite an existing file.

You can configure keyword shortcuts for the **copy** command using the following commands:

- **IP ftp password** to configure a password shortcut.
- **IP ftp userName** to configure a username shortcut.

Authorization: admin

Examples

The following example performs the same operation as the previous copy ftp example using passive FTP.

```
SCE#copy-passive appl/analysis.sli  

ftp://myname:mypw@10.1.1.105/p:/applications/analysis.sli  

SCE#
```

Related Commands

copy running-config startup-config

Builds a configuration file with general configuration commands called `config.txt`, which is used in successive boots.

copy running-config startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

This command must be entered to save newly configured parameters, so that they will be effective after a reboot. You can view the running configuration before saving it using the **more running-config** command.

The old configuration file is automatically saved in the `tffs0:system/prevconf` directory.

Authorization: admin

Examples

The following example saves the current configuration for successive boots.

```
SCE#copy running-config startup-config
Backing-up configuration file...
Writing configuration file...
SCE#
```

Related Commands

copy source-file ftp://

Uploads a file to a remote station, using FTP.

copy *source-file* **ftp://***username[:password]@server-address[:port]/path/destination-file*

Syntax Description

source-file The name of the source file located in the local flash file system.

username The username known by the FTP server.

password The password of the given username.

server-address The dotted decimal IP address.

port Optional port number on the FTP server.

destination-file The name of the file to be created in the FTP server.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the following format for remote upload/download using FTP:

ftp://username[:password]@serveraddress[:port]/path/file

You can configure keyword shortcuts for the **copy** command using the following commands:

- **IP ftp password** to configure a password shortcut.
- **IP ftp userName** to configure a username shortcut.

Authorization: admin

Examples

The following example uploads the analysis.sli file located on the local flash file system to the host 10.1.1.105.

```
SCE#copy /appl/analysis.sli
ftp://myname:mypw@10.1.1.105/p:/applications/analysis.sli
SCE#
```

Related Commands

copy source-file startup-config

Copies the specified source file to the startup-config file.

Use this command to upload a backup configuration file created using the **copy startup-config destination-file** command.

This is useful in a cascaded solution for copying the configuration from one SCE platform to the other.

copy *source-file* **startup-config**

Syntax Description

source-file The name of the backup configuration file.

```
ftp://user:pass@host/drive:/dir/backupconfig.txt
/tffs0
```

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The source file name should be in 8.3 format, that is, there are a maximum of 8 characters before the period and three characters following it.

Authorization: admin

Examples

The following example shows how to upload a backup configuration file.

```
copy ftp://user:pass@host/drive:/dir/backupconfig.txt startup-config
```

Related Commands

[copy startup-config destination-file](#) (on page 2-55)

copy startup-config destination-file

Copies the startup-config file to the specified destination file.

Use this command to create a backup configuration file.

This is useful in a cascaded solution for copying the configuration from one SCE platform to the other. The file created by this command can then be uploaded to the second SCE platform using the **copy source-file startup-config** command.

copy startup-config destination-file

Syntax Description

destination-file The name of the file to which the configuration is copied.

```
ftp://user:pass@host/drive:/dir/backupconfig.txt
/tffs0
```

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The source file name should be in 8.3 format, that is, there are a maximum of 8 characters before the period and three characters following it.

Authorization: admin

Examples

The following example shows how to create a backup configuration file.

```
copy startup-config
ftp://user:pass@host/drive:/dir/backupconfig.txt
```

Related Commands

[copy source-file startup-config](#) (on page 2-54)

default subscriber template all

Removes all user-defined subscriber templates from the system. The default template only remains.

default subscriber template all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example removes all user-defined subscriber templates.

```
SCE(config if)# default subscriber template all
SCE(config if)#
```

Related Commands

delete

Deletes a file from the local flash file system.

Use the recursive switch to delete a complete directory and its contents. When used with the recursive switch, the filename argument specifies a directory rather than a file.

delete *file-name* [/recursive]

Syntax Description

file-name The name of the file or directory to be deleted.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the delete command:

EXAMPLE 1:

The following example deletes the oldlog.txt file.

```
SCE#delete oldlog.txt
SCE#
```

EXAMPLE 2:

The following example deletes the oldlogs directory.

```
SCE#delete oldlogs /recursive
3 files and 1 directories will be deleted.
Are you sure? y
3 files and 1 directories have been deleted.
SCE#
```

Related Commands

dir

Displays the files in the current directory.

dir [**applications**] [**-r**]

Syntax Description

applications Filters the list of files to display only the application files in the current directory.

-r Includes all files in the subdirectories of the current directory as well as the files in the current directory.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example displays the files in the current directory (root).

```
SCE#dir
File list for /tffs0/
512  TUE JAN 01 00:00:00 1980  LOGDBG          DIR
512  TUE JAN 01 00:00:00 1980  LOG             DIR
7653 TUE JAN 01 00:00:00 1980  FTP.SLI
29   TUE JAN 01 00:00:00 1980  SCRIPT.TXT
512  TUE JAN 01 00:00:00 1980  SYSTEM         DIR
SCE#
```

Related Commands

disable

Moves the user from a higher level of authorization to a lower user level.

disable [*level*]

Syntax Description

level User authorization level (0, 5, 10, 15) as specified in [CLI Authorization Levels](#) (on page 1-6).

Defaults

This command has no default settings.

Command Modes

Exec

Usage Guidelines

Use this command with the level option to lower the user privilege level. If a level is not specified, it defaults to User mode.

Authorization: user

Examples

The following example shows exits from root to admin mode:

```
SCE#>disable 10  
SCE#
```

Related Commands

do

Use the 'do' command to execute an EXEC mode command (such as a show command) or a privileged EXEC (such as **show running-config**) without exiting to the relevant command mode.

do *command*

Syntax Description

command command to be executed.

Defaults

This command has no default settings.

Command Modes

All configuration modes

Usage Guidelines

Use this command when in any configuration command mode (global configuration, linecard configuration or any interface configuration) to execute a user, viewer, or privileged exec command.

Enter the entire command with all parameters and keywords as you would if you were in the relevant command mode.

Authorization: admin

Examples

The following example assumes that the on-failure action of the SCE platform has been changed to 'bypass'. The connection mode configuration is then displayed to verify that the parameter was changed. The do command is used to avoid having to exit to the privileged exec mode.

```
SCE(config if)#connection-mode on-failure bypass
SCE(config if)#do show interface LineCard 0 connection-mode
```

Related Commands

duplex

Configures the duplex operation of the FastEthernet Interface to either half duplex, or full duplex. **auto** means auto-negotiation (do not force duplex on the link).

duplex *mode*

no duplex

Syntax Description	<i>mode</i> Set to auto , full or half to indicate the duplex mode.
Defaults	Auto
Command Modes	FastEthernet Interface Configuration
Usage Guidelines	<p>Changing this configuration takes effect only if the speed (see speed (on page 2-253)) is not configured to auto.</p> <p>Authorization: admin</p>
Examples	<p>The following example configures the FastEthernet port to half duplex mode.</p> <pre>SCE(config if)#duplex half SCE(config if)#</pre>
Related Commands	

enable

Enables the user to access a higher authorization level.

enable [*level*]

Syntax Description	<i>level</i> User authorization level (0, 5, 10, 15) as specified in CLI Authorization Levels (on page 1-6).
Defaults	admin
Command Modes	Exec
Usage Guidelines	If a level is not specified, the level defaults to the Privileged Exec mode, level 10. Authorization: User
Examples	The following example accesses the administrator authorization level. Note that the prompt changes from <i>SCE></i> to <i>SCE#</i> , indicating that the privilege is the administrator privilege level. SCE>enable Password: [pwd] SCE#
Related Commands	

enable password

Configures a password for the specified authorization level, thus preventing unauthorized users from accessing the SCE platform.

Use the **no** form of the command to disable the password for the specified authorization level.

enable password [**Level** *Level*] [*encryption-type*] *password*

no enable password [**Level** *level*]

Syntax Description

level User authorization level (0, 5, 10, 15) as specified in [CLI Authorization Levels](#) (on page 1-6). If no level is specified, the default is Admin (10).

encryption-type If you want to enter the encrypted version of the password, set the *encryption type* to **5**, to specify the algorithm used to encrypt the password.

password A regular or encrypted password set for the access level. If you specify *encryption-type*, you must supply an encrypted password.

Defaults

password: **pcube** or **cisco**

Command Modes

Global Configuration

Usage Guidelines

After the command is entered, any user executing the **enable** command must supply the specified password.

- Passwords must be at least 4 and no more than 100 characters long.
- Passwords can contain any printable characters.
- Passwords must begin with a letter.
- Passwords cannot contain spaces.
- Passwords are case-sensitive.

Authorization: admin

Examples

The following example sets a level 10 password as a123*man.

```
SCE(config)#enable password Level 10 a123*man
SCE(config)#
```

Related Commands

no enable password

erase startup-config-all

Removes all current configuration by removing all configuration files.

erase startup-config-all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

The following data is deleted by this command:

Usage Guidelines

- General configuration files
- Application configuration files
- Static party DB files
- Management agent installed MBeans

After using this command, the SCE platform should be reloaded immediately to ensure that it returns to the 'factory default' state.

Authorization: admin

The following example shows how to erase the startup configuration.

```
SCEconfig# erase startup-config-all
```

Example

Related Commands

exit

Exits the current mode and reverts to the mode used prior to the current mode.

exit

Syntax Description

This command has no arguments and keywords.

Defaults

This command has no default settings.

Command Modes

All

Usage Guidelines

Use this command each time you want to exit a mode. The system prompt changes to reflect the lower-level mode.

Authorization: admin

Examples

The following example exits from the Configure Interface Mode to Global Configuration Mode and then to Privileged Exec Mode.

```
SCE(config if)#exit
```

```
SCE(config)#exit
```

```
SCE#
```

Related Commands

failure-recovery operation-mode

Specifies the operation mode to be applied after boot resulting from failure. When using the **default** switch, you do not have to specify the mode.

failure-recovery operation-mode *mode*

default failure-recovery operation-mode

Syntax Description	<i>mode</i> operational or non-operational . Indicates whether the system will boot as operational or not following a failure.
Defaults	mode = operational
Command Modes	Global Configuration
Usage Guidelines	Authorization: admin
Examples	The following example sets the system to boot as operational after a failure <pre>SCE(config)#failure-recovery operation-mode operational SCE(config)#</pre>
Related Commands	

force failure-condition (SCE 2000 only)

Forces a virtual failure condition, and exits from the failure condition, when performing an application upgrade.

force failure-condition

no force failure-condition

Syntax Description

This command has no arguments or keywords

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example forces a virtual failure condition.
SCE(config if)#force failure-condition

Related Commands

help

Displays information relating to all available CLI commands.

help bindings|tree

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Exec

Usage Guidelines

Use the *bindings* keyword to print a list of keyboard bindings (shortcut commands).

Use the *tree* keyword to display the entire tree of all available CLI commands.

Authorization: User

Examples

The following example shows the partial output of the help bindings command.

SCE>help bindings

Line Cursor Movements

Ctrl-F /-> Moves cursor one character to the right.
 Ctrl-B /<- Moves cursor one character to the left.
 Esc-F Moves cursor one word to the right.
 Esc-B Moves cursor one word to the left.
 Ctrl-A Moves cursor to the start of the line.
 Ctrl-E Moves cursor to the end of the line.
 Esc F Moves cursor forward one word.
 Esc B Moves cursor backward one word.

Editing

Ctrl-D Deletes the character where the cursor is located.
 Esc-D Deletes from the cursor position to the end of the word.
 Backspace Deletes the character before the current location of the cursor.
 Ctrl-H " " " " " " " " " "
 Ctrl-K Deletes from the cursor position to the end of the line.
 Ctrl-U Deletes all characters from the cursor to the beginning of the line.
 Ctrl-X " " " " " " " " " "
 Ctrl-W Deletes the word to the left of the cursor.
 Ctrl-Y Recall the last item deleted.

Help and Operation Features

? Argument help.
 <Tab> Toggles between possible endings for the typed prefix.
 <Esc><Tab> Displays all the possible arguments backwards.
 Ctrl-I <TAB>

SCE>

 Related Commands

history

Enables the history feature, that is, a record of the last command lines that executed. Use the no form of this command to disable history.

history
no history

Syntax Description

This command has no arguments or keywords.

Defaults

History is enabled.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example enables the **history** feature.

```
SCE#history  
SCE#
```

The following example disables the **history** feature.

```
SCE#no history  
SCE#
```

Related Commands

history size

Sets the number of command lines that the system records in the history.

history size *size*

no history size

Syntax Description

size The number of command lines stored in the history of commands for quick recall.

Defaults

10 lines

Command Modes

Privileged EXEC

Usage Guidelines

The size of the history buffer can be any number from 0-50. Use the **[no]** form of this command to restore the default size.

Authorization: admin

Examples

The following example sets the history buffer size to 50 command lines.

```
SCE#history size 50
```

```
SCE#
```

Related Commands

hostname

Modifies the name of the SCE Platform. The host name is part of the displayed prompt.

hostname *host-name*

Syntax Description

host-name The new host name.

Defaults

SCE

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example changes the host name to MyHost.

```
SCE(config)#>hostname MyHost  
MyHost(config)#>
```

Related Commands

interface FastEthernet

Enters FastEthernet Interface Configuration mode.

interface FastEthernet *slot-number/interface-number*

Syntax Description

slot-number The number of the identified slot. Enter a value of **0**.

interface-number The FastEthernet interface number. Enter a value of **0** to configure the management port, or a value of **1 - 4** to configure one of the line ports.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use this command to configure the management port for the **SCE1000** and the **SCE2000** platforms.

This command is used to configure the line ports only for the **SCE 2000 4/8xFE**.

The system prompt is changed to reflect the Fast Ethernet Interface Configuration mode. To return to the Global Configuration Mode, type **exit**.

Authorization: admin

Examples

The following example enters into FastEthernet Configure Interface Mode.

```
SCE(config)#interface FastEthernet 0/0
```

```
SCE(config if)#
```

Related Commands

interface GigabitEthernet

Enters GigabitEthernet Interface Configuration mode.

interface GigabitEthernet *slot-number/interface-number*

Syntax Description

slot-number Enter a value of **0**.

interface-number The GigabitEthernet interface number. Enter a value of **1 - 4** to configure one of the line ports.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use this command to configure the line ports only for **SCE 2000 4xGBE** platform. This command is not used for configuring the management ports.

The SCE 1000 platform uses line ports 1 - 2 and the SCE 2000 platform uses line ports 1 - 4.

The system prompt is changed to reflect the GigabitEthernet Interface Configuration mode. To return to the Global Configuration Mode, type **exit**.

Authorization: admin

Examples

The following example enters into GigabitEthernet Configure Interface Mode to configure line port 1.

```
SCE(config)#interface GigabitEthernet 0/1
SCE(config if)#
```

Related Commands

interface LineCard

Enters LineCard Interface Configuration Mode.

interface LineCard *slot-number*

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The system prompt is changed to reflect the Line Card Configuration mode. To return to the Global Configuration Mode, type **exit**.

Authorization: admin

Examples

The following example enters LineCard Interface Configuration Mode.

```
SCE(config)#interface LineCard 0  
SCE(config if)#
```

Related Commands

interface Mng

Enters Management Interface Configuration mode.

interface Mng *slot-number/interface-number*

Syntax Description

slot-number The number of the identified slot. Enter a value of **0**.

interface-number The Management interface number. Enter a value of **1** or **2** to configure the desired Management port.

Defaults

This command has no default settings.

Command Modes

Management Interface Configuration

Usage Guidelines

Use this command to configure the management ports for the SCE platforms.

The system prompt is changed to reflect the Management Interface Interface Configuration mode. To return to the Global Configuration Mode, type **exit**.

Authorization: admin

Examples

The following example enters into Management Interface Configure Interface Mode.

```
SCE(config)#interface Mng 0/1
```

```
SCE(config if)#
```

Related Commands

ip access-class

Set the global IP access class. The access list defined here contains the definitions for all IP addresses with permission to access the SCE Platform system. IP addresses not permitted in this access list cannot access or detect the SCE Platform, that is, even a ping command will receive no response if it is not from a permitted IP address.

Use the no form of the command to reset global access to the SCE Platform from any IP address.

ip access-class *number*

no ip access-class

Syntax Description	<i>number</i> The access-class number.
Defaults	none (all IP addresses can access the system)
Command Modes	Global Configuration
Usage Guidelines	Authorization: admin
Examples	The following example sets access list 1 as the global access list. SCE(config)#ip access-class 1 SCE(config)#
Related Commands	no ip access-class

ip address

Sets the IP address and subnet mask of the FastEthernet Management Interface.

ip address *new-address subnet-mask*

Syntax Description

new-address The new IP address.

subnet-mask The network mask for the associated IP network.

Defaults

This command has no default settings.

Command Modes

FastEthernet Interface Configuration

Usage Guidelines

If there is a routing table entry mapped to the old address, but not to the new address, the command may fail.

This command is valid for the management interface only, **Interface FastEthernet 0/0**.

Authorization: admin

Examples

The following example sets the IP address of the SCE Platform to 10.1.1.1 and the subnet mask to 255.255.0.0.

```
SCE(config if)#ip address 10.1.1.1 255.255.0.0
SCE(config if)#
```

Related Commands

ip advertising

Enables IP advertising. If the destination and/or interval is not configured, the default values are assumed.

Use the **no** version of the command to disable IP advertising.

Use the **default** version of the command to restore IP advertising destination or interval to the default values.

ip advertising [*destination destination*] [*interval interval*]

no ip advertising

default ip advertising

Syntax Description

<i>destination</i>	The IP address of the destination for the ping requests Default: 127.0.0.1
<i>interval</i>	The frequency of the ping requests in seconds Default: 300 seconds

Defaults

disabled
 destination = 127.0.0.1
 interval = 300 seconds

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of the **ip advertising** command:

EXAMPLE 1:

The following example enables IP advertising, specifying 10.1.1.1 as the destination and an interval of 240 seconds.

```
SCE(config)#ip advertising destination 10.1.1.1 interval 240
SCE(config)#
```

EXAMPLE 2:

The following example restores the IP advertising destination to the default value.

```
SCE(config)#default ip advertising destination
SCE(config)#
```

Related Commands

ip default-gateway

Configures the default gateway for the SCE Platform. Use the **no** form of this command to unset the SCE Platform default gateway.

ip default-gateway *x.x.x.x*

no ip default-gateway

Syntax Description	<i>x.x.x.x</i> The IP address of the default gateway for the SCE Platform.
Defaults	This command has no default settings.
Command Modes	Global Configuration
Usage Guidelines	<p>Authorization: admin</p>
Examples	<p>The following example sets the default gateway IP of the SCE Platform to 10.1.1.1.</p> <pre><i>SCE</i>(config)#ip default-gateway 10.1.1.1 <i>SCE</i>(config)#</pre>
Related Commands	

ip domain-lookup

Enables or disables the domain name lookups.

Use the **no** form of the command to disable the domain name lookup.

ip domain-lookup

no ip domain-lookup

Syntax Description

This command has no arguments or keywords.

Defaults

enabled

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

EXAMPLE 1:

The following example enables the domain lookup.

```
SCE(config)#ip domain-lookup  
SCE(config)#
```

EXAMPLE 2:

The following example disables the domain lookup.

```
SCE(config)#no ip domain-lookup  
SCE(config)#
```

Related Commands

ip domain-name

Defines a default domain name. Use the **no** parameter of this command to remove the current default domain name. When using the **no** parameter, you do not have to specify the domain name.

ip domain-name *domain-name*

no ip domain-name

Syntax Description	<i>domain-name</i> The default domain name used to complete host names that do not specify a domain. Do not include the initial period that separates an unqualified name from the domain name.
--------------------	---

Defaults	This command has no default settings.
----------	---------------------------------------

Command Modes	Global Configuration
---------------	----------------------

Usage Guidelines

Authorization: admin

Examples	The following examples illustrate the use of the ip domain-name command:
----------	---

EXAMPLE 1:

The following example configures the domain name.
SCE(config)#ip domain-name Cisco.com
SCE(config)#

EXAMPLE 2:

The following example removes the configured domain name.
SCE(config)#no ip domain-name
SCE(config)#

Related Commands

ip filter fragment

Use this command to enable the filtering out of IP fragments.

The following options are available:

Enables or disables the filtering out of IP fragments.

ip filter fragment enable

ip filter fragment disable

Syntax Description

This command has no arguments or keywords.

Defaults

By default, IP fragment filtering is disabled.

Command Modes

Global Configuration

Usage Guidelines

Use the **enable** keyword to enable IP fragment filtering.

Use the **disable** keyword to disable IP fragment filtering.

User-configurable security mechanism: accomplished via two IP filters at user-configurable intervals:

- IP fragment filter: Drops all IP fragment packets
- IP filter monitor: Measures the rate of accepted and dropped packets for both permitted and not-permitted IP addresses.

This command configures the IP fragment filter.

Authorization: admin

Examples

The following example shows how to enable IP fragment filtering.

```
SCE(config)# ip filter fragment enable
```

Related Commands

[ip filter monitor](#) ("ip filter monitor" on page 2-84)

[show ip filter](#) (on page 2-195)

ip filter monitor

Configures the limits for permitted and not-permitted IP address transmission rates.

ip filter monitor { **ip_permitted** | **ip_not_permitted** } **low_rate** *low_rate* **high_rate** *high_rate*
burst *burst size*

Syntax Description	<p><i>low_rate</i> lower threshold; the rate in Mbps that indicates the attack is no longer present</p> <p><i>high_rate</i> upper threshold; the rate in Mbps that indicates the presence of an attack</p> <p><i>burst size</i> duration of the interval in seconds that the high and low rates must be detected in order for the threshold rate to be considered to have been reached</p>
Defaults	<p>Default low rate = 20 Mbps</p> <p>Default high rate = 20 Mbps</p> <p>Default burst size = 10 seconds</p>
Command Modes	<p>Global Configuration</p> <p>User-configurable security mechanism: accomplished via two IP filters at user-configurable intervals:</p>
Usage Guidelines	<ul style="list-style-type: none"> • IP fragment filter: Drops all IP fragment packets • IP filter monitor: Measures the rate of accepted and dropped packets for both permitted and not-permitted IP addresses. <p>This command configures the IP filter monitor.</p> <p>Use the ip permitted keyword to apply configured limits to permitted IP addresses.</p> <p>Use the ip not-permitted keyword to apply configured limits to not-permitted IP addresses.</p> <p>if this parameter is not specified, it is assumed that the configured limits apply to both permitted and not-permitted IP addresses.</p> <p>Authorization: admin</p>
Examples	<p>The following example shows how to configure the rates for both permitted and not-permitted IP addresses.</p> <pre>SCE(config)# ip filter monitor ip permitted low_rate 25 high_rate 30 burst 15</pre>
Related Commands	<p>ip filter fragment (on page 2-83)</p> <p>show ip filter (on page 2-195)</p>

ip ftp password

Specifies the password to be used for FTP connections for the current session. The system will use this password if no password is given in the copy FTP command.

ip ftp password *password*

Syntax Description

password The password for FTP connections.

Defaults

Default password is **admin**

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example sets the password to be used in the FTP connection to mypw.
SCE#ip ftp password mypw
SCE#

Related Commands

ip ftp username

Configures the username for FTP connections for the current session. This username will be used if no username is given in the copy FTP command.

ip ftp username *user-name*

Syntax Description

user-name The username for FTP connections.

Defaults

Default username is **anonymous**

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example sets myname as the username for FTP connections.

```
SCE#ip ftp username myname  
SCE#
```

Related Commands

ip host

Adds a host name and address to the host table.

Use the **no** form of the command to remove a host name and address from the host table.

ip host *hostname ip-address*

no ip host *hostname [ip-address]*

Syntax Description

hostname The host name to be added.

ip-address The host IP address in x.x.x.x format.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example adds a host to the host table.

```
SCE(config)#ip host PC85 10.1.1.61
```

```
SCE(config)#
```

Related Commands

no ip host

ip name-server

Specifies the address of 1–3 servers to use for name and address resolution. The system maintains a list of up to 3 name servers. If the current list is not empty, this command adds the specified servers to the list. The no option of this command removes specified servers from the current list.

ip name-server *server-address1* [*server-address2*] [*server-address3*]

no ip name-server

Syntax Description

server-address1 The IP address of the name server.

server-address2 The IP address of an additional name server.

server-address3 The IP address of an additional name server.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example adds the DNS 10.1.1.60 and 10.1.1.61 to the configured servers list.

```
SCE(config)#ip name-server 10.1.1.60 10.1.1.61
```

```
SCE(config)#
```

Related Commands

ip route

Adds or removes an IP routing entry to the routing table. Use the **no** option to remove an IP routing entry from the routing table.

ip route *prefix mask [next-hop]*
no ip route *prefix mask [next-hop]*
no ip route all

Syntax Description

prefix	The new entry's prefix.
mask	The new entry's subnet mask.
next-hop	The new entry's next hop in the route.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

All addresses must be in dotted notation.

The next-hop must be within the Management FastEthernet Interface subnet.

Use the **all** keyword with the **no** form of the command to remove all IP routing entries from the routing table.

Authorization: admin

Examples

The following examples illustrate the use of the **ip route** command:

EXAMPLE 1:

The following example sets the next-hop to 10.1.1.2 for IP addresses in the range 244.50.4.0 to 244.50.4.255.

```
SCE(config)#ip route 244.50.4.0 255.255.255.0 10.1.1.2  

SCE(config)#
```

EXAMPLE 2:

The following example removes the entry added in the previous example.

```
SCE(config)#no ip route 244.50.4.0 255.255.255.0  

SCE(config)#
```

Related Commands

ip rpc-adapter

Enables the RPC adapter. Use the **no** option of this command to disable the RPC adapter.

ip rpc-adapter

no ip rpc-adapter

Syntax Description

This command has no arguments or keywords

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of the **ip rpc-adapter** command:

EXAMPLE 1:

The following example enables the RPC adapter.

```
SCE(config)#ip rpc-adapter
```

EXAMPLE 2:

The following example disables the RPC adapter.

```
SCE(config)#no ip rpc-adapter
```

Related Commands

ip rpc-adapter port

Defines the RPC adapter port. Use the **default** option to reset the RPC adapter port assignment to the default port of 14374.

ip rpc-adapter port *port-number*

default ip rpc-adapter port

Syntax Description

port-number The number of the port assigned to the RPC adapter.

Defaults

The default port number is 14374

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of the **ip rpc-adapter port** command:

EXAMPLE 1:

The following example shows how to configure the RPC interface, specifying 1444 as the RPC adapter port.

```
SCE(config)#ip rpc-adapter  
SCE(config)#ip rpc-adapter port 1444
```

EXAMPLE 2:

The following example shows how reset the RPC adapter port.

```
SCE(config)#default ip rpc-adapter port
```

Related Commands

ip ssh

Enables the SSH server.

Use the **no** option to disable the SSH server.

ip ssh

no ip ssh

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of the **ip ssh** command:

EXAMPLE 1:

The following example enables the SSH server.

```
SCE(config)#ip ssh
```

```
SCE(config)#
```

EXAMPLE 2:

The following example disables the SSH server.

```
SCE(config)#no ip ssh
```

```
SCE(config)#
```

Related Commands

ip ssh access-class

Assigns an access class list (ACL) to the SSH server, so that access to the SSH server is limited to the IP addresses defined in the ACL. (See ACLs.)

Use the **no** keyword to remove the ACL assignment from the SSH server.

ip ssh access-class *access-list-number*
no ip ssh access-class

Syntax Description

access-list-number The access list number of an ACL

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

EXAMPLE 1:

The following example assigns an existing ACL to the SSH server.

```
SCE(config)#ip ssh access-class 4  

SCE(config)#
```

EXAMPLE 2:

The following example removes the ACL assignment from the SSH server.

```
SCE(config)#no ip ssh access-class  

SCE(config)#
```

Related Commands

ip ssh key

Generates or removes the SSH key set.

ip ssh key [generate|remove]

Syntax Description

generate generates a new SSH key set and saves it to non-volatile memory. Key size is always 2048 bits.

remove removes the existing key set.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

EXAMPLE 1:

The following example generates a new SSH key set.

```
SCE(config)#ip ssh key generate  
SCE(config)#
```

EXAMPLE 2:

The following example removes the SSH key set,

```
SCE(config)#ip ssh key remove  
SCE(config)#
```

Related Commands

ip-tunnel L2TP skip

Configures the recognition of L2TP tunnels and skipping into the internal IP packet. Use the **no** form of this command to disable tunnel recognition.

ip tunnel L2TP skip

no ip tunnel

Syntax Description

This command has no arguments or keywords

Defaults

ip tunnel recognition is disabled

Command Modes

LineCard Interface Configuration

Usage Guidelines

An IP tunnel is mutually exclusive with using VLAN for classification.

Authorization: admin

Examples

The following example enables recognition of L2TP tunnels.

```
SCE(config if)#ip tunnel L2TP skip
```

Related Commands

show tunnel mode

L2TP identify-by

Configures the port number that the LNS and LAC use for L2TP tunnels. The default port number is 1701.

L2TP identify-by port-number *port-number*

L2TP identify-by default port

Syntax Description	<i>port-number</i> The port number to be configured for L2TP tunnels.
Defaults	Default port-number = 1701
Command Modes	LineCard Interface Configuration
Usage Guidelines	Use the default port keyword to replace the user-configured port number with the default port. Authorization: admin
Examples	The following example identifies the L2TP port as being port# 1000. SCE(config if)#L2TP identify-by port-number <1000>
Related Commands	

line vty

Enters Line Configuration Mode for Telnet lines, configuring all Telnet lines.

line vty *start-number* [*end-number*]

Syntax Description

start-number A number in the range 0-4. The actual number supplied does not matter. All telnet lines will be configured by this command.

end-number A number in the range 0-4. The actual number supplied does not matter. All telnet lines will be configured by this command.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The system prompt changes to reflect the Line Configuration mode. To return to Global Configuration Mode, type **exit**.

Authorization: admin

Examples

The following example enters the Line Configuration Mode for all lines.

```
SCE(config)#line vty 0
```

```
SCE(config-line)#
```

Related Commands

link failure-reflection

Enables/disables the link failure reflection.

link failure-reflection [on-all-ports] [linecard-aware]

no link failure-reflection [linecard-aware-mode]

Syntax Description

on-all-ports Enables reflection of a link failure to all ports

linecard-aware Prevents link failure reflection if the indications are that the failure is in the line card (SCE 2000 4xGBE platforms only)

Defaults

By default, link failure reflection is disabled

Command Modes

LineCard Interface Configuration

Usage Guidelines

Use the **on-all-ports** keyword to enable reflection of a link failure to all ports

Use the **linecard-aware** keyword when each link of the SCE 2000 platform (Subscriber-side interface and the corresponding Network-side interface) is connected to a different linecard.

This mode reflects a failure of one port to the other three ports of the SCE 2000, differently, depending on whether the failure appears to be in the SCE platform itself or not, as follows:

- One interface of the SCE 2000 is down, indicating a problem with the SCE platform: Link failure is reflected to the other three SCE platform ports.
- Two reciprocal ports of the SCE 2000 are down, indicating a problem in the linecard to which the SCE platform is connected and not the interface: No action is taken. This allows the second link in the SCE platform to continue functioning without interruption

Use the **no** form of this command to disable failure reflection. The **on-all-ports** keyword is not used in the **no** form of the command.

Use the **no** form of this command with the **linecard-aware-mode** keyword to disable the linecard aware mode, without disabling link failure reflection itself.

Authorization: admin

Examples

The following example enables the reflection of a link failure to all ports:

```
SCE(config if)#link failure-reflection on-all-ports
SCE(config if)#
```

Related Commands

link mode

Configures the link mode. The link mode allows the user to enforce the specified behavior on the link. This may be useful during installation and for debugging the network.

link mode *link mode*

Syntax Description

<i>link</i>	Use this parameter for SCE 2000 platforms only GBE: GBE1-GBE2 GBE3-GBE4 FE: LINK1 LINK2 all-links
<i>mode</i>	Forwarding Bypass Cutoff Sniffing

Defaults

Command Modes

LineCard Interface Configuration

Usage Guidelines

Use the *link* parameter for the SCE 2000 4xGBE and the SCE 2000 4/8xFE platforms only. Since the SCE 1000 platform has only one link, it is not necessary to specify the link.

Use the 'all-links' keyword to configure the link mode for all links (SCE 2000 platforms only).

The 'sniffing' option can be configured only for all links (use the all-links' keyword).

Authorization: admin

Examples

The following examples illustrate the use of the link mode command:

EXAMPLE 1:

The following example configures "bypass" as the link mode on the first link for the SCE 2000 GBE platform.

```
SCE(config if)#link mode GBE1-GBE2 bypass
```

EXAMPLE 2:

The following example configures "forwarding" as the link mode for the SCE 1000 GBE platform.

```
SCE(config if)#link mode forwarding
```

EXAMPLE 3:

The following example configures "sniffing" as the link mode on all links for the SCE 2000 GBE platform.

```
SCE(config if)#link mode all-links sniffing
```

Related Commands

logger add-user-message

Adds a message string to the user log files.

logger add-user-message *message-text*

Syntax Description

message-text The message string you wish to add.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example adds "testing 123" as the message to the user log files:

```
SCE#Logger add-user-message "testing 123"  
SCE#
```

Related Commands

logger device User-File-Log

Disables or enables the logger device.

logger device User-File-Log *status*

Syntax Description	<i>status</i> enabled or disabled , indicating whether to turn on or off logging.
--------------------	---

Defaults	enabled
----------	----------------

Command Modes	Global Configuration
---------------	----------------------

Usage Guidelines	Authorization: admin
------------------	----------------------

Examples	The following example disables the User-File-Log device. SCE(config)#logger device User-File-Log disabled SCE(config)#
----------	--

Related Commands	
------------------	--

logger device User-File-Log max-file-size

Sets the maximum log file size.

logger device User-File-Log max-file-size

Syntax Description

size The maximum size for the user log (in bytes).

Defaults

1,000,000 bytes

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example configures the maximum size of the User-File-Log device to 65000 bytes.

```
SCE(config)#logger device User-File-Log max-file-size 65000  
SCE(config)#
```

Related Commands

logger get support-file

Generates a log file for technical support. Note that this operation may take some time.

logger get support-file *filename*

Syntax Description

filename Name of the generated log file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example generates a log file named *tech_sup* for technical support.

```
SCE#logger get support-file tech_sup  
SCE#
```

Related Commands

logger get user-log file-name

Outputs the current user log to a target file. The output file name can be a local path, full path, or full ftp path file name.

logger get user-log file-name *target-file*

Syntax Description

target-file The log file name where the system will write the log file information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example retrieves the current user log files.

```
SCE#logger get user-log file-name  
ftp://myname:mypw@10.1.1.205/d:/log.txt  
SCE#
```

Related Commands

logout

Logs out of the Command-Line Interface of the SCE Platform.

Logout

Syntax Description

This command has no arguments or keywords

Defaults

This command has no default settings.

Command Modes

Exec

Usage Guidelines

Authorization: User

Examples

The following example shows how the user logs out (and confirms the logout).

```
SCE>logout  
Are you sure? Y
```

Related Commands

management-agent access-class

Assigns an access class list (ACL) to the management agent, so that access to the management agent is limited to the IP addresses defined in the ACL. (See ACLs.)

Use the **no** keyword to remove the ACL assignment from the management agent.

management-agent access-class *access-list-number*

management-agent access-class

Syntax Description

access-list-number The access list number of an ACL

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

EXAMPLE 1:

The following example assigns an existing ACL to the management agent.

```
SCE(config)#management-agent access-class 4
SCE(config)#
```

EXAMPLE 2:

The following example removes the ACL assignment from the management agent.

```
SCE(config)#no management-agent access-class
SCE(config)#
```

Related Commands

management-agent sce-api logging

Enables the SCE subscriber API trouble-shooting logging, which is written to the user-log.

Use the **no** form of this command to disable SCE subscriber API trouble-shooting logging.

management-agent sce-api logging

no management-agent sce-api logging

Syntax Description

This command has no arguments or keywords

Defaults

By default, the SCE subscriber API trouble-shooting logging is disabled.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example enables SCE subscriber API trouble-shooting logging.

```
SCE(config)# management-agent sce-api logging
```

Related Commands

management-agent sce-api timeout

Defines the timeout interval for disconnection of an SCE subscriber API client, after which the resources allocated for this client would be released.

management-agent sce-api timeout *timeout-interval*

Syntax Description

timeout-interval default time in seconds that the client waits before timing out.

Defaults

Default = 300 seconds

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

This example shows how to configure a timeout interval of 10 seconds.

```
product>(config)# management-agent sce-api timeout 10
```

Related Commands

management-agent system

Specifies a new package file to install for the management agent. The SCE Platform extracts the actual image file(s) from the specified package file only during the **copy running-config startup-config** command.

When using the **no** version of this command, you do not have to specify the package-file-name.

management-agent system *package-file-name*

no management-agent system

Syntax Description

Package file name The name of a package file that contains the new management agent software. The filename should end with the .pkg extension.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use this command to upgrade the SCE Platform management agent. The package file is verified for the system and checked that it is not corrupted. The actual upgrade takes place only after executing the copy running-config startup-config command and rebooting the SCE Platform.

Authorization: admin

Examples

The following example upgrades the system with the *mng45.pkg* package.

```
SCE(config)#management-agent system mng45.pkg
Verifying package file...
Package file verified OK.
SCE(config)#exit
SCE#copy running-config startup-config
Backing -up configuration file...
Writing configuration file...
Extracting new management agent...
Extracted OK.
```

Related Commands

mkdir

Creates a new directory.

mkdir *directory-name*

Syntax Description

directory-name The name of the directory to be created.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example creates a new directory named mydir.

```
SCE#mkdir mydir
```

```
SCE#
```

Related Commands

more

Displays the contents of a file.

more *file-name*

Syntax Description

file-name The name of the file to be displayed.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The running-config option displays the running configuration file.

The startup-config option displays the startup configuration file.

Authorization: admin

Examples

The following partial sample output displays the content of some file.

```
SCE#more somefile.txt  
I am a happy little file.  
SCE#
```

Related Commands

[show running-config](#) (on page 2-216)

[show startup-config](#) (on page 2-228)

more user-log

Displays the user log on the CLI console screen.

more user-log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example displays the user log on the CLI console screen.

```
SCE#more user-log
```

```
<INFO>      | 01/28/97  22:29:22 | CPU #000 | Logger: Task  
Initialized successfully
```

Related Commands

MPLS

Configures the MPLS environment.

MPLS Traffic-Engineering skip

Syntax Description

This command has no parameters or keywords..

Defaults

By default, **Traffic-Engineering** is enabled.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Use the **Traffic-Engineering** keyword when all IP addresses are unique, and the MPLS labels may be omitted.

-

Authorization: admin

Examples

Related Commands

no subscriber

Removes a specified subscriber from the system. Use the 'all' form to remove all introduced subscribers.

no subscriber name *subscriber-name*

no subscriber all

Syntax Description	<i>subscriber-name</i> The specific subscriber name to be removed from the system.
--------------------	--

Defaults	This command has no default settings.
----------	---------------------------------------

Command Modes	LineCard Interface Configuration
---------------	----------------------------------

Usage Guidelines

Authorization: admin

Examples	<p>The following example removes all subscriber.</p> <pre>SCE(config if)# no subscriber all SCE(config if)#</pre>
----------	--

Related Commands

no subscriber anonymous-group

Removes a specified anonymous subscriber group from the system. Use the 'all' form to remove all anonymous subscriber groups.

no subscriber anonymous-group name *group-name*
no subscriber anonymous-group all

Syntax Description

group-name The anonymous subscriber group to be removed from the system.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example removes all anonymous subscriber groups.

```
SCE(config if)# no subscriber anonymous-group all  
SCE(config if)
```

Related Commands

no subscriber mappings included-in

Use this command to remove all existing subscriber mappings from a specified TIR or IP range.

no subscriber mappings included-in TP-IP-range name *TP-IP-range-name IP-range*

no subscriber mappings included-in IP-range *P-range*

Syntax Description	<i>TP-IP-range-name</i> Meaningful name assigned to this traffic processor IP range
	<i>IP-range</i> IP address and mask length defining the IP range

Defaults This command has no default settings.

Command Modes LineCard Interface Configuration

Usage Guidelines Use the **TP-IP-range name** parameter to remove all existing subscriber mappings from a specified TIR.

Use the **IP-range** parameter to remove all existing subscriber mappings from a specified IP range.

Authorization: admin

Examples The following example removes any existing subscriber mappings from the CTMS1 TIR.
SCE(config if)# no subscriber mappings included-in TP-IP-range name CMTS1

Related Commands

ping

Pings the given host to test for connectivity. The ping program sends a test message (packet) to an address and then awaits a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

ping *host*

Syntax Description

<i>host</i>	The host name or IP address of a remote station to ping.
-------------	--

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example pings the host 10.1.1.201.

```
SCE#ping 10.1.1.201
pinging 10.1.1.201 ...
PING 10.1.1.201: 56 data bytes
64 bytes from host (10.1.1.201): icmp_seq=0. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=1. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=2. time=0. ms
64 bytes from host (10.1.1.201): icmp_seq=3. time=0. ms
----10.1.1.201 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/0/0
SCE#
```

Related Commands

pqi install file

Installs the specified *pqi* file using the installation options specified (if any). This may take up to 5 minutes

pqi install file *filename* [*options options*]

Syntax Description

<i>filename</i>	The filename of the <i>pqi</i> application file to be installed.
<i>options</i>	The desired installation options. Use the show pqi file command to display the available installation options.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example installs the Subscriber Manager anr10015.pqi file. No options are specified.

```
SCE (config if)#pqi install file anr10015.pqi
```

Related Commands

[show pqi file](#) (on page 2-207)

pqi rollback file

Reverses an upgrade of the specified *pqi* file. This may take up to 5 minutes

pqi rollback file *filename*

Syntax Description

filename The filename of the *pqi* application file to be rolled-back. It must be the *pqi* file that was last upgraded.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Always specify the last *pqi* file that was upgraded.

Authorization: admin

Examples

The following example reverses the upgrade for the Subscriber Manager using the `anr100155.pqi` file.

```
SCE (config if)#pqi rollback file anr100155.pqi
```

Related Commands

pqi uninstall file

Uninstalls the specified *pqi* file. This may take up to 5 minutes

pqi uninstall file *filename*

Syntax Description

filename The filename of the *pqi* application file to be uninstalled. It must be the *pqi* file that was installed last.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Always specify the last *pqi* file that was installed.

Always run the **pqi uninstall** command before installing a new *pqi* file to prevent accumulation of old files on the disk.

Authorization: admin

Examples

The following example uninstalls the Subscriber Manager anr10015.pqi file.

```
SCE(config if)#pqi uninstall file anr10015.pqi
```

Related Commands

pqi upgrade file

Upgrades the application using the specified *pqi* file and the upgrade options specified (if any). This may take up to 5 minutes

pqi upgrade file *filename* [*options options*]

Syntax Description

<i>filename</i>	The filename of the <i>pqi</i> application file to be used for the upgrade.
<i>options</i>	The desired upgrade options. Use the show pqi file command to display the available options.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

A given *pqi* upgrade file is suitable for upgrading only from specific previously installed *pqi* files. The upgrade procedure checks that an upgrade is possible from the currently installed *pqi* file. The upgrade procedure will be stopped with an error message if the upgrade is not possible.

Authorization: admin

Examples

The following example upgrades the Subscriber Manager using the anr100155.pqi file. No options are specified.

```
SCE (config if)#pqi upgrade file anr100155.pqi
```

Related Commands

[show pqi file](#) (on page 2-207)

pwd

Displays the current working directory.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current working directory as tffs0.

```
SCE#pwd  
tffs0:  
SCE#
```

Related Commands

queue

Sets the queue shaping.

queue *queue-number* **bandwidth** *bandwidth* **burst-size** *burstsize*

Syntax Description

queue-number Queue-number from 1–4, where 4 is the highest priority (fastest). 1=BE, 2, 3=AF, and 4=EF. BE is the best effort queue, that is the lowest priority. EF is the Expedited Forwarding queue, that is the highest priority forwarding. The AF (Assured Forwarding) queues are middle-priority, with 3 being a higher priority queue, that is, packets from queue 3 are transferred faster than those in queue 2.

bandwidth Bandwidth measured in kbps. 0 disables packet transmission from the queue. The maximum bandwidth is determined by the line rate. Bandwidth is set in resolutions of ~140Kbps, that is rounded to the nearest multiple of approximately 140 Kbps.

burstsize Burst size in bytes, from 0–16000000.

Defaults

Bandwidth = 100000K (100 Mbps)

Burst size = 8000 (8K bytes)

Command Modes

FastEthernet Interface Configuration
GigabitEthernet Interface Configuration

Usage Guidelines

This command is valid for the FastEthernet and the GigabitEthernet line interfaces only.

Interface FastEthernet 0/#
Interface GigabitEthernet 0/#

Authorization: admin

Examples

The following sets queue shaping for queue 1.

```
SCE(config-if)#queue 2 bandwidth 20000 burstsize 1000  
SCE(config-if)#
```

Related Commands

RDR-formatter category-number

Assigns a meaningful name to a category. This category name can then be used in any **rdr-formatter** command instead of the category number. It also defines the buffer size.

Use the **no** option of this command to disassociate the name from the category. The name will then not be recognized by any CLI commands. Use the **default** form of this command to remove all configuration (name and buffer size).

RDR-formatter category-number [1-4] **name** *category name*

no RDR-formatter category-number [1-4] **name** *category name*

RDR-formatter category-number [1-4] **buffer-size** *size*

default RDR-formatter category-number [1-4] **buffer-size**

Syntax Description

category name The user-defined name to be assigned to the category.

size Buffer size

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example assigns the name “prepaid” to Category 1.

```
SCE(config)#RDR-formatter category-number 1 name prepaid
```

```
SCE(config)#
```

Related Commands

RDR-formatter destination

Configures an RDR destination entry. Up to four entries can be configured. Each entry must have a different priority. The entry with the highest priority is used by the RDR formatter, provided that a connection with this destination can be established. This is where the RDR-formatter sends the events produced by the LineCard Interface.

Use the all form of the command to remove the mappings of an RDR formatter destination to categories. When all categories for a destination are removed, the entire destination is removed.

RDR-formatter destination *ip-address* **port** *port-number* [**category** {**name** *category name* }|
{**number** [1-4]}] [**priority** *priority-value*]
no RDR-formatter destination *ip-address* **port** *port-number* [**category** {**name** *category name* }|
{**number** [1-4]}]
no RDR-formatter destination all

Syntax Description

ip-address The destination IP address.

port-number The destination port number.

category (Optional) Use this parameter to assign a priority to a particular category for this destination.

category name (Optional) User-defined name that identifies the category

number (Optional) Use this parameter to identify the category by number (1 to 4).

priority-value The priority of the destination. The priority value may be any number between 1 (lowest) to 100 (highest).

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The category may be identified by either name or number.

Assign a high priority to send RDRs from the specified category to this destination. Assign a low priority if RDRs from the specified category should not be sent to this destination.

For the first entry, if no priority is set, the highest priority is automatically assigned.

For all subsequent entries, the priority must be explicitly defined.

It is also possible to assign a different priority to each category for each destination. If no category is specified, the same priority is assigned to both categories for that destination.

Use the **all** keyword with the **no** form of the command to remove all of the configured RDR-formatter peer connection for the list of possible destinations.

Authorization: admin

Examples

The following examples illustrate the use of the **RDR-formatter destination** command:

EXAMPLE 1:

The following example configures an RDR-formatter destination with the default priority (highest) both categories.

```
SCE(config)#RDR-formatter destination 10.1.1.205 port 33000  
SCE(config)#
```

EXAMPLE 2:

The following example configures an RDR-formatter destination with a different priority for each category. This configuration will send RDRs from category 2 to this destination, but not RDRs from category 1.

```
SCE(config)#RDR-formatter destination 10.1.1.206 port 34000  
category number 1 priority 10 category number 2 priority 90  
SCE(config)#
```

Related Commands

no RDR-formatter destination all

show RDR-formatter destination (on page [2-212](#))

RDR-formatter forwarding-mode

Defines the mode in which the RDR formatter will send the RDRs to the destinations.

RDR-formatter forwarding-mode *mode*

Syntax Description

mode Settings: **redundancy**, **multicast**, **simple-load-balancing** as described in the Valid Mode Settings table in the Usage Guidelines.

Defaults

Default *mode* = **redundancy**

Command Modes

Global Configuration

Usage Guidelines

Table 2-3 Valid Mode Settings

redundancy	All RDRs are sent only to the primary (active) connection.
multicast	All RDRs are sent to all destinations.
simple-load-balancing	Not currently supported

Authorization: admin

Examples

The following example sets the RDR formatter mode to “**redundancy**”.

```
SCE(config)#RDR-formatter forwarding-mode redundancy
SCE(config)#
```

Related Commands

[show RDR-formatter forwarding-mode](#) (on page 2-214)

RDR-formatter history-size

Configures the size of the history buffer.

This command is currently not supported.

RDR-formatter history-size *size*

Syntax Description	<i>size</i> Size of the history buffer in bytes. Must be = 0 only (default)
Defaults	Default size = 0
Command Modes	Global Configuration
Usage Guidelines	<p>Do not change the size of the history buffer from the default value.</p> <p>Since currently only RDRv1 is supported, the size of the history buffer must be zero bytes, even though the system will accept a command specifying a larger size</p> <p>Authorization: admin</p>
Examples	
Related Commands	

RDR-formatter protocol

Defines the protocol (RDR formatter version) of the RDR formatter.

This command is currently not supported.

RDR-formatter protocol *protocol-version*

Syntax Description

protocol-version Must be **RDRv1**

Defaults

Default protocol-version = RDRv1

Command Modes

Global Configuration

Usage Guidelines

Do not change the RDR-formatter protocol version.

Only the default value, RDRv1, is supported.

Authorization: admin

Examples

Related Commands

RDR-formatter protocol RDRv2 connection-timeout

Configures the amount of time after which an inactive RDR formatter connection will timeout.

This command is currently not supported.

RDR-formatter protocol RDRv2 connection-timeout *time*

Syntax Description	<i>time</i>	Timeout value in seconds.
--------------------	-------------	---------------------------

Defaults	Default time = 10
----------	-------------------

Command Modes	Global Configuration
---------------	----------------------

Usage Guidelines	This command is currently not supported.
------------------	--

Authorization: admin

Examples

Related Commands

RDR-formatter rdr-mapping

Adds a dynamic RDR mapping to a category or removes one from a category.

Use the no form of this command to remove an existing mapping.

RDR-formatter rdr-mapping (tag-ID *tag number* category-number *category number*)

no RDR-formatter rdr-mapping (tag-ID *tag number* category-number *category number*)

Syntax Description

tag number The complete 32 bit value given as an hexadecimal number. The RDR tag must be already configured in the Formatter by the application.

category number Number of the category (1-4) to which to map the RDR tag

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The configuration of categories to RDR tags is done by adding and removing mappings. You can add a mapping of RDR tag to a category and remove a mapping, including the default mapping. If the table already contains a mapping with the same tag and category number, an error is issued and nothing is done.

If only one category is left configured for a certain tag, it cannot be removed.

Authorization: admin

Examples

The following examples illustrate how to add and remove mappings, and how to restore default mapping

EXAMPLE 1

This example shows how to add a mapping to a category.

RDR-formatter rdr-mapping tag-ID 0xf0f0f000 category-number 1

EXAMPLE 2

This example shows how to restore the default mapping for a specified RDR tag.

default RDR-formatter rdr-mapping tag-ID 0xf0f0f000

Related Commands

reload

Reboots the SCE Platform system.

reload



Warning

In order not to lose the current configuration, use the **copy running-config-all startup-config-all** command before using the **reload** command.

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows backing up of the configuration and performing a system reboot.

```
SCE#copy running-config-all startup-config-all
SCE#reload
Are you sure? Y
The system is about to reboot, this will end your CLI session
```

Related Commands

reload shutdown

Shuts down the SCE Platform system, preparing it for being turned off.

reload shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use this command to shut down the SCE Platform system in an orderly manner, before turning it off. After issuing this command, the only way to revive the SCE Platform from its power-down state is to turn it off, then back on.

This command can only be issued from the serial CLI console port. When issued during a telnet CLI session, an error message is returned and the command is ignored. This is done to prevent the possibility of shutting it down from a remote location, from which it is not possible to power back up.

Authorization: admin

Examples

The following example shows the shutdown process.

```
SCE#reload shutdown
```

```
You are about to shut down the system.
```

```
The only way to resume system operation after this  
is to cycle the power off, and then back on.
```

```
Continue?
```

```
Y
```

```
IT IS NOW SAFE TO TURN THE POWER OFF.
```

Related Commands

rename

Changes the file name to the specified name.

rename *existing-file-name* *new-file-name*

Syntax Description

existing-file-name The original name of the file.

new-file-name The new name of the file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example changes the name of file test1.pkg to test3.pkg.

```
SCE#rename test1.pkg test3.pkg
```

```
SCE#
```

Related Commands

rmdir

Removes an empty directory.

To remove a directory that is not empty, use the delete command with the recursive switch.

rmdir *directory-name*

Syntax Description

directory-name The name of the directory to be deleted.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

You can only remove an empty directory.

Authorization: admin

Examples

The following example deletes the code directory.
SCE#rmdir code
SCE#

Related Commands

script capture

Begins the recording of a script. It tracks all commands typed until the **script stop** command is used. Use this command to capture a sequence of repeated commands into a file for the purpose of executing the commands again. Use the **script stop** command to stop capturing the script.

script capture *script-file-name*

Syntax Description

script-file-name The name of the output file where the script is stored.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the script capture for the script1.txt.

```
SCE#script capture script1.txt
SCE#cd log
SCE#cd ..
SCE#pwd
SCE#script stop
```

Related Commands

[script stop](#) (on page 2-141)

script print

Displays a script file.

script print *script-file-name*

Syntax Description

script-file-name The name of the file containing the script.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example prints the commands captured in script1.txt.

```
SCE#script print script1.txt  
cd log  
cd ..  
pwd  
script stop  
SCE#
```

Related Commands

[script capture](#) (on page 2-138)

script run

Runs a script. The **halt** parameter causes the command to break script on errors.

script run *script-file-name* [**halt**]

Syntax Description

script-file-name The name of the file containing the script.

halt Stops the script running if one of the commands results in an error.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use this command to run a script that you have previously created using the **script capture** command.

Authorization: admin

Examples

The following example runs the script named script1.txt.

```
SCE#script run script1.txt
cd log
cd ..
pwd
tffs0:
script stop
SCE#
```

Related Commands

[script capture](#) (on page 2-138)

script stop

Stops script capture. Used in conjunction with the **script capture** command, it marks the end of a script being recorded.

script stop

Syntax Description

This command has no arguments or keywords.

Defaults

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example stops the capturing of a script.

```
SCE#script capture script1.txt
SCE#cd log
SCE#cd ..
SCE#pwd
SCE#script stop
SCE#
```

Related Commands

[script capture](#) (on page 2-138)

service password-encryption

Enables password encryption, so that the password remains secret when the configuration file is displayed. Use the **no** form of this command to disable password encryption.

service password-encryption
no service password-encryption

Syntax Description	This command has no arguments or keywords.
Defaults	Disabled (no encryption)
Command Modes	Global Configuration
Usage Guidelines	<p>Passwords that were configured in an encrypted format are not deciphered when password encryption is disabled.</p> <p>Authorization: admin</p>
Examples	<p>The following example shows the effect of enabling password encryption.</p> <pre> SCE#configure SCE(config)#enable password abcd SCE(config)#exit SCE#more running-config #This is a general configuration file (running-config). #Created on 10:20:57 ISR TUE July 3 2001 ... enable password level 10 0 "abcd" ... SCE#configure SCE(config)#service password-encryption SCE(config)#exit SCE#more running-config #This is a general configuration file (running-config). #Created on 10:21:12 ISR TUE July 3 2001 ... service password-encryption enable password level 10 5 "e2fc714c4727ee9395f324cd2e7f331f" ... SCE# </pre>
Related Commands	

service RDR-formatter

Enables/disables the RDR-formatter. The RDR-formatter is the element that formats the reports of events produced by the LineCard and sends them to an external data collector.

Use the **no** keyword of this command to disable the RDR-formatter.

service RDR-formatter

no service RDR-formatter

Syntax Description

This command has no arguments or keywords

Defaults

Enabled

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of the **service RDR-formatter** command:

EXAMPLE 1:

The following example enables the RDR-formatter.

```
SCE(config)#service rdr-formatter
SCE(config)#
```

EXAMPLE 2:

The following example disables the RDR-formatter.

```
SCE(config)#no service rdr-formatter
SCE(config)#
```

Related Commands

service telnetd

Enables/disables Telnet daemon. Use the **no** form of this command to disable the daemon preventing new users from accessing the SCE Platform via Telnet.

service telnetd

no service telnetd

Syntax Description

This command has no arguments or keywords,

Defaults

Telnet daemon enabled

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of the **service telnetd** command:

EXAMPLE 1:

The following example enables the Telnet daemon.

```
SCE(config)#service telnetd
```

```
SCE(config)#
```

EXAMPLE 2:

The following example disables the Telnet daemon.

```
SCE(config)#no service telnetd
```

```
SCE(config)#
```

Related Commands

setup

Invokes the setup utility, which is a dialog, or series of questions, that guides the user through the basic configuration process. This utility runs automatically upon initial connection to the local terminal. The utility may also be invoked explicitly to make changes to the system configuration.

setup

Following is a brief list of the parameters configured via the setup command:

- Host ID parameters: IP address, subnet mask, and hostname
- Passwords: admin password, password encryption
The root password can be configured upon initial system configuration and when accessed from the root user.
- Time settings: time zone, offset from UTC, local time and date
- SNMP configuration: multicast client, unicast server, unicast query interval
- Domain Name Server configuration: default domain name and IP address (up to 3)
- RDR-formatter destination: IP address and TCP port number
- Access Control Lists: up to 100 lists, with 20 IP addresses in each list, each entry can be designated as permitted or denied.

Create ACLs for IP access, Telnet access, SNMP GET community access, and SNMP SET community access as needed:

- SNMP configuration:
Define the following:
 - GET community names (up to 20)
 - SET community names (up to 20)
 - trap managers (up to 20): IP address, community string, version
 - name of system manager
- Topology configuration:
Define the following:
 - connection mode
 - administrative status after abnormal reboot
 - SCE 1000 Platform:
 - link-bypass mode when operational
 - redundancy
 - link-bypass mode when not operational
 - SCE 2000 Platform:
 - deployment type
 - physically-connected-link index

- priority
- on-failure link behavior

For a complete description of the command, see the SCE Platform Installation and Configuration Guide.

Syntax Description

The setup command does not include parameters in the usual sense of the word. However, the setup utility questions prompt for many global configuration parameters. Following is a table listing all parameters for which values may be requested by the setup dialog.

The table in the *Usage Guidelines* lists all the parameter values that are necessary to complete the initial configuration. It is recommended that you obtain all these values before beginning the setup.

Defaults

Command Modes

Privileged EXEC

Usage Guidelines

Table 2-4 Setup Command Parameters

Parameter	Definition
IP address	IP address of the SCE Platform.
subnet mask	Subnet mask of the SCE Platform.
default gateway	Default gateway.
hostname	Character string used to identify the SCE Platform
admin password	Admin level password.
root password	Root level password.
password encryption status	Character string from 4-100 characters beginning with an alpha character. Enable or disable password encryption?
Time Settings	
time zone name and offset	Standard time zone abbreviation and minutes offset from UTC.
local time and date	Current local time and date. Use the format: 00:00:00 1 January 2002
SNTP Configuration	
broadcast client status	Set the status of the SNTP broadcast client. If enabled, the SCE will synchronize its local time with updates received from SNTP broadcast servers.
unicast query interval	Interval in seconds between unicast requests for update (64 – 1024)

Parameter	Definition
unicast server IP address	IP address of the SNTP unicast server.
DNS Configuration	
DNS lookup status	Enable or disable IP DNS-based hostname translation.
default domain name	Default domain name to be used for completing unqualified host names
IP address	IP address of domain name server. (maximum of 3 servers)
RDR Formatter Destination Configuration	
IP address	IP address of the RDR-formatter destination
TCP port number	TCP port number of the RDR-formatter destination
Access Control Lists	
Access Control List number	How many ACLs will be necessary? What IP addresses will be permitted/denied access for each management interface? You may want ACLs for the following: <ul style="list-style-type: none"> • Any IP access • Telnet access • SNMP GET access • SNMP SET access
list entries (maximum 20 per list)	IP address, and whether permitted or denied access.
IP access ACL	ID number of the ACL controlling IP access.
telnet ACL	ID number of the ACL controlling telnet access.
SNMP Configuration	
SNMP agent status	Enable or disable SNMP management.
GET community names	Community strings to allow GET access and associated ACLs (maximum 20).
SET community names	Community strings to allow SET access and associated ACLs (maximum 20).
trap managers (maximum 20)	Trap manager IP address, community string, and SNMP version.
Authentication Failure trap status	Sets the status of the Authentication Failure traps.
enterprise traps status	Sets the status of the enterprise traps.
system administrator	Name of the system administrator.
Topology Configuration (Both Platforms)	
connection mode	Is the SCE Platform installed in bump-in-the-wire topology (inline) or out of line using splitter or switch (receive-only)?
Admin status of the SCE Platform after abnormal boot	After a reboot due to a failure, should the SCE Platform remain in a Failure status or move to operational status provided no other problem was detected?
Topology Configuration (SCE 1000)	

Parameter	Definition
link bypass mode on operational status	When the SCE 1000 is operational, should it bypass traffic or not?
redundant SCE 1000 platform?	Is there a redundant SCE 1000 installed as a backup?
link bypass mode on non-operational status	When the SCE 1000 is not operational, should it bypass traffic or cut it off?
Topology Configuration (SCE 2000)	
type of deployment	Is this a cascade topology, with two SCE Platforms connected via the cascade ports? Or is this a single platform topology?
physically connected link (cascade topology only)	In a cascade deployment this parameter sets the index for the link that this SCE 2000 is deployed on. The options for the SCE 2000 are link-0 or link-1. In a single-SCE 2000 Platform deployment this parameter is not relevant since one SCE 2000 is deployed on both links. In this case the link connected to port1-port2 is by default link-0 and the link connected to port3-port4 is by default link-1.
priority (cascade topology only)	If this is a cascaded topology, is this SCE 2000 the primary or secondary SCE 2000?
on-failure behavior (inline connection mode only)	If this SCE 2000 is deployed inline, should the failure behavior be bypass or cutoff of the link?

Authorization: admin

Examples

The following example runs the setup utility.

SCE#setup

```
--- System Configuration Dialog ---
```

```
At any point you may enter a question mark '?' followed by
'Enter' for help.
```

```
Use ctrl-C to abort configuration dialog at any prompt.
```

```
Use ctrl-Z to jump to the end of the configuration dialog at any
prompt.
```

```
Default settings are in square brackets '['].
```

```
Would you like to continue with the System Configuration Dialog?
[yes/no]: y
```

Related Commands

show access-lists

Shows all access-lists or a specific access list.

show access-lists [*number*]

Syntax Description

number Number of the access list to show

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example displays the configuration of access-list 1.

```
SCE#show access-lists 1
Standard IP access list 1
  Permit 10.1.1.0, wildcard bits 0.0.0.255
  deny any
SCE#
```

Related Commands

[access-list](#) (on page 2-7)

show blink

Displays the blinking status of a slot. A slot blinks after it receives a blink command.

show blink slot *slot-number*

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the blink status of slot 0.

```
SCE#show blink slot 0  
Slot 0 blink status: off
```

```
SCE#
```

Related Commands

[blink](#) (on page 2-26)

show calendar

Displays the time maintained by the real-time system calendar clock.

show calendar

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current system calendar.

```
SCE#show calendar
```

```
12:50:03 UTC MON November 13 2001
```

```
SCE#
```

Related Commands

[calendar set](#) (on page 2-28)

show clock

Displays the time maintained by the system clock.

show clock

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current system clock.

```
SCE#show clock
```

```
12:50:03 UTC MON November 13 2001
```

```
SCE#
```

Related Commands

[clock set](#) (on page 2-40)

show failure-recovery operation-mode

Displays the operation mode to apply after boot resulted from failure.

show failure-recovery operation-mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **failure-recovery operation-mode** command to configure this.

Authorization: admin

Examples

The following example displays the failure recovery operation mode:

```
SCE#show failure-recovery operation-mode
```

```
System Operation mode on failure recovery is: operational
```

```
SCE#
```

Related Commands

[failure-recovery operation-mode](#) (on page 2-66)

show hostname

Displays the currently configured hostname.

show hostname

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows that *SCE* is the current hostname.

```
SCE#show hostname
```

```
SCE
```

```
SCE#
```

Related Commands

[hostname](#) (on page 2-72)

show hosts

Displays the default domain name, the address of the name server, and the content of the host table.

show hosts

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the domain and hosts configured.

```
SCE#show hosts
```

```
Default domain is cisco.com
```

```
Name/address lookup uses domain service
```

```
Name servers are 10.1.1.60, 10.1.1.61
```

```
Host                Address
```

```
----                -
```

```
PC85                10.1.1.61
```

```
SCE#
```

Related Commands

show interface FastEthernet

Displays the details of a FastEthernet Interface.

show interface FastEthernet *slot-number/interface-number* [**counters** [*direction*]]**duplex****ip address****speed****queue** *queue-number*]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

interface-number FastEthernet interface number 0, 1 - 4.

direction Optional direction specification, to show only counters of a specific direction. Use **in** or **out**.

queue-number Number of queue, in the range 0-3.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The **counters** keyword displays the values of counters of a line FastEthernet interface (SCE 2000 4/8xFE platform only).

The **duplex** keyword displays the configured duplex mode and the actual status of it (Mng port only).

The **ip-address** keyword displays the currently configured IP address and subnet mask of the Management FastEthernet Interface (Mng port only).

The **speed** keyword displays the configured speed mode and the actual status of it (Mng port only).

The **queue** keyword displays the values of counters of a queue in a line FastEthernet interface (SCE 2000 4/8xFE platform only).

Enter a value of 0 for the interface number when using the **ip-address**, **duplex**, or **speed** keywords.

Enter a value of 1 - 4 in the *interface-number* parameter for line ports 1 - 4 to show information on the line interfaces for the **SCE 2000 4/8xFE** platform only (**counters** or **queue** keywords).

Authorization: admin

Examples

The following examples illustrate the use of the **show interface FastEthernet** command:

EXAMPLE 1:

The following example shows the FastEthernet details.

```
SCE#show interface FastEthernet 0/0
ip address: 10.1.6.145
subnet mask: 255.255.0.0
Configured speed: auto, configured duplex: auto
AutoNegotiation is On, link is Up, actual speed: 100, actual
duplex: half
SCE#
SCE#show interface FastEthernet 0/1
Configured speed: auto, configured duplex: auto
AutoNegotiation is On, link is Up, actual speed: 100Mb/s, actual
duplex: full
Bandwidth: 100000 Kbps, Burst-size: 5000 bytes
SCE#
```

EXAMPLE 2:

The following example shows the FastEthernet interface counters.

```
SCE#show interface FastEthernet 0/1 counters
In total octets: 191520
In good unicast packets: 560
In good multicast packets: 0
In good broadcast packets: 0
In packets discarded: 0
In packets with CRC/Alignment error: 0
In undersized packets: 0
In oversized packets: 0
Out total octets: 0
Out unicast packets: 0
Out non unicast packets: 0
Out packets discarded: 0
SCE#
```

EXAMPLE 3:

The following example shows the FastEthernet interface duplex mode configuration and status.

```
SCE#show interface FastEthernet 0/1 duplex
Configured duplex: auto
AutoNegotiation is On, link is Up, actual duplex: half
SCE#
```

EXAMPLE 4:

The following example shows the configured IP address.

```
SCE#show interface FastEthernet 0/0 ip address
Ip address: 10.1.5.120
Subnet mask: 225.255.0.0
SCE#
```

EXAMPLE 5:

The following example shows the FastEthernet interface speed configuration and status.

```
SCE#show interface FastEthernet 0/1 speed  
Configured speed: auto  
AutoNegotiation is On, link is Up, actual speed: 100  
SCE#
```

EXAMPLE 6:

The following example shows the FastEthernet interface queue number 3.

```
SCE#show interface FastEthernet 0/1 queue 3  
Bandwidth: 100000 Kbps, Burst-size: 8000 bytes  
SCE#
```

Related Commands

duplex (on page 2-61)

interface FastEthernet (on page 2-73)

ip address (on page 2-78)

queue (on page 2-125)

speed (on page 2-253)

show interface GigabitEthernet

Displays the details of a GigabitEthernet Interface.

show interface GigabitEthernet *slot-number/interface-number* [**counters** [*direction*]]**queue** *queue-number*]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

interface-number GigabitEthernet interface number 1 - 2, or 1 - 4.

direction Optional direction specification, to show only counters of a specific direction. Use **in** or **out**.

queue-number Number of queue, in the range 0-3

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Enter a value of 1 - 2 for the *interface-number* parameter for line ports 1 - 2 to show information on the line interfaces for the **SCE 1000 2xGBE** platform.

Enter a value of 1 - 4 for the *interface-number* parameter for line ports 1 - 4 to show information on the line interfaces for the **SCE 2000 4xGBE** platform.

The **counters** keyword displays the values of counters of a line GigabitEthernet interface.

The **queue** keyword displays the values of counters of a queue in a line GigabitEthernet interface.

Authorization: admin

Examples

The following example shows the GigabitEthernet details.
SCE#show interface GigabitEthernet0/1

Related Commands

show interface Mng

Displays the following information for the specified management interface.

- speed
- duplex
- IP address
- auto-fail-over (SCE 2000 platform only)

```
show interface Mng {0/1 | 0/2} [auto-fail-over|duplex|ip
address|speed]
```

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

interface-number Management interface number 1 - 2.

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

Speed and duplex parameters are specific to the selected interface (port), while other parameters apply to both ports and are displayed by a command to either interface.

Authorization: admin

Examples

This example shows how to display the statistics for the designated Management port.

```
SCE# show interface Mng {01 | 0/2} ip address
```

Related Commands

show interface LineCard

Displays information for a specific LineCard Interface.

show interface LineCard *slot-number*

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: user

Examples

The following example shows that the LineCard Interface does not currently have an application assigned to it.

```
SCE#show interface linecard 0  
No application is assigned to slot 0  
Silent is off  
Shutdown is off  
SCE#
```

Related Commands

[interface LineCard](#) (on page 2-75)

show interface LineCard application

Displays the name of the application assigned to the LineCard Interface.

show interface LineCard *slot-number* **application**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current application.

```
SCE#show interface LineCard 0 application
/tffs0/app/apricot.sli
SCE#
```

Related Commands

[interface LineCard](#) (on page 2-75)

show interface LineCard attack-detector

Displays the configuration of the specified attack detector.

show interface LineCard *slot-number* **attack-detector** [**default**|**all**]

show interface LineCard *slot-number* **attack-detector** *attack-detector*

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

attack-detector The number of the specific attack detector to be displayed.

all Displays the configuration of all existing attack detectors

default Displays the default attack detector configuration.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **all** keyword to display the configuration of all existing attack detectors.

Use the **default** keyword to display default attack detector configuration.

Authorization: admin

Examples

The following examples illustrate the **show interface LineCard attack-detector** command:

EXAMPLE 1:

The following example displays the configuration of attack detector number 3.

```
SCE#show interface LineCard 0 attack-detector 3
```

EXAMPLE 2:

The following example displays the configuration of the default attack detectors.

```
SCE#show interface LineCard 0 attack-detector default
```

EXAMPLE 3:

The following example displays the configuration of all existing attack detectors.

```
SCE#show interface LineCard 0 attack-detector all
```

Related Commands

[attack-detector](#) (on page 2-14)

show interface LineCard attack-filter

Displays the attack filtering configuration.

show interface LineCard *slot-number* **attack-filter** [*option*]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

option See Usage Guidelines for the list of options.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Following is a list of options that may be displayed:

- **query IP address configured**: displays the configured threshold values and action for the attack detector for a specified IP address
- **query IP address counters**: displays the current counters for the attack detector for all protocols and attack directions for a specified IP address
- **current-attacks**: displays all currently handled attacks
- **dont-filter**: displays all existing stopped attack filters
- **force-filter**: displays all existing forced attack filters
- **subscriber-notification ports**: displays the list of subscriber-notification ports

Authorization: admin

Examples

The following examples illustrate the use of the **show interface LineCard attack-filter** command:

EXAMPLE 1:

The following example displays the configuration of the attack detector for a specified IP address.

```
SCE#show interface LineCard 0 attack-filter query IP address
10.10.10.10 configured
```

EXAMPLE 2:

The following example displays all existing forced attack filters.

```
SCE#show interface LineCard 0 attack-filter force-filter
```

EXAMPLE 3:

The following example displays the subscriber notification ports.

```
SCE#show interface LineCard 0 attack-filter subscriber-  
notification ports
```

Related Commands

[attack-filter](#) ("[attack-filter \(LineCard Interface Configuration\)](#)" on page 2-18)

show interface LineCard connection-mode

Shows the LineCard Interface connection mode (inline or receive-only).

show interface LineCard *slot-number* **connection-mode**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the LineCard connection mode configuration parameter value.

```
SCE#show interface LineCard 0 connection-mode
inline
SCE#
```

Related Commands

[connection-mode \(SCE 2000 platform\)](#) (on page 2-48)

show interface LineCard counters

Displays the LineCard Interface hardware counters.

show interface LineCard *slot-number* **counters** [**bandwidth**] [**cpu-utilization**]

show interface LineCard *slot-number* **counters VAS-traffic-bandwidth** (SCE 2000 platform only)

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Specify any of the optional keywords to display only the desired counters.

Authorization: admin

Examples

The following example shows the hardware counters for the LineCard Interface.

```
SCE#show interface linecard 0 counters
DP packets in: 100
DP packets out: 100
DP IP packets in: 90
DP Non-IP packets: 10
DP IP packets with CRC error: 0
DP IP packets with length error: 0
DP IP broadcast packets: 10
DP IP fragmented packets: 0
DP IP packets with TTL=0 error: 0
DP Non TCP/UDP packets: 10
DP TCP/UDP packets with CRC error: 0
FF counter #0: 0
FF counter #1: 0
FF counter #2: 0
FF counter #3: 0
...
```

Related Commands

show interface LineCard link mode

Displays the configured LineCard Interface link mode.

show interface LineCard *slot-number* **link mode**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the configured link mode for the LineCard Interface.

```
SCE#show interface LineCard 0 link mode  
SCE#
```

Related Commands

[link mode](#) (on page 2-99)

show interface LineCard link-bypass (SCE 1000 only)

Displays the current LineCard link-bypass mode, as well as the configured modes for boot- time, normal operation, and failure.

show interface LineCard *slot-number* **link-bypass**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current and configured bypass modes.

```
SCE#show interface LineCard 0 link-bypass
```

```
Link-Bypass configuration according to status:
```

```
On-Boot      : Bypass
```

```
On-Operational: No-Bypass
```

```
On-Failure   : Bypass
```

```
Current bypass state is: No-Bypass
```

```
SCE#
```

Related Commands

show interface LineCard physically-connected-links (SCE 2000 only)

Displays the link mapping for the LineCard Interface.

show interface LineCard *slot-number* **physically-connected-links**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the link mapping for the LineCard Interface.

```
SCE#show interface LineCard 0 physically-connected-links  
slot 0 is connected to link-0 and link-1  
SCE#
```

Related Commands

show interface LineCard silent

Displays the current LineCard Interface silent state. When the silent state is Off, the LineCard events reporting function is enabled.

show interface LineCard *slot-number* silent

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the LineCard Interface silent mode.

```
SCE#show interface LineCard 0 silent  
Of f  
SCE#
```

Related Commands

[silent](#) (on page 2-242)

show interface LineCard subscriber

Displays subscribers meeting one of the following specified criteria:

- Having a value of a subscriber property that is equal to, larger than, or smaller than a specified value
- Having a subscriber name that matches a specific prefix
- Having a subscriber name that matches a specific suffix

Use the “amount” form to display the number of subscribers meeting the criteria rather than listing actual subscriber names.

show interface LineCard *slot-number* **subscriber** [amount] [**prefix** *prefix*] [**suffix** *suffix*] [**property** *propertyname* **equals|bigger-than|less-than** *property-val*]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

prefix The desired subscriber name prefix to match.

suffix The desired subscriber name suffix to match.

propertyname The name of the subscriber property to match.

property val The value of the specified subscriber property. Specify whether to search for values equal to, greater than, or less than this value.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

Following is an example that lists the number of subscribers with the prefix ‘gold’ in the subscriber name.

```
SCE#show interface linecard 0 subscriber amount prefix gold
There are 40 subscribers with name prefix 'gold'.
SCE#
```

Related Commands

show interface LineCard subscriber aging

Displays the subscriber aging for the specified type of subscriber (anonymous or introduced).

show interface LineCard *slot-number* **subscriber aging** [**anonymous|introduced**]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following is an example of how to display the aging of introduced subscribers.

```
SCE#show interface linecard 0 subscriber aging introduced  
SCE#
```

Related Commands

show interface LineCard subscriber anonymous

Displays the subscribers in a specified anonymous subscriber group. Use the “amount” form to display the number of subscribers in the group rather than a complete listing of members.

show interface LineCard *slot-number* **subscriber anonymous** [**amount**] [**name** *group-name*]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

group-name The anonymous subscriber group.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

If no group-name is specified, all anonymous subscribers in all groups are displayed.

Authorization: admin

Examples

The following is an example of how to display the number of subscribers in the anonymous subscriber group anon1.

```
SCE#show interface linecard 0 subscriber anonymous amount name
anon1
SCE#
```

Related Commands

show interface LineCard subscriber anonymous-group

Displays the configuration of the specified anonymous subscriber group. Use the “all” form with no group name to display all existing anonymous subscriber groups.

show interface LineCard *slot-number* **subscriber anonymous-group** [**name** *group-name*] [**all**]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

group-name The anonymous subscriber group.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following is an example of how to display the anonymous subscriber groups.

```
SCE#show interface linecard 0 subscriber anonymous-group  
SCE#
```

Related Commands

[subscriber anonymous-group export csv-file](#) (on page 2-255)

[subscriber anonymous-group import csv-file](#) (on page 2-256)

show interface LineCard subscriber db counters

Displays following subscriber database counters:

- Current number of subscribers
- Current number of introduced subscribers
- Current number of anonymous subscribers
- Current number of active subscribers (with active traffic sessions)
- Current number of subscribers with mappings
- Current number of IP mappings
- Current number of vlan mappings
- Max number of subscribers that can be introduced
- Max number of subscribers with mappings
- Max number of subscribers with mappings date / time
- Total aggregated number introduced
- Total number of aged subscribers
- Total number of pull events

Number of traffic sessions currently assigned to the default subscriber

show interface LineCard *slot-number* subscriber db counters**Syntax Description**

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows how to display the subscriber database counters:

```
SCE#show interface LineCard 0 subscriber db counters
Current values:
=====
Subscribers: 555 used out of 99999 max.
Introduced subscribers: 555.
Anonymous subscribers: 0.
Subscribers with mappings: 555 used out of 79999 max.
IP mappings: 555 used.
VLAN Entries: 0 used.
Subscribers with open sessions: 0.
Subscribers with TIR mappings: 0.
Sessions mapped to the default subscriber: 0.

Peak values:
=====
Peak number of subscribers with mappings: 555
Peak number occurred at: 17:55:20 UTC THU December 15 2005
Peak number cleared at: 13:28:49 UTC THU December 15 2005

Event counters:
=====
Subscriber introduced: 555.
Subscriber pulled: 0.
Subscriber aged: 0.
Pull-request notifications sent: 0.
State notifications sent: 0.
Logout notifications sent: 0.
Subscriber mapping TIR contradictions: 0.

SCE#
```

Related Commands

show interface LineCard subscriber mapping

Displays subscribers whose mapping meets one of the following specified criteria:

- Is within a specified range of IP addresses
- Intersects a specified IP range
- Matches a specified VLAN tag
- Has no mapping

show interface LineCard *slot-number* **subscriber mapping** [**IP** *iprange*] [**included-in** *iprange*] [**IP** *ipaddress/range*] [**MPLS-VPN PE-ID** *id*] [**VLANid** *vlanid*] [**none**]

Syntax Description	
<i>slot-number</i>	The number of the identified slot. Enter a value of 0.
<i>iprange</i>	Specified range of IP addresses.
<i>vlanid</i>	Specified VLAN tag.

Defaults This command has no default settings.

Command Modes Privileged EXEC

Usage Guidelines

Authorization: admin

Examples The following is an example that lists the number of subscribers with no mapping.

```
SCE#show interface linecard 0 subscriber mapping amount none
Subscribers with no mappings:
N/A
Total 1 subscribers listed.
SCE#
```

Related Commands

show interface LineCard subscriber name

Displays information about a specified subscriber. The following information can be displayed:

- Mappings
- OS counters (bandwidth and current number of flows)
- All values of subscriber properties
- VAS servers used per VAS Server Group
- All of the above

If no category is specified, a complete listing of property values, mappings and counters is displayed.

show interface LineCard *slot-number* **subscriber name** *name* [**mappings**] [**counters**] [**properties**] [**VAS-servers**]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

name The subscriber name.

mappings Display subscriber mappings.

counters Display OS counters.

properties Display values of all subscriber properties

vas-servers Display the VAS servers used by the specified subscriber (SCE 2000 platform only)

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following is an example of how to list the OS counters for the specified subscriber.

```
SCE#show interface linecard 0 subscriber name gold123 counters
SCE#
```

Related Commands

show interface LineCard subscriber properties

Displays all existing subscriber templates.

show interface LineCard *slot-number* **subscriber properties**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following is an example of how to display the subscriber templates.

```
SCE#show interface linecard 0 subscriber templates
SCE#
```

Related Commands

show interface LineCard subscriber TP-mappings statistics

Displays the traffic processor mappings state.

show interface LineCard *slot-number* **subscriber TP-mappings statistics**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following is an example of how to display the traffic processor mappings .

```
SCE#show interface linecard 0 subscriber TP-mappings statistics  
SCE#
```

Related Commands

[subscriber TP-mappings](#) (on page 2-263)

show interface LineCard subscriber TP-IP-range

Displays the configuration of a specified TIR.

show interface LineCard *slot-number* **subscriber TP-IP-range** *TP-IP-range-name* [**all**]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

TP-IP-range-name Name of the TIR to be displayed.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **all** keyword to display all existing TIR configurations.

Authorization: admin

Examples

Following is an example of how to display all existing TIR configurations .

```
SCE#show interface linecard 0 subscriber TP-IP-range all  
SCE#
```

Related Commands

[subscriber TP-IP-range](#) (on page 2-264)

show interface LineCard subscriber mapping included-in TP-IP-range

Displays the existing subscriber mappings for a specified TIR or IP range.

show interface LineCard *slot-number* **subscriber** [**amount**] **mapping included-in TP-IP-range** [*TP-IP-range-name* | *IP*]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

TP-IP-range-name Name of the TIR for which mappings should be displayed.

IP IP range for which mappings should be displayed.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **amount** keyword to display the number of existing mappings only, rather than the mappings themselves.

Authorization: admin

Examples

The following examples illustrate the **show interface LineCard subscriber mapping included-in TP-IP-range** command:

EXAMPLE 1:

Following is an example of how to display all existing mappings for TIR CMTS1.

```
SCE#show interface linecard 0 subscriber mapping included-in TP-IP-range CMTS1
SCE#
```

EXAMPLE 2:

Following is an example of how to display the number of existing mappings for TIR CMTS1.

```
SCE#show interface linecard 0 subscriber amount mapping included-in TP-IP-range CMTS1
SCE#
```

Related Commands

[subscriber TP-IP-range](#) (on page 2-264)

show interface LineCard tos-marking mode

Displays the current LineCard TOS marking status.

show interface LineCard *slot-number* **tos-marking mode**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows that the tos marking mode is enabled:
SCE#show interface LineCard 0 tos-marking mode
 ToS marking mode on slot 0 is enabled
SCE#

Related Commands

[tos-marking mode](#) (on page 2-270)

show interface LineCard tos-marking table

Displays the current LineCard TOS marking table.

show interface LineCard *slot-number* **tos-marking table**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the ToS marking table:

```
SCE#show interface LineCard 0 tos-marking table
          BE   AF1  AF2  AF3  AF4  FE
green     0x0  0xa  0x12 0x1a 0x22 0x2e
yellow    0x0  0xc  0x14 0x1c 0x24 0x2e
red       0x0  0xe  0x16 0x1e 0x24 0x2e
SCE#
```

Related Commands

[tos-marking set-table-entry](#) (on page 2-272)

show interface LineCard traffic-counter

Displays the specified traffic counter.

show interface linecard *slot-number* **traffic-counter** *name* [**all**]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

name Name of the traffic counter to be displayed.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **all** keyword to display all traffic counters.

Authorization: admin

Examples

The following example displays information for all existing traffic counters.

```
SCE#show interface linecard 0 traffic-counter all
Counter 'cnt' value: 0 packets. Rules using it: None.
Counter 'cnt2' value: 1284 packets. Rules using it: Rule2.
2 counters listed out of 32 available.
```

Related Commands

[traffic-counter](#) (on page 2-274)

show interface LineCard traffic-rule

Displays the specified traffic rule configuration.

show interface linecard *slot-number* **traffic-rule name** *name*|**tunnel-id-mode**|**all**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

name Name of the traffic rule to be displayed.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **all** keyword to display all traffic counter rules.

Use the **tunnel-id-mode** to display all rules defined in tunnel-id-mode.

Authorization: admin

Examples

The following example displays information for the Rule1 traffic rule.

```
SCE#show interface linecard 0 traffic-rule name Rule1
```

Related Commands

[traffic-rule](#) (on page 2-275)

show interface linecard VAS-traffic-forwarding

Displays the following information for VAS configuration and operational status summary.

- Global VAS status summary — VAS mode, the traffic link used
- VAS Server Groups information summary — operational status, number of configured servers, number of current active servers.

This information may be displayed for a specific server group or all server groups

- VAS servers information summary — operational status, Health Check operational status, number of subscribers mapped to this server.

This information may be displayed for a specific server or all servers

- VAS health check counters

show interface linecard *slot-number* VAS-traffic-forwarding

show interface linecard *slot-number* VAS-traffic-forwarding health-check

show interface linecard *slot-number* VAS-traffic-forwarding VAS server-group *number*

show interface linecard *slot-number* VAS-traffic-forwarding VAS server-group all

show interface linecard *slot-number* VAS-traffic-forwarding VAS server-id *number*

show interface linecard *slot-number* VAS-traffic-forwarding VAS server-id all

show interface linecard *slot-number* VAS-traffic-forwarding VAS server-id *number* counters health-check

show interface linecard *slot-number* VAS-traffic-forwarding VAS server-id all counters health-check

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

number ID number of either the specified VAS server or VAS server group for which to display information

Defaults

This command has no default settings.

Command Modes

Viewer

Usage Guidelines

Use the basic command with no parameters to display global VAS traffic forwarding information.

Use the **VAS server-group** parameter to display information relating to VAS server groups.

Use the **VAS server-id** parameter to display information relating to individual VAS servers.

Use the **counters health-check** parameter with the **VAS server-id** parameter to display information relating to VAS health check.

Use the **all** keyword with the **VAS server-group** parameter or the **VAS server-id** parameter to display information for all servers or server groups.

Authorization: viewer

Examples

The following examples illustrate how to display VAS traffic forwarding information and provide sample outputs.

EXAMPLE 1

This example shows how to display global VAS status and configuration.

show interface linecard 0 VAS-traffic-forwarding

Sample output:

```
VAS traffic forwarding is enabled
VAS traffic link configured: Link-1    actual: Link-1
```

EXAMPLE 2

This example shows how to display operational and configuration information for a specific VAS Server Group.

show interface linecard 0 VAS-traffic-forwarding VAS server-group 0

Sample output:

```
VAS server group 0:
State: Failure  configured servers: 0    active servers: 0
minimum active servers required for Active state: 1    failure
action: Pass
```

EXAMPLE 3

This example shows how to display operational and configuration information for a specific VAS server.

show interface linecard 0 VAS-traffic-forwarding VAS server-id 0

Sample output:

```
AS server 0:
configured mode: enable  actual mode: enable  VLAN: 520  server group: 3
State: UP
Health Check configured mode: enable  status: running
Health Check source port: 63140  destination port: 63141
Number of subscribers: 0
```

EXAMPLE 4

This example shows how to display health check counters for a specific server. (To clear these counters, see [clear interface linecard VAS-traffic-forwarding VAS counters health-check](#) (on page 2-34).)

show interface linecard 0 VAS-traffic-forwarding VAS server-id 0 counters health-check

Sample output

```

Health Checks statistics for VAS server '0'      Upstream      Downstream
-----
Flow Index '0'
-----
Total packets sent                :      31028   :      31027   :
Total packets received            :      31028   :      31027   :
Good packets received             :      31028   :      31027   :
Error packets received            :           0   :           0   :
Not handled packets               :           0   :           0   :
Average roundtrip (in millisecond):           0   :           0   :
Error packets details             :             :             :
-----
Reordered packets                 :           0   :           0   :
Bad Length packets                :           0   :           0   :
IP Checksum error packets         :           0   :           0   :
L4 Checksum error packets         :           0   :           0   :
L7 Checksum error packets         :           0   :           0   :
Bad VLAN tag packets              :           0   :           0   :
Bad Device ID packets             :           0   :           0   :
Bad Server ID packets             :           0   :           0   :

```

Related Commands

show interface LineCard subscriber name (on page 2-179) (To display VAS server used by specified subscriber)

show interface LineCard counters (on page 2-167) (To display VAS bandwidth and VAS dropped bytes)

clear interface linecard VAS-traffic-forwarding VAS counters health-check (on page 2-34)

show interface LineCard [VLAN|L2TP|IP-tunnel]

Displays the tunnel configuration.

show interface LineCard *slot-number* [VLAN|L2TP|IP-tunnel]

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the IP tunnel configuration.

```
SCE#show interface LineCard 0 ip-tunnel  
tunnel mode: tunneling disable  
SCE#
```

Related Commands

MPLS
[L2TP identify-by](#) (on page 2-96)
[ip tunnel](#) ("ip-tunnel L2TP skip" on page 2-95)
[VLAN](#) (on page 2-294)

show interface LineCard vlan translation

Shows vlan translation configuration.

show interface LineCard *slot-number* **vlan translation**

Syntax Description

slot-number The number of the identified slot. Enter a value of 0.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the vlan translation configuration.

```
SCE#show interface LineCard 0 vlan translation
vlan translation constant: increment 16
SCE#
```

Related Commands

[vlan translation](#) (on page 2-295)

show ip access-class

Shows the access list defined for global IP access to the SCE Platform system. Only IP addresses permitted access according to this access list are allowed access to the system.

show ip access-class

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the IP access class mapping.

```
SCE#show ip access-class  
IP layer is using access-list # 1.  
SCE#
```

Related Commands

[ip access-class](#) (on page 2-77)

show ip advertising

Shows the status of IP advertising, the configured destination and the configured interval.

Use the [destination] and [interval] versions of the command to display only the configured destination or interval, respectively.

show ip advertising [destination|interval]

Syntax Description	<p>destination Displays IP advertising destination.</p> <p>interval Displays the interval between ping commands</p>
Defaults	This command has no default settings.
Command Modes	Privileged EXEC
Usage Guidelines	<p>Use the form show ip advertising destination to display the IP advertising destination.</p> <p>Use the form show ip advertising interval to display the interval between ping commands.</p> <p>Authorization: admin</p>
Examples	<p>The following example shows the IP advertising status and configuration.</p> <pre>SCE#show ip advertising IP advertising is disabled IP advertising destination is 10.10.10.10 IP advertising interval is 853 seconds</pre>
Related Commands	ip advertising (on page 2-79)

show ip filter

Displays the following information for management interface IP filtering.

- IP fragment filter enabled or disabled
- configured attack threshold (permitted and not-permitted IP addresses)
- configured end of attack threshold (permitted and not-permitted IP addresses)
- burst size in seconds (permitted and not-permitted IP addresses)

show ip filter

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Viewer

Usage Guidelines

Authorization: viewer

Examples

The following command shows how to display information for management interface IP filtering

```
SCE# show ip filter
```

Related Commands

show ip default-gateway

Shows configured default gateway.

show ip default-gateway

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example displays the default gateway.

```
SCE#show ip default-gateway  
Default gateway: 10.1.1.1  
SCE#
```

Related Commands

[ip domain-lookup](#) (on page 2-81)

show ip route

Shows the entire routing table and the destination of last resort (default-gateway). When using the *prefix* and *mask* parameters, it shows the routing entries from the subnet specified by the prefix and mask pair.

show ip route [*prefix mask*]

Syntax Description

prefix The prefix of the routing entries to be included.

mask Used to limit the search of routing entries.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of the **show ip route** command:

EXAMPLE 1:

The following example shows the default gateway.

```
SCE#show ip route
gateway of last resort is      10.1.1.1
SCE#
```

EXAMPLE 2:

The following example shows retrieval of the ip route.

```
SCE#show ip route 10.1.60.0 255.255.255.0
| prefix | mask | next hop |
|-----|-----|-----|
| 10.1.60.0 | 255.255.255.0 | 10.1.1.5 |
SCE#
```

Related Commands

[ip route](#) (on page 2-89)

show ip rpc-adapter

Displays the status of the RPC adapter (enabled or disabled) and the configured port.

show ip rpc-adapter [sessions]

Syntax Description

sessions Display information regarding RPC adapter sessions.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the configuration of the RPC adapter.

```
SCE#show ip rpc-adapter
RPC Server is OFFLINE
RPC Server port is 14374
```

Related Commands

[ip rpc-adapter](#) (on page 2-90)

show ip ssh

Shows the status of the SSH sever, including current SSH sessions.

show ip ssh

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows how to retrieve the current SSH status.

```
SCE#show ip ssh
```

Related Commands

[ip ssh](#) (on page 2-92)

show line vty

Displays the Telnet configuration.

show line vty timeout|access-class in

Syntax Description

timeout Shows the timeout configured to the Telnet sessions.

access-class in Shows the access list configured to the Telnet server that contains the list of addresses that have access to the system.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the access list configured for telnet lines.

```
SCE#show line vty access-class in  
Telnet server is using access-list # 1.  
SCE#
```

Related Commands

[line vty](#) (on page 2-97)

show logger device User-File-Log

Displays the SCE Platform logger configuration status and maximum file size.

show logger device User-File-Log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the SCE Platform logger User-File-Log status and configuration.

```
SCE#show logger device User-File-Log  
SCE User-File-Log status: Enabled  
SCE User-File-Log file size: 64000  
SCE#
```

Related Commands

[logger device User-File-Log](#) (on page 2-102)

show logger device User-File-Log counters

Displays the SCE Platform logger counters.

show logger device User-File-Log counters

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current SCE Platform User-File-Log counters.

```
SCE#show logger device user-file-log counters
Logger SCE User-File-Log counters:
Total info messages: 73
Total warning messages: 44
Total error messages: 0
Total fatal messages: 0
SCE#
```

Related Commands

logger device User-File-Log

(on page [2-102](#))

show logger device User-File-Log max-file-size

Displays the SCE Platform logger maximum file size.

show logger device User-File-Log max-file-size

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Privileged EXEC

Command Modes

Usage Guidelines

Authorization: admin

Examples

The following example shows the SCE Platform logger User-File-Log max file size configuration.

```
SCE#show logger device User-File-Log max-file-size
```

```
SCE User-File-Log file size: 64000
```

```
SCE#
```

Related Commands

[logger device User-File-Log max-file-size](#) (on page 2-103)

show logger device User-File-Log status

Displays the SCE Platform logger configuration status.

show logger device User-File-Log status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the SCE Platform logger User-File-Log status.

```
SCE#show logger device User-File-Log status  
SCE User-File-Log status: Enabled  
SCE#
```

Related Commands

logger device User-File-Log (on page 2-102)

show logger device User-File-Log nv-counters

Shows the non-volatile counters for the user log file.

show logger device User-File-Log nv-counters

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the user log file non-volatile counters.

```
SCE#show logger device user-file-log nv-counters  
SCE#
```

Related Commands

[show logger device User-File-Log counters](#) (on page 2-202)

show management-agent sce-api

Displays statistics for theSCE subscriber API clients.

show management-agent sce-api

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Viewer

Authorization: viewer

Usage Guidelines

Examples

The following example enables an SNTP server at a specified IP address.

```
SCE(config)#show management-agent sce-api  
SCE(config)#
```

Related Commands

show pqi file

Displays information, such as installation options, about the specified application file.

show pqi file *filename* info

Syntax Description

filename The filename of the desired application file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows how to display application file information.

```
SCE#show pqi file myfile.txt info  
application:    sm  
description:    SCE 1000 sm  
target SCE:    SCE 1000  
module names:  sm20001.pm0
```

Related Commands

[pqi install file](#) (on page 2-120)

show pqi last-installed

Displays the name of the last pqi file that was installed.

show pqi last-installed

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows how to display application file information.

```
SCE#show pqi last-installed
```

```
package name:   pack1
```

```
package date:   Tue Jun 10 17:27:55 GMT+00:00 2003
```

```
operation:      Upgrade
```

Related Commands

[pqi install file](#) (on page 2-120)

show RDR-formatter

Displays the RDR formatter configuration.

show RDR-formatter

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the configuration of the RDR formatter.

```
SCE#show RDR-formatter
```

```
Status: enabled
```

```
Connection is: down
```

```
Forwarding mode: redundancy
```

```
Connection table:
```

Collector IP Address / Host-Name	Port	Status	Priority per Category:	
			Category1	Category2
10.1.1.205	33000	Down	100	100
10.1.1.206	33000	Down	60	60
10.12.12.12	33000	Down	40	40

```
RDR: read: 0 ,sent: 0, thrown: 0
```

```
UM: read: 0 ,sent: 0, thrown: 0
```

```
Logger: read: 0 ,sent: 0, thrown: 0
```

```
Errors: thrown: 0
```

```
Last time these counters were cleared: 14:05:57 UTC SUN February 23 2003
```

```
SCE#
```

Related Commands

[RDR-formatter destination](#) (on page 2-127)

show RDR-formatter connection-status

Shows the current RDR formatter connection table and status (main connection status: up/down, forwarding mode, and connection/activity information for each destination).

show RDR-formatter connection-status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the RDR-formatter connection status.

```
SCE#show RDR-formatter connection-status
```

```
Connection is: up
```

```
Forwarding mode: redundancy
```

```
Connection table:
```

```
-----
```

Collector IP Address / Host-Name	Port	Status	Priority per Category:	
			Category1	Category2
10.1.1.205	33000	Up	100 primary	100 primary
10.1.1.206	33000	Down	60	60
10.12.12.12	33000	Up	40	40

```
-----
```

```
SCE#
```

Related Commands

show RDR-formatter counters

Shows the RDR-formatter counters.

show RDR-formatter counters

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the RDR-formatter counters.

SCE#show RDR-formatter counters

RDR: read: 0 ,sent: 0, thrown: 0

UM: read: 0 ,sent: 0, thrown: 0

Logger: read: 0 ,sent: 0, thrown: 0

Errors: thrown: 0

Last time these counters were cleared: 14:05:57 UTC SUN February
23 2003

SCE#

Related Commands

show RDR-formatter destination

Shows the RDR-formatter destinations.

show RDR-formatter destination

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the RDR-formatter configured destinations.

```
SCE#show RDR-formatter destination
```

```
Destination: 10.1.1.205
```

```
Port: 33000
```

```
Destination: 10.1.1.206
```

```
Port: 33000
```

```
Destination: 10.10.12.10
```

```
Port: 33000
```

```
SCE#
```

Related Commands

[RDR-formatter destination](#) (on page 2-127)

show RDR-formatter enabled

Shows the RDR-formatter status (enabled/disabled).

show RDR-formatter enabled

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows that the RDR formatter is enabled.

```
SCE#show RDR-formatter enabled
```

```
Status:  enabled
```

```
SCE#
```

Related Commands

show RDR-formatter forwarding-mode

Shows the configured RDR-formatter forwarding-mode (redundancy/multicast).

show RDR-formatter forwarding-mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the RDR formatter forwarding-mode.

```
SCE#show RDR-formatter forwarding-mode
```

```
Forwarding mode:  redundancy
```

```
SCE#
```

Related Commands

[RDR-formatter forwarding-mode](#) (on page 2-129)

show RDR-formatter statistics

Shows the current RDR formatter statistics.

show RDR-formatter statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current RDR statistics.

SCE#show RDR-formatter statistics

```
Total:
  sent:      0
  in-queue:  0
  thrown:    0
  rate:      0 RDRs per second
  max rate:  0 RDRs per second
Destination: 10.1.1.205 Port: 33000 Status: down Active: no
  Sent:      0
  Rate: 0    Max: 0
Last connection establishment: 14:05:57 UTC SUN February 23
2003
Destination: 10.1.1.206 Port: 33000 Status: down Active: no
  Sent:      0
  Rate: 0    Max: 0
Last connection establishment: 14:05:57 UTC SUN February 23
2003
Destination: 10.10.12.10 Port: 33000 Status: down Active: no
  Sent:      0
  Rate: 0    Max: 0
Last connection establishment: 14:05:57 UTC SUN February 23
2003
SCE#
```

Related Commands

show running-config

Shows the current configuration.

show running-config [all-data]
more running-config [all-data]

Syntax Description

all data Displays defaults as well as non-default settings.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The **all data** switch may to see sample usage for many CLI configuration commands.

Authorization: admin

Examples

The following example shows the partial output of the **more running-config** command.

```
SCE#>more running-config all-data
#This is a general configuration file (running-config).
#Created on 16:48:11 UTC WED June 13 2001

cli-type 1
#version 1

service logger

no service password-encryption
enable password level 10 0 "pcube"
enable password level 15 0 "pcube"
service RDR-formatter
no RDR-formatter destination all
RDR-formatter history-size 0
clock timezone UTC 0
ip domain-lookup
no ip domain-name
no ip name-server
service telnetd

FastEthernet 0/0
ip address 10.1.5.120 255.255.0.0
speed auto
duplex auto

exit
ip default-gateway 10.1.1.1
no ip route all

line vty 0 4
no access-class in
timeout 30
exit
SCE#>
```

Related Commands

show snmp

Displays the SNMP configuration and counters.

show snmp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the SNMP server configuration and status.

SCE#show snmp

SNMP server status: Enabled

Location: London_Office

Contact: Brenda

Authentication Trap Status: Enabled

Communities:

Community: public, Access Authorization: RO, Access List

Index: 1

Trap managers:

Trap host: 10.1.1.205, community: public, version: SNMPv2c

SNMP stats:

29 SNMP packets input

0 Bad SNMP version errors

29 Unknown community name

0 Illegal operation for community name supplied

0 Encoding errors

0 Number of requested variables

0 Number of altered variables

0 Get-request PDUs

0 Get-next PDUs

0 Set-request PDUs

29 SNMP packets output

0 Too big errors

0 No such name errors

0 Bad values errors

0 General errors

0 Response PDUs

29 Trap PDUs

SCE#

Related Commands

show snmp community

Displays configured communities.

show snmp community

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the SNMP manager communities.

```
SCE#show snmp community
```

```
Community: public, Access Authorization: RO, Access List Index:  
1
```

```
SCE#
```

Related Commands

[snmp-server community](#) (on page 2-244)

show snmp contact

Displays the configured MIB-2 variable sysContact.

show snmp contact

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the system contact.

```
SCE#show snmp contact
```

```
Contact: Brenda@mycompany.com
```

```
SCE#
```

Related Commands

[snmp-server contact](#) (on page [2-245](#))

show snmp enabled

Displays the SNMP agent status (enabled/disabled).

show snmp enabled

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the SNMP server enabled status.

```
SCE#show snmp enabled  
SNMP server status: Enabled  
SCE#
```

Related Commands

[snmp-server](#) (on page 2-243)

show snmp host

Displays the destination hosts for SNMP traps.

show snmp host

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the destination hosts for SNMP traps.

```
SCE#show snmp host
```

```
Trap host: 10.1.1.205, community: public, version: SNMPv2c
```

```
SCE#
```

Related Commands

[snmp-server host](#) (on page 2-248)

show snmp location

Displays the configured MIB-2 variable sysLocation.

show snmp location

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the system location.

```
SCE#show snmp location  
Location: London_Office  
SCE#
```

Related Commands

[snmp-server location](#) (on page 2-249)

show snmp MIB

Displays MIB variables.

show snmp MIB *mib variables variables*

Syntax Description

<i>mib</i>	Name of MIB to display. MIB-II pcube-SE-MIB
<i>variables</i>	Name of group to display. MIB-II: Use one of the following values: AT, ICMP, interfaces, IP, SNMP, system, TCP or UDP. pcube-SE-MIB: Use one of the following values: <i>application, chassis, disk, global-controller, link, logger, module, port, rdr-formatter, subscriber, system, traffic-counters, tx-queue, vas-traffic-forwarding</i>

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the MIB-2 system group.

```
SCE#show snmp MIB MIB-II system
sysDescr.0 = CiSCO Service Engineering, SW version: Control Card
Version 1.30 build 29, HW version: SCE GE "RevE"
sysObjectID.0 = 1.3.6.1.4.1.5655.1.2
sysUpTime.0 = 14 hours, 25 minutes, 59 seconds
sysContact.0 = Brenda@mycompany.com
sysName.0 = SCE
sysLocation.0 = London_Office
sysServices.0 = 2
SCE#
```

Related Commands

show snmp traps

Displays the SNMP traps generation status (enabled/disabled)

show snmp traps

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the SNMP server traps status.

```

SCE#sh snmp traps
Authentication-failure trap status: Disabled
operational-status traps status:    Enabled
system-reset trap status:           Enabled
chassis traps status:               Enabled
RDR-formatter traps status:         Enabled
Telnet traps status:                Enabled
logger traps status:                Enabled
SNTP traps status:                  Enabled
link-bypass traps status:            Enabled
subscriber traps status:             Enabled
pull-request-failure traps status:   Disabled
attack traps status:                 Enabled
vas-traffic-forwarding traps status: Enabled
port-operational-status traps status: Enable
SCE#

```

Related Commands

[snmp-server enable traps](#) (on page 2-246)

show sntp

Displays the SNTP configuration and update statistics.

show sntp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows statistics from the SNTP clients.

```
SCE#show sntp
SNTP broadcast client: disabled
last update time: not available
```

```
SNTP uni-cast client: enabled
there is one server:
1: 128.182.58.100
last update time: Feb 10 2002, 14:06:41
update interval: 100 seconds
```

```
SCE#
```

Related Commands

[sntp server](#) (on page 2-250)

show startup-config

Shows the startup configuration file. Use this command to review the configuration used by the SCE platform at boot time in comparison with the current configuration to make sure that you approve of all the differences before saving the configuration by using **copy running-config startup-config** command.

show startup-config
more startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows a sample output.

```
SCE#more startup-config
#Created on 20:17:46 UTC THU January 1 2001
#cli-type 1
#version 1
logger SCE User-File-Log max-file-size 20000
ip domain-name *pcube*
ip name-server 10.1.1.1
interface FastEthernet 0/0
ip address 10.1.4.202 255.0.0.0
interface LineCard 0
silent
SCE#
```

Related Commands

[copy running-config startup-config](#) (on page 2-52)

show system operation-status

Displays the operation status of the system.

show system operation-status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the system operation status:

```
SCE#show system operation-status
```

```
System Operation status is Operational
```

```
SCE#
```

Related Commands

show system-uptime

Displays the length of time the system has been running since the last reboot..

show system-uptime

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the system uptime for the SCE Platform.

```
SCE#show system-uptime
```

```
SCE uptime is 21 minutes, 37 seconds
```

```
SCE#
```

Related Commands

show tacacs

Displays statistics for the TACACS+ servers.

show tacacs

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Viewer

The **'all'** option is available only at the Privileged Exec level.

Use the **all** keyword to display keys and timeouts as well as other statistics.

Usage Guidelines

Note that, although most show commands are accessible to viewer level users, the **'all'** option is available only at the admin level. Use the command **'enable 10'** to access the admin level.

Authorization: viewer

The **'all'** option is at the admin authorization level.

Example 1

This example shows how to display statistics for all TACACS+ servers.

```
SCE> show tacacs
Server: 100.10.10.10./49: opens=0 closes=0 error=0
      messages in=0 messages out=0
SCE>
```

Example 2

This example shows how to display statistics, including keys and timeouts, for all TACACS+ servers.

```
SCE# show tacacs all
Server: 100.10.10.10./49: opens=0 closes=0 error=0
      messages in=0 messages out=0
      timeout=20
      uses default timeout= yes
      key= a
      uses default key= no
SCE>
```

Related Commands

show telnet sessions

Displays any active Telnet sessions.

show telnet sessions

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows that there is one active Telnet session.

```
SCE#show telnet sessions
```

```
There is 1 active telnet session:
```

```
Index | Source
=====
  0   | 10.1.1.201
SCE#
```

Related Commands

[telnet](#) (on page [2-268](#))

show telnet status

Displays the status of the telnet server daemon.

show telnet status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows that the telnet daemon is currently enabled.

```
SCE#show telnet status  
Telnet daemon is enabled.  
SCE#
```

Related Commands

show timezone

Displays the current time zone and daylight saving time configuration as configured by the user.

show timezone

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the time zone configured by the user.

```
SCE#show timezone
```

```
Time zone: ISR    minutes offset from UTC: 120
```

```
SCE#
```

Related Commands

[clock timezone](#) (on page 2-44)

show users

Displays the users in the local database, including passwords.

show users

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privilege Exec

Usage Guidelines

Note that, although most show commands are accessible to viewer level users, this command is available only at the admin level. Use the command '**enable 10**' to access the admin level.

Authorization: admin

Examples

This example shows how to display the users in the local database.

SCE# show users

```
User:  name = Joe
      privilege level = 10
      password = joe's pwd
      is password encrypted = no
```

SCE#

Related Commands

show version

Displays the configuration information for the system including the hardware version, the software version, the application used, and other configuration information.

show version

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current version information of the SCE Platform.

SCE#show version

```
System version: Version 3.0.0 Build 240
Build time: Dec 11 2005, 07:34:47
Software version is: Version 3.0.0 Build 240
Hardware information is:
rx          : 0x0075
dp          : 0x1808
tx          : 0x1708
ff          : 0x0077
cls         : 0x1721
cpld        : 0x0025
Lic         : 0x0176
rev         : G001
Bootrom     : 2.1.0
L2 cache    : Samsung 0.5
lic type    : MFEoptic mode      :
Part number: 53AA-BXC1-AAAA
Revision: A02A
Software revision: G001
Serial number: 043P6982
Power Supply type: AC
```

SML Application information is:

```
Application file: /tffs0/temp.sli
Application name:
Application help:
Original source file:
H:\work\Emb\jrt\V2.5\sml\actions\drop\drop_basic_anyflow.san
Compilation date: Wed, November 22, 2005 at 21:25:21
Compiler version: SANc v3.00 Build 32 gcc_codelets=true built
on: Tue November 21 2005 09:51:57 AM.;SME plugin v1.1
Default capacity option used.
```

Logger status: Enabled

```
Platform: SCE 2000 - 4xFE
Management agent interface version: SCE Agent 3.0.0 Build 18
Software package file:
ftp://vk:vk@10.1.8.22/P:/EMB/LatestVersion/3.0.0/se1000.pkg
```

SCE2000 uptime is 21 minutes, 37 seconds

SCE#

Related Commands

show version all

Displays the complete version information as well as the running configuration for all components.

show version all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows version and configuration information for all the system components.

SCE#show version all

System version: Version 3.0.0 Build 240
Build time: Dec 11 2005, 07:34:47
Software version is: Version 3.0.0 Build 240
Hardware information is:

rx : 0x0075
dp : 0x1808
tx : 0x1708
ff : 0x0077
cls : 0x1721
cpld : 0x0025
Lic : 0x0176
rev : G001
Bootrom : 2.1.0
L2 cache : Samsung 0.5
lic type : MFE
optic mode :
Part number: 53AA-BXC1-AAAA
Revision: A02A
Software revision: G001
Serial number: 043P6982
Power Supply type: AC

SML Application information is:

Application file: /tffs0/temp.sli
Application name:
Application help:
Original source file:
H:\work\Emb\jrt\V2.5\sml\actions\drop\drop_basic_anyflow.san
Compilation date: Wed, September 22, 2004 at 21:25:21
Compiler version: SANc v3.0.0 Build 32 gcc_codelets=true built
on: Tue November 22 2004 09:51:57 AM.;SME plugin v1.1
Default capacity option used.

Logger status: Enabled

Platform: SCE2000 - 4xFE
Management agent interface version: SCE Agent 3.0.0 Build 18
Software package file:
ftp://vk:vk@10.1.8.22/P:/EMB/LatestVersion/3.0.0/se1000.pkg

SCE2000 uptime is 21 minutes, 37 seconds

SCE#

.

```
Current configuration:
=====
#This is a general configuration file (running-config).
#Created on 10:14:59 UTC TUE December 11 2005
.
interface LineCard 0
connection-mode active
no silent
.
.

Software package file: Not available
Unified management package file: /tffs0/images/um13012.pkg
SCE#
```

Related Commands

show version software

Displays version information for the current software.

show version software

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows the current software version.

```
SCE#show version software
```

```
Software version is: Version 3.0.0 Build 240
```

```
SCE#
```

Related Commands

silent

Disables the LineCard from reporting events. Use the [no] form of this command if you want the LineCard to send reports.

silent
no silent

Syntax Description	This command has no arguments or keywords.
--------------------	--

Defaults	No silent
----------	-----------

Command Modes	LineCard Interface Configuration
---------------	----------------------------------

Usage Guidelines	Authorization: admin
------------------	----------------------

Examples	The following example changes the LineCard state to silent. <i>SCE</i> (config if)# silent <i>SCE</i> (config if)#
----------	---

Related Commands	
------------------	--

snmp-server

Enables the SNMP agent. You can use any of the other SNMP-server commands to enable the SNMP agent.

Use the **no** form to disable the SNMP agent from responding to SNMP managers. All SNMP settings are saved and are restored when the SNMP agent is re-enabled.

snmp-server enable
no snmp-server

Syntax Description

This command has no arguments or keywords

Defaults

disabled

Command Modes

Global Configuration

Usage Guidelines

You must define at least one community string in order to allow SNMP access. For complete information on community strings.

Authorization: admin

Examples

The following example disables the SNMP server.

```
SCE(config)#no snmp-server  
SCE(config)#
```

Related Commands

[snmp-server community](#) (on page 2-244)

snmp-server community

Sets a community string. Use the **no** form of the command to remove a community string.

The optional **acl-number** parameter states the access list number to restrict the managers that can use this community.

snmp-server community *community-string* [*read-option*] [*acl-number*]
no snmp-server community *community-string* [*read-option*] [*acl-number*]
no snmp-server community all

Syntax Description	<p><i>community-string</i> The SNMPv1 and SNMPv2c security string that identifies a community of managers that can access the SNMP server.</p> <p><i>read-option</i> Legal values are ro and rw. The default ro (read-only) option allows managers to view MIB variables. rw sets the variable to read-write.</p> <p><i>acl-number</i> Number of the access list that lists the managers who may access the SCE Platform via SNMP.</p>
Defaults	no SNMP access
Command Modes	Global Configuration
Usage Guidelines	<p>Use the all keyword with the no form of the command to remove all configured communities.</p> <p>Authorization: admin</p>
Examples	<p>The following example configures an SNMP managers community that has read-only permissions for the SCE Platform MIB. Only SNMP managers in access list 1 can access the SCE Platform.</p> <pre>SCE(config)#snmp-server community public ro 1 SCE(config)#</pre>
Related Commands	

snmp-server contact

Sets the MIB-2 variable system contact. Use the **no** form of this command to remove the contact setting.

snmp-server contact *contact*

no snmp-server contact

Syntax Description

contact A string that identifies the system contact.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example configures the system contact.

```
SCE(config)#snmp-server contact Brenda@MyCompany.com  
SCE(config)#
```

Related Commands

snmp-server enable traps

Enables/disables SNMP traps (only authentication-failure traps and enterprise traps can be controlled using this command). Use the **[default]** form of this command to reset SNMP traps to the default status.

```
snmp-server enable traps [snmp [snmp trap name]] [enterprise
enterprise trap name]
```

```
no snmp-server enable traps [snmp [snmp trap name]] [enterprise
enterprise trap name]
```

```
default snmp-server enable traps [snmp [snmp trap name]]
enterprise [enterprise trap name]
```

Syntax Description

snmp trap name Optional parameter used with the **snmp** parameter to control a specific snmp trap.

Setting = **Authentication**

enterprise trap name Optional parameter used with the **enterprise** parameter to control a specific enterprise trap.

Settings = **attack, chassis, link-bypass, logger, operational-status, port-operational-status, pull-request-failure, RDR-formatter, session, Sntp, subscriber, system-reset, telnet, vas-traffic-forwarding**

Defaults

snmp traps: disabled
enterprise traps: enabled

Command Modes

Global Configuration

Usage Guidelines

There are two classes of SNMP traps that are controlled by this command

- snmp traps
- enterprise traps

The options **snmp** and **enterprise** are parameters specifying the class of traps that are to be enabled/disabled by this command. Each class, or type, is composed of specific traps. Use these parameters as follows:

- To enable/disable all traps of one type: Specify only **snmp** or **enterprise**.
- To enable/disable only one specific trap: Specify **snmp** or **enterprise** with the additional trap name parameter naming the desired trap.
- To enable/disable all traps: Do not specify either **snmp** or **enterprise**.

Since, at this time, the only snmp type trap is the authentication trap, the **snmp** and **authentication** parameters are currently redundant.

Authorization: admin

Examples

The following example configures the SNMP server to send traps.

```
SCE(config)#snmp-server enable traps  
SCE(config)#
```

snmp-server host

Sets destination hosts for SNMP traps.

snmp-server host *address* [**traps**] [**version** *version*] *community-string*
no snmp-server host *address* [**traps**] [**version** *version*] *community-string*
no snmp-server host all

Syntax Description	<p><i>address</i> The IP address of the SNMP server host.</p> <p>traps Optional switch, does not influence command functionality.</p> <p><i>version</i> Version of the SCE Platform software running in the system. Can be set to 1 or 2c.</p> <p><i>community-string</i> The SNMPv1 and SNMPv2c security string that identifies a community of managers that are able to access the SNMP server.</p>
Defaults	No hosts
Command Modes	Global Configuration
Usage Guidelines	<p>If no communities are specified by the snmp-server community command, the community string specified by this command is used by the SCE Platform, as if an snmp-server community community-string ro was given.</p> <p>Use the all keyword with the no form of the command to remove all configured hosts.</p> <p>Authorization: admin</p>
Examples	<p>The following example adds a host destination for SNMP traps.</p> <pre>SCE(config)#snmp-server host 10.1.1.205 version 2c public SCE(config)#</pre>
Related Commands	no snmp-server host all

snmp-server location

Gives a name to the SCE Platform location, setting the MIB-2 variable sysLocation. Use the **no** form of this command to remove the location setting.

snmp-server location *location*

no snmp-server location

Syntax Description

location A string that specifies the system location.

Defaults

no location

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example configures the system location.

```
SCE(config)#snmp-server location London_Office
```

```
SCE(config)#
```

Related Commands

sntp server

Enables the SNTP uni-cast client to query the specified SNTP server. Use the **no** form of this command to disable the SNTP uni-cast server.

sntp server {*address*/*hostname*}

no sntp server *hostname*

no sntp server all

Syntax Description	<i>address</i> The IP address of the SNTP server. <i>hostname</i> The hostname of the SNTP server.
Defaults	SNTP uni-cast server is disabled
Command Modes	Global Configuration Use the all keyword with the no form of this command to disable all SNTP uni-cast servers.
Usage Guidelines	Authorization: admin
Examples	The following example enables an SNTP server at a specified IP address. SCE(config)#sntp server 128.182.58.100 SCE(config)#
Related Commands	no sntp server all

sntp broadcast client

Enables the SNTP multicast client to accept SNTP broadcasts from any SNTP server. Use the **no** form of this command to disable the SNTP multicast client.

sntp broadcast client
no sntp broadcast client

Syntax Description

This command has no arguments or keywords.

Defaults

disabled

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example enables the SNTP multicast client.

```
SCE(config)#sntp broadcast client  
SCE(config)#
```

Related Commands

sntp update-interval

Defines the interval (in seconds) between SNTP uni-cast update queries.

sntp update-interval interval

Syntax Description	<i>interval</i> The interval between queries in seconds.
--------------------	--

Defaults	900 seconds
----------	-------------

Command Modes	Global Configuration
---------------	----------------------

Usage Guidelines	
------------------	--

Authorization: admin

Examples	<p>The following example sets the SNTP update interval for 100 seconds.</p> <pre>SCE(config)#sntp update-interval 100 SCE(config)#</pre>
----------	---

Related Commands	
------------------	--

speed

Configures the speed of the FastEthernet Interface to either 10 Mbps or 100 Mbps. Auto means auto-negotiation (do not force speed on the link).

speed *speed*

no speed

Syntax Description

speed The speed in Mbps or auto-negotiation. Can be set to **10**, **100** or **auto**.

Defaults

Auto

Command Modes

FastEthernet Interface Configuration

Usage Guidelines

Changing this configuration takes effect only if the **duplex** mode is not configured to **auto**.

Authorization: admin

Examples

The following example configures a FastEthernet port to 100 Mbps speed.

```
SCE(config if)#speed 100
```

```
SCE(config if)#
```

Related Commands

subscriber aging

Enables/disables subscriber aging for the specified type of subscribers (anonymous or introduced).

The aging period may also be defined when aging is enabled.

subscriber aging anonymous|introduced [timeout *aging-time*]
no subscriber aging anonymous|introduced

Syntax Description

aging-time In minutes.
anonymous Anonymous groups subscribers
introduced Introduced subscribers

Defaults

Command Modes

LineCard Interface Configuration

Usage Guidelines

The most common usage for aging is for anonymous subscribers, since this is the easiest way to ensure that anonymous subscribers that have logged-out of the network are removed from the SCE Platform and are no longer occupying resources. Aging time can be configured individually for introduced subscribers and for anonymous subscribers.

Authorization: admin

Examples

The following example enables subscriber aging for anonymous subscribers with a timeout period of 10 minutes.

```
SCE(config if)#subscriber aging anonymous timeout 10  

SCE(config if)#
```

Related Commands

subscriber anonymous-group export csv-file

Exports anonymous groups to the specified csv file.

subscriber anonymous-group export csv-file *filename*

Syntax Description

filename Name of the csv file to which the anonymous groups information is to be exported.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example exports anonymous groups information to the specified file

```
SCE(config if)# subscriber anonymous-group export csv-file  
s_g_0507.csv  
SCE(config if)#
```

Related Commands

subscriber anonymous-group import csv-file

Creates anonymous groups by importing anonymous subscribers from the specified csv file.

subscriber anonymous-group import csv-file *filename*

Syntax Description

filename Name of the *csv* file containing the anonymous groups information.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Anonymous Group *csv* files have a fixed format. All lines have the same structure, as described below:

Anonymous-group-name, IP-range [, subscriber-template-number].

If no subscriber-template-number is specified, then the anonymous subscribers of that group will use the default template (#0), which cannot be changed by template import operations.

Following is an example of an anonymous group *csv* file:

```
group1, 10.1.0.0/16, 2
group2, 176.23.34.0/24, 3
group3, 10.2.0.0/16
```

Authorization: admin

Examples

The following example imports subscriber from the file *subscribers_groups.csv*.

```
SCE(config if)# subscriber anonymous-group import csv-file
subscribers_groups.csv
SCE(config if)#
```

Related Commands

subscriber export csv-file

Exports subscribers to the specified csv file. Subscriber csv files are application-specific. Refer to the relevant application documentation for the definition of the file format.

subscriber export csv-file *filename*

Syntax Description

filename Name of the *csv* file to which the subscriber information is to be exported.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Subscriber *csv* files are application-specific. Refer to the relevant application documentation for the definition of the file format.

Authorization: admin

Examples

The following example exports subscribers to the specified file.

```
SCE(config if)# subscriber export csv-file  
gold_subscribers_04072003.csv  
SCE(config if)#
```

Related Commands

subscriber import csv-file

Imports subscribers from the specified csv file.

subscriber import csv-file *filename*

Syntax Description

filename Name of the *csv* file containing the subscriber information.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Subscriber *csv* files are application-specific. Refer to the relevant application documentation for the definition of the file format.

Authorization: admin

Examples

The following example imports subscriber from the file *gold_subscribers.csv*.

```
SCE(config if)# subscriber import csv-file gold_subscribers.csv  
SCE(config if)#
```

Related Commands

subscriber sm-connection-failure

Configures the behavior of the system in case of communication failure between the SM and the SCE platform.

subscriber sm-connection-failure action [force-failure|none|remove-mappings|shut]

subscriber sm-connection-failure action timeout *timeout*

default subscriber sm-connection-failure

Syntax Description

<i>timeout</i>	The timeout interval in seconds.
<i>force-failure</i>	Force failure of the SCE platform in the event of any loss of connection with the SM The SCE platform then acts according to the behavior configured for the failure state.
<i>none</i>	No action needs to be taken in the event of any loss of connection between the SCE platform and the SM
<i>remove-mappings</i>	Remove all current subscriber mappings in the event of any loss of connection between the SCE platform and the SM
<i>shut</i>	The SCE platform shuts down and quits providing service.

Defaults

Default action = none

Command Modes

LineCard Interface Configuration

Usage Guidelines

If SM functionality is not critical to the operation of the system: no action needs to be configured.

If SM functionality is critical to the operation of the system: configure forced failure of the SCE Platform in the event of any loss of connection with the SM.

Use the **timeout** parameter to configure the time interval after which a failure condition is detected and the specified action will be taken by the system.

Authorization: admin

Examples

The following example configures forced failure of the SCE Platform in case of failure of the SM.

```
SCE (config if)#subscriber sm-connection-failure action force-failure
SCE (config if)#
```

Related Commands

subscriber template export csv-file

Exports a subscriber template to the specified csv file, according to the party template.

subscriber template export csv-file *filename*

Syntax Description

filename Name of the *csv* file to which the subscriber template is to be exported.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example exports the subscriber template to the specified file.

```
SCE(config if)# subscriber template export csv-file gold0507.csv
SCE(config if)#
```

Related Commands

subscriber template import csv-file

Imports a subscriber template from the specified csv file, creating a party template.

subscriber template import csv-file *filename*

Syntax Description

filename Name of the *csv* file containing the subscriber template.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example imports the subscriber template from the file *gold0507.csv*.

```
SCE(config if)# subscriber template import csv-file gold0507.csv  
SCE(config if)#
```

Related Commands

subscriber TP-IP-range name IP-range target-TP

Use this command to create or update a TIR. Use the **no** form of this command to delete a specified TIR.

subscriber TP-IP-range name *TP-IP-range-name* **IP-range target-TP** *IP-range target-TP* [**remove-subscriber-mapping**]

no subscriber TP-IP-range [**name** *name* | **all**] [**remove-subscriber-mapping**]

Syntax Description

TP-IP-range name Meaningful name assigned to this traffic processor IP range

IP-range IP address and mask length defining the IP range

target-TP number of the traffic processor to which this TIR is to be assigned

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Use the **remove-subscriber-mappings** keyword when editing or deleting a TIR to remove any existing subscriber mappings. If mappings exist, and this keyword is not used, the command will not execute.

- When deleting a TIR, only the range name is required.
- To delete all existing TIRs, use the [no] form of the command with the **all** keyword instead of the range name.

Authorization: admin

Examples

The following example creates a TIR named CMTS1 and assigns it to traffic processor# 5. The **remove-subscriber-mappings** keyword is used to remove any existing subscriber mappings.

```
SCE(config if)#subscriber TP-IP-range name CMTS1 IP-range
10.10.10.0/128 target-TP 5 remove-subscriber-mappings
```

Related Commands

subscriber TP-mappings

Reserves a specified number of subscriber rules for TIRs.

subscriber TP-mappings max-TP-IP-ranges *max-TP-IP-ranges*

default subscriber TP-mappings

Syntax Description

max-TP-IP-ranges Number of rules to allocate for TIRs

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

The maximum number of allowed reserved rules is 4096.

- By default 0 (zero) rules are reserved for TIRs.
- Updating this configuration is a major system event and can only be performed when no subscriber mappings or TIRs are configured.

Use the **default** version of this command to restore default subscriber rule allocation.

Authorization: admin

Examples

The following example reserves 500 subscriber rules for TIRs.

```
SCE(config if)#subscriber TP-mappings max-TP-IP-ranges 500
```

Related Commands

subscriber TP-IP-range

Use this command to import TIR definitions from a *csv* file and to export TIR definitions to a *csv* file.

subscriber TP-IP-range { **import** | **export** } **csv-file** *filename*

Following is the format of the *csv* file:

range name, ip-address/mask-length, target-TP

Syntax Description

csv-filename *csv* file to be imported or exported to

import Import from the specified *csv* file.

export Export to the specified *csv* file.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Use the **remove-subscriber-mappings** keyword when importing TIR definitions to remove any existing subscriber mappings for specified IP ranges. If mappings exist, and this keyword is not used, the import command will not execute.

The **remove-subscriber-mappings** keyword is not applicable when exporting to a *csv* file.

Authorization: admin

Examples

The following example imports TIR information from the *csv* file *TIR_definitions*. The **remove-subscriber-mappings** keyword is used to remove any subscriber mappings that currently exist in the system on any of the IP ranges specified in the file.

```
SCE(config if)#subscriber TP-IP-range import csv-file
TIR_definitions remove-subscriber-mappings
```

Related Commands

tacacs-server host

Defines a new TACACS+ server host that is available to the SCE platform TACACS+ client.

Use the **no** form of the command to remove a TACACS+ server host.

The Service Control solution supports a maximum of three TACACS+ server hosts.

tacacs-server host *host-name* [**port** *port#*] [**timeout** *timeout-interval*] [**key** *key-string*]

no tacacs-server host *host-name*

Syntax Description

host-name name of the server

port # TACACS+ port number

timeout-interval time in seconds that the server waits for a reply from the server host before timing out

key-string encryption key that the server and client will use when communicating with each other. Make sure that the specified key is actually configured on the TACACS+ server host.

Defaults

Default *port#* = 49

Default *timeout-interval* = 5 seconds or user-configured global default timeout interval

Default *key-string* = no key or user-configured global default key

Command Modes

Global Configuration

Usage Guidelines

The user can configure a global default timeout interval that will be applied as the timeout to all TACACS+ server hosts. The timeout interval then does not need to be configured explicitly for each server. (See [tacacs-server timeout](#) (on page 2-267))

Similarly, the user can configure a global default key that will be applied to all TACACS+ server hosts. (See [tacacs-server key](#) (on page 2-266))

If the global default timeout interval and key string are configured, an explicitly configured value for a specific TACAS+ server overrides the global default for that server.

Authorization: admin

Examples

The following example shows how to configure a TACACS+ server host using the default port and no key.

```
SCE(config)# tacacs-server host server1 timeout 8
```

Related Commands

[tacacs-server key](#) (on page 2-266)

[tacacs-server timeout](#) (on page 2-267)

tacacs-server key

Defines the global default encryption key for the TACACS+ server hosts.

Use the **no** form of the command to clear the TACACS+ key.

tacacs-server key *key-string*

no tacacs-server key

Syntax Description	<i>key-string</i> default encryption key that all TACACS servers and clients will use when communicating with each other. Make sure that the specified key is actually configured on the TACACS+ server hosts.
Defaults	Default is no encryption
Command Modes	Global Configuration
Usage Guidelines	<p>This default key can be overridden for a specific TACACS+ server host by explicitly configuring a different key for that TACACS+ server host.</p> <p>If no global default key is defined, each TACACS+ server host may still have a specific key defined. However, any server host that does not have a key explicitly defined (uses the global default key) is now configured to use no key.</p> <p>Authorization: admin</p>
Examples	<p>The following example show how to configure the keystring.</p> <pre>SCE(config)# tacacs-server key ABCDE</pre>
Related Commands	<i>tacacs-server host</i> (on page 2-265)

tacacs-server timeout

Defines the global default timeout interval for the TACACS+ server hosts.

Use the **no** form of the command to clear the global default timeout interval.

tacacs-server timeout *timeout-interval*

no tacacs-server timeout

Syntax Description

timeout-interval default time in seconds that the server waits for a reply from the server host before timing out.

Defaults

Default = 5 seconds

Command Modes

Global Configuration

Usage Guidelines

This default timeout interval can be overridden for a specific TACACS+ server host by explicitly configuring a different timeout interval for that TACACS+ server host.

If no global default timeout interval is defined, each TACACS+ server host may still have a specific timeout interval defined. However, any server host that does not have a timeout interval explicitly defined (uses the global default timeout interval) is now configured to a five second timeout interval.

Authorization: admin

Examples

This example shows how to configure a default timeout interval of 10 seconds.

```
product>(config)# tacacs-server timeout 10
```

Related Commands

[tacacs-server host](#) (on page 2-265)

telnet

Starts a Telnet session.

telnet *address* [*ports*]

Syntax Description

address Telnet access address.

ports Optional port number.

Defaults

Default port is 23.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example starts a telnet session:
SCE#telnet 10.1.5.120
connecting to 10.1.5.120:23...

Related Commands

timeout

Configures the timeout for the Telnet session when the Telnet session is idle. After this time, the Telnet session is disconnected.

Use the **no** form of the command to configure the Telnet server to work with no timeout. No matter how long there is no activity on the Telnet session, the system does not automatically disconnect the Telnet session.

timeout *time*
no timeout

Syntax Description

<i>time</i>	Timeout length in minutes.
-------------	----------------------------

Defaults

time = 30 minutes

Command Modes

Line Configuration Mode

Usage Guidelines

Authorization: admin

Examples

The following example sets the timeout to 45 minutes.

```
SCE(config-line)#timeout 45  

SCE(config-line)#
```

Related Commands

no timeout

tos-marking mode

Enables TOS marking. The SCE Platform can mark the IP ToS field of transmitted packets, according to the Diffserv scheme standard code points.

Use the no form of the command to disable the TOS marking.

The platform supports the association of services to the following Diffserv classes: BE (Best effort), EF (Expedited forwarding), AF1, AF2, AF3 and AF4 (Assured forwarding 1-4, respectively). When packets exceed the bandwidth limit they are configured with, they are internally marked in RED color and dropped by the SCE Platform itself. Packets that are below their limit are marked with either green or yellow drop precedence depending on their actual relative rate.



Note

When TOS marking is enabled, the first few TCP packets are associated and marked with a default AF4 class that is mapped to the IQ2 queue. This occurs because the SCE Platform transmits the first few packets before classifying the flow and identifying the application or service

tos-marking mode *mode*
no tos-marking mode *mode*

Syntax Description	<i>mode</i> Mode for TOS marking. Currently the system supports only Diffserv .
--------------------	--

Defaults	By default, TOS marking is disabled.
----------	--------------------------------------

Command Modes	LineCard Interface Configuration
---------------	----------------------------------

Usage Guidelines	
------------------	--

Authorization: admin

Examples	The following example enables TOS marking: SCE(config if)#tos-marking mode Diffserv SCE(config if)#
----------	---

Related Commands	no tos-marking diffserv
------------------	-------------------------

tos-marking reset-table

Resets TOS settings to the Diffserv defaults.

tos-marking reset-table

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example resets the TOS marking.
SCE(config if)#tos-marking reset-table
SCE(config if)#

Related Commands

[tos-marking set-table-entry](#) (on page 2-272)

tos-marking set-table-entry

The SCE Platform supports configuration via CLI of the mapping between the class and coloring and the exposed DSCP (Diffserv Code Points) values. The default of this table is direct mapping of the Diffserv standard code points.

The TOS table reads the class and color of the packet being transmitted, and assigns the value set in the table according to the color and class.

tos-marking set-table-entry class *class* color *color* value *value*

Syntax Description		
	<i>class</i>	Internal class of service assigned to the packet. Legal values are BE , AF1 , AF2 , AF3 , AF4 and EF .
	<i>color</i>	Internal color assigned to the packet. Legal values are green , yellow , red and any .
	<i>value</i>	Value of the TOS marking, assigned to the packet IP header, as transmitted by the SCE Platform. This is a 6-bit value, expressed as a hex number in the range 0x0 to 0x3f .

Defaults

Diffserv defaults

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example sets a TOS marking table entry.

```
SCE(config if)# tos-marking set-table-entry class AF4 color yellow value 0x24
SCE(config if)#
```

Related Commands

tracert

Determines the route packets take to reach a specified host.

tracert [*hostname/IP-address*]

Syntax Description

hostname Destination hostname

IP-address Destination IP address

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

The destination of the traceroute function can be specified as either a known hostname or an IP address.

Authorization: admin

Examples

Following is a tracert command with sample output.

tracert 64.103.125.118

Sample output

SCE#traceroute to 10.56.217.103, 30 hops max, 40 byte packets

1	10.56.217.1 (10.56.217.1)	0 ms	1 ms	0 ms
2	10.56.223.9 (10.56.223.9)	1 ms	0 ms	1 ms
3	64.103.115.209 (64.103.115.209)	0 ms	1 ms	0 ms
4	64.103.125.118 (64.103.125.118)	0 ms	0 ms	0 ms

Trace complete.

SCE#

Related Commands

traffic-counter

Defines a new traffic counter. Use the no form of the command to delete an existing traffic counter.

traffic-counter name *name* { **count-bytes** | **count-packets** }

no traffic-counter { **name** *name* | **all** }

Syntax Description

name Name to be assigned to this traffic counter.

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

The following are usage guidelines for the **traffic-counter** command:

- Use the **count-bytes** keyword to enable counting the bytes in each packet.
The counter will increment by the number of bytes in each packet.
- Use the **count-packets** keyword to enable counting whole packets.
The counter will increment by one for each packet.

Use the **all** keyword with the **no** form to delete all existing traffic counters.

Authorization: admin

Examples

The following are examples of the **traffic-counter** command:

EXAMPLE 1:

Following is an example of creating a traffic counter that will count bytes.

```
SCE(config if)# traffic-counter name counter1 count-bytes
```

EXAMPLE 2:

The following example demonstrates how to delete all traffic counters.

```
SCE(config if)# no traffic-counter all
```

Related Commands

traffic-rule

Defines a new traffic rule. Use the no form of the command to delete an existing traffic rule.

traffic-rule *name* **IP addresses** *IP-addresses* **protocol** *protocol* [**tunnel-id** *tunnel-id*] **direction** *direction* **traffic-counter** *traffic-counter* **action** *action*

traffic-rule tunnel-id-mode

no traffic-rule {**name** *name* |**all**|**tunnel-id-mode**}

Syntax Description

<i>name</i>	name to be assigned to this traffic rule.
<i>IP-addresses</i>	subscriber-side and network-side <IP specification> (see below)
<i>protocol</i>	Any one of the following protocols: <i>TCP/UCP/ICMP/IGRP/EIGRP/IS-IS/OSPF/Other</i>
<i>tunnel-id</i>	Tunnel ID, <tunnel Id specification> (see below).
<i>direction</i>	upstream/downstream/both
<i>traffic-counter</i>	name of traffic counter/none
<i>action</i>	<i>block ignore</i>

Defaults

This command has no default settings.

Command Modes

LineCard Interface Configuration

Usage Guidelines

The following are the usage guidelines for the **traffic-rule** command:

IP specification:

all([all-but] (<ip-address>|<ip-range>))

- <ip-address> is a single IP address in dotted-decimal notation, such as 10.1.2.3
- <ip-range> is an IP subnet range, in the dotted-decimal notation followed by the number of significant bits, such as 10.1.2.0/24.

tunnel id specification:

all([all-but] tunnel id)

- tunnel id is a Hex Tunnel id range, in the format '(HEX)Tunnel-id' or '(HEX)MinTunnelId:(HEX)MaxTunnelId'

traffic-counter:

Either of the following:

- *Name of an existing traffic counter*: Packets meeting the criteria of the rule are to be counted in the specified counter. If a counter name is defined, the “count” action is also defined implicitly.
- *none*: If **none** is specified, then an action must be explicitly defined via the **action** option.
- Use the **all** keyword with the no form to delete all existing traffic rules.
- Use the **tunnel-id-mode** keyword to enable or disable defining the traffic rule according to the tunnel ID.

Authorization: admin

Examples

The following are examples of the traffic-rule command:

EXAMPLE 1:

This example creates the following traffic rule:

Name = rule2

IP addresses: subscriber side = all IP addresses, network side = all IP addresses EXCEPT the subnet 10.10.10.0/24

Protocol = TCP

Direction = downstream

Traffic counter = counter2

Action = Block

The actions performed will be counting and blocking

```
SCE (config if)# traffic-rule rule2 IP-addresses subscriber-side
all network-side all-but 10.10.10.0/24 protocol TCP direction
downstream traffic-counter counter2 action block
```

EXAMPLE 2:

This example creates the following traffic rule:

Name = rule3

IP addresses: all

Protocol = IS-IS

Direction = upstream

Traffic counter = none

Action = ignore (required since traffic-counter = none)

The only action performed will be **Ignore**.

```
SCE (config if)# traffic-rule rule3 IP-addresses all protocol IS-  
IS direction upstream traffic-counter none action ignore
```

EXAMPLE 3:

The following example demonstrates how to delete all traffic rules.

```
SCE(config if)# no traffic-rule all
```

Related Commands

unzip

Extracts a zip file to the current directory.

unzip *filename*

Syntax Description

filename Zip file to be extracted.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example extracts the zipfile.zip:

```
SCE#unzip zipfile.zip
```

```
Unzipping '/tffs0/zipfile.zip'...
```

```
Zip file has 3 entries:
```

```
  1.sli, 13429 bytes extracted
```

```
  preflut.sli, 12558 bytes extracted
```

```
  temp/SLI/x/IpraeLut.sli, 12929 bytes extracted
```

```
Finished, Extracted 3 files.
```

Related Commands

username

Adds a new user to the local database

Use the **no** form of the command to remove a user from the database.

username *name* { **password** *password* | **nopassword** | **secret** { **0** *password* | **5** *password* }

no username *name*

Syntax Description

<i>name</i>	name of the user to be added
<i>password</i>	a clear text password.
<i>secret</i>	the password is saved in MD5 encrypted form. The keywords 0 or 5 indicate the format of the password as entered in the command:

Defaults

Command Modes

Global Configuration

Usage Guidelines

Up to 100 users may be defined.

The password is defined with the username. There are several password options:

- **No password:** use the *nopassword* keyword.
- **Password:** Password is saved in clear text format in the local list.
Use the *password* parameter.
- **Encrypted password:** Password is saved in encrypted (MD5) form in the local list. Use the *secret* keyword and either of the following options.

Password may be defined by either of the following methods:

- Specify a clear text password, which is saved in MD5 encrypted form
- Specify an MD5 encryption string, which is saved as the user MD5-encrypted secret password

The following keywords are available:

- **nopassword:** There is no password associated with this user
- **secret:** the password is saved in MD5 encrypted form. Use with either of the following keywords to indicate the format of the password as entered in the command:
 - **0:** the *<password>* parameter specifies a clear text password that will be saved in MD5 encrypted form
 - **5:** the *<password>* parameter specifies an MD5 encryption string that will be saved as the user MD5-encrypted secret password

Authorization: admin

Examples**EXAMPLE 1**

This example shows how to add a new user to the local database with a clear text password.

```
product>(config)# username johndoe password mypassword
```

EXAMPLE 2

This example shows how to add a new user to the local database with no password.

```
product>(config)# username johndoe nopassword
```

EXAMPLE 3

This example shows how to add a new user to the local database with with an MD5 encrypted password entered in clear text.

```
product>(config)# username johndoe secret 0 mypassword
```

Related Commands

username privilege

Sets the privilege level of the specified user.

username *name* **privilege** *level*

Syntax Description

<i>name</i>	name of the user whose privilege level is set
<i>level</i>	the privilege level permitted to the specified user. These levels correspond to the CLI authorization levels, which are entered via the enable command:
	0: User
	5: Viewer
	10: Admin
	15: Root

Defaults

Default level = 15

Command Modes

Global Configuration

Usage Guidelines

When a user requests an authorization for a specified privilege level, by using the "**enable**" command, the SCE platform sends an authentication request to the TACACS+ server specifying the requested privilege level. The SCE platform grants the requested privilege level only after the TACACS+ server authenticates the "**enable**" command password and verifies that the user has sufficient privileges to enter the requested privilege level.

Authorization: admin

Examples

The following level sets the privilege level for the user to "Viewer".
SCE(config)# username johndoe privilege 5

Related Commands

VAS-traffic-forwarding

Enables VAS traffic forwarding.

Use the **no** form of the command to disable VAS traffic forwarding. Refer to the example below for complete instructions on how to disable VAS traffic.

VAS-traffic-forwarding

no VAS-traffic-forwarding

Syntax Description

This command has no arguments or keywords.

Defaults

By default, VAS traffic forwarding is disabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

There are certain other SCE platform features that are incompatible with VAS traffic forwarding. Before enabling VAS traffic forwarding, it is the responsibility of the user to make sure that no incompatible features or modes are configured.

The features and modes listed below cannot coexist with VAS mode:

- Line-card connection modes: receive-only, receive-only-cascade, inline-cascade
- Link mode other than forwarding
- All link encapsulation protocols, including VLAN, MPLS, L2TP

Authorization: admin

Examples

This example shows how to enable VAS traffic forwarding.

Step 1 From the SCAS BB console, remove all the VAS table associations to packages and apply the changed policy.

Step 2 Shutdown the line card:

Execute the CLI command **shutdown** from the LineCard Interface Configuration mode.

Step 3 Disable VAS traffic forwarding:

Execute the CLI command **no VAS-traffic-forwarding** from the LineCard Interface Configuration mode.

Step 4 Re-enable the line card:

Execute the CLI command 'no shutdown' from the LineCard Interface Configuration mode.

Related Commands

VAS-traffic-forwarding VAS server-id (on page 2-290)

VAS-traffic-forwarding VAS traffic-link (on page 2-293)

VAS-traffic-forwarding VAS server-id health-check (on page 2-284)

VAS-traffic-forwarding VAS server-group (on page 2-286)

VAS-traffic-forwarding VAS server-group failure (on page 2-288)

show interface linecard 0 VAS-traffic-forwarding (on page 2-188)

VAS-traffic-forwarding VAS server-id health-check

Enables or disables the VAS health check, and defines the ports it should used.

Use the **UDP ports** keyword to define source and destination UDP ports to be used by the health check packets.

Use the **no** form of this command to disable the health check.

Use either the **no** or **default** form of this command with the **UDP ports** keyword to remove the UDP port configuration.

VAS-traffic-forwarding VAS server-id *number* health-check

VAS server-id *number* health-check UDP ports source *<port number>* **destination** *<port number>*

no VAS-traffic-forwarding VAS server-id *number* health-check

no VAS-traffic-forwarding VAS server-id *number* health-check UDP ports

default VAS-traffic-forwarding VAS server-id *number* health-check UDP ports

Syntax Description

number ID number of the VAS server for which to enable or disable the health check
port-number source or destination port number (use with the **source** and **destination** options)

Defaults

By default, the health check is enabled.

Default port numbers = <63140,63141> used for server #0 through <63154,63155> used for server #7.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Use the **UDP ports** keyword to define **source** and **destination** UDP ports to be used by the health check packets.

Note that the health check is activated only if all the following conditions are true. If the health check is enabled but one or more of the following conditions are not met, the server state will be **Down**:

- VAS Traffic Forwarding mode is enabled
- Pseudo IPs are configured for the SCE platform GBE ports on the VAS traffic link
- VAS server is enabled
- Server has a VLAN tag
- Health check for the server is enabled

If the health check of the server is disabled, its operational status depends on the following (requirements for **Up** state are in parentheses):

- admin status (enable)
- VLAN tag configuration (VLAN tag defined)
- group mapping (assigned to group)

Authorization: admin

Examples

The following examples illustrate how to disable the health check, and how to define the UDP ports.

EXAMPLE 1

This example shows how to disable the health check for VAS server 5.

```
no VAS-traffic-forwarding VAS server-id 5 health-check
```

EXAMPLE 2

This example shows how to define the source and destination ports for VAS server 5 and enable the health check.

```
VAS-traffic-forwarding VAS server-id 5 health-check UDP ports  
source 63150 destination 63151  
VAS-traffic-forwarding VAS server-id 5 health-check
```

EXAMPLE 3

This example shows how to remove the UDP port configuration. You can use either the **no** keyword or the **default** keyword, the result is the same.

```
no VAS-traffic-forwarding VAS server-id <number> health-check UDP ports  
default VAS-traffic-forwarding VAS server-id <number> health-  
check UDP ports
```

Related Commands

[VAS-traffic-forwarding](#) (on page 2-282)

[VAS-traffic-forwarding VAS server-id](#) (on page 2-290)

[VAS-traffic-forwarding VAS traffic-link](#) (on page 2-293)

[VAS-traffic-forwarding VAS server-group](#) (on page 2-286)

[VAS-traffic-forwarding VAS server-group failure](#) (on page 2-288)

[show interface linecard 0 VAS-traffic-forwarding](#) (on page 2-188)

VAS-traffic-forwarding VAS server-group

Adds servers to and removes them from a specified VAS server group.

Use the **no** form of this command to remove a specified server from the VAS server group.

VAS-traffic-forwarding VAS server-group *group-number* **server-id** *server-number*

no VAS-traffic-forwarding VAS server-group *group-number* **server-id** *server-number*

Syntax Description

group-number The ID number of the VAS server group

server-number The ID number of the VAS server

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

The user may define up to eight VAS server groups. Each VAS server group has the following parameters:

Usage Guidelines

- Server Group ID
- A list of VAS servers attached to this group.
- Failure detection — minimum number of active servers required for this group so it will be considered to be Active. If the number of active servers goes below this minimum, the group will be in Failure state.
- Failure action — action performed on all new data flows that should be mapped to this Server Group while it is in Failure state.

If no VAS server ID is specified in the **no** form of the command, all servers are removed from the server group and all group parameters (failure detection and action) are set to the default values (see [VAS-traffic-forwarding VAS server-group failure](#) (on page 2-288)).

Authorization: admin

Examples

The following examples illustrate how to add servers to and remove servers from a specified VAS server group.

EXAMPLE 1

This example shows how to add VAS server 5 to VAS server group 1.

VAS-traffic-forwarding VAS server-group 1 VAS server-id 5

EXAMPLE 2

This example shows how to remove VAS server 5 from VAS server group 1.

```
no VAS-traffic-forwarding VAS server-group 1 VAS server-id 5
```

EXAMPLE 3

This example shows how to remove all VAS servers from VAS server group 1 and set all group parameters (failure detection and action) to the default values.

```
no VAS-traffic-forwarding VAS server-group 1
```

Related Commands

[VAS-traffic-forwarding](#) (on page 2-282)

[VAS-traffic-forwarding VAS server-id](#) (on page 2-290)

[VAS-traffic-forwarding VAS traffic-link](#) (on page 2-293)

[VAS-traffic-forwarding VAS server-id health-check](#) (on page 2-284)

[VAS-traffic-forwarding VAS server-group failure](#) (on page 2-288)

[show interface linecard 0 VAS-traffic-forwarding](#) (on page 2-188)

VAS-traffic-forwarding VAS server-group failure

Configures the failure parameters for the specified VAS server group.

Use either the **no** form or the **default** form of the command to set the specified failure parameter to the default value.

VAS-traffic-forwarding VAS server-group *group-number* **failure minimum-active-servers** *min-number*

VAS-traffic-forwarding VAS server-group *group-number* **failure action** {**block** | **pass**}

default VAS-traffic-forwarding VAS server-group *group-number* **failure minimum-active-servers**

no VAS-traffic-forwarding VAS server-group *group-number* **failure minimum-active-servers**

default VAS-traffic-forwarding VAS server-group *group-number* **failure action**

no VAS-traffic-forwarding VAS server-group *group-number* **failure action**

Syntax Description

group-number The ID number of the VAS server group

min-number The minimum number of active servers required for the specified server group.

failure action The action to be applied to all new flows mapped to this server group while it is Failure state

block — all new flows assigned to the failed VAS server group will be blocked by the SCE platform

pass — all new flows assigned to the failed VAS server group will be considered as regular non-VAS flows, and will be processed without VAS service.

Defaults

Default failure minimum-active-servers min-number = 1

Default failure action = pass

Command Modes

Interface Linecard Configuration

Usage Guidelines

To set both group parameters (failure detection and action) to the default values, use the **no** form of the command without specifying any parameter (see [VAS-traffic-forwarding VAS server-group](#) (on page 2-286).)

Authorization: admin

Examples

The following examples illustrate how to set the failure parameters to specified values or to the default value.

EXAMPLE 1

The following example shows how to configure the minimum number of active servers for VAS server group 5.

```
SCE(config-if)#VAS-traffic-forwarding VAS server-group 5 failure  
minimum-active-servers 3
```

EXAMPLE 2

The following example shows how to reset the minimum number of active servers for VAS server group 5 to the default value.

```
SCE(config-if)#default VAS-traffic-forwarding VAS server-group 5  
failure minimum-active-servers
```

Related Commands

[VAS-traffic-forwarding](#) (on page 2-282)

[VAS-traffic-forwarding VAS server-id](#) (on page 2-290)

[VAS-traffic-forwarding VAS traffic-link](#) (on page 2-293)

[VAS-traffic-forwarding VAS server-id health-check](#) (on page 2-284)

[VAS-traffic-forwarding VAS server-group](#) (on page 2-286)

[show interface linecard 0 VAS-traffic-forwarding](#) (on page 2-188)

VAS-traffic-forwarding VAS server-id

Enables or disables a VAS server. Use the **enable** keyword to enable a new or existing VAS server. Use the **disable** keyword to disable an existing VAS server (server properties are not deleted).

Use the **no** form or the **default** form of this command to delete all server properties from a specified VAS server.

VAS-traffic-forwarding VAS server-id *number* **enable**

VAS-traffic-forwarding VAS server-id *number* **disable**

no VAS-traffic-forwarding VAS server-id *number*

default VAS-traffic-forwarding VAS server-id *number*

Syntax Description	<i>number</i> The ID number of the VAS server
Defaults	By default, a defined VAS server is enabled.
Command Modes	LineCard Interface Configuration
Usage Guidelines	<p>The VAS server is not operational until the VLAN tag is defined (<i>VAS-traffic-forwarding server-id VLAN</i> (on page 2-292)).</p> <p>Authorization: admin</p>
Examples	<p>The following examples illustrate how to create, enable, and disable a VAS server:</p> <p>EXAMPLE 1:</p> <p>The following example defines a VAS server, server ID number = 4, that is not yet operational.</p> <p>SCE(config if)# VAS-traffic-forwarding VAS server-id 4 enable</p> <p>EXAMPLE 2:</p> <p>The following example disables the VAS server, but does not delete the server definition or the associated VLAN tag.</p> <p>SCE(config if)# VAS-traffic-forwarding VAS server-id 4 disable</p>
Related Commands	<p><i>VAS-traffic-forwarding</i> (on page 2-282)</p> <p><i>VAS-traffic-forwarding server-id VLAN</i> (on page 2-292)</p> <p><i>VAS-traffic-forwarding VAS traffic-link</i> (on page 2-293)</p>

VAS-traffic-forwarding VAS server-id health-check (on page 2-284)

VAS-traffic-forwarding VAS server-group (on page 2-286)

VAS-traffic-forwarding VAS server-group failure (on page 2-288)

show interface linecard 0 VAS-traffic-forwarding (on page 2-188)

VAS-traffic-forwarding server-id VLAN

Assigns the VLAN ID to a specified VAS server.

Use the **no** form or the **default** form of this command to delete the VLAN tag assignment from a specified VAS server.

VAS-traffic-forwarding VAS server-id *number* **VLAN** *vlan-number*

no VAS-traffic-forwarding VAS server-id *number* **VLAN**

default VAS-traffic-forwarding VAS server-id *number* **VLAN**

Syntax Description	<p><i>number</i> The ID number of the VAS server</p> <p><i>vlan-number</i> The VLAN tag to use for the specified VAS server</p>
Defaults	Default vlan-number = No VLAN
Command Modes	LineCard Interface Configuration
Usage Guidelines	<p>Note the following important points:</p> <ul style="list-style-type: none"> • The VAS server is not operational until the VLAN tag is defined. • Disabling the server does not remove the VLAN tag number configured to the server. • The no form of the command (same as the default form of the command), removes the previously configured VLAN tag (no VLAN is the default configuration). <p>Authorization: admin</p> <p>The following example assigns the vlan id = 10 to server ID number = 4.</p>
Examples	VAS-traffic-forwarding VAS server-id 4 VLAN 10
Related Commands	<p>VAS-traffic-forwarding (on page 2-282)</p> <p>VAS-traffic-forwarding VAS server-id (on page 2-290)</p> <p>VAS-traffic-forwarding VAS server-group (on page 2-286)</p> <p>VAS-traffic-forwarding VAS server-group failure (on page 2-288)</p> <p>VAS-traffic-forwarding VAS traffic-link (on page 2-293)</p> <p> </p> <p>show interface linecard 0 VAS-traffic-forwarding (on page 2-188)</p>

VAS-traffic-forwarding traffic-link

Configures the link on which to transmit VAS traffic (the link to which the VAS servers are connected).

Use the **no** form of the command to remove the VAS link configuration and revert to the VAS link defaults.

VAS-traffic-forwarding traffic-link *{link-0/link-1}*

no VAS-traffic-forwarding traffic-link

Syntax Description

Enter the link number on which to transmit VAS traffic

Link-0

Link-1

Defaults

Default traffic link = Link-1

Command Modes

Interface Linecard Configuration

Usage Guidelines



Note

The VAS traffic link should be in Forwarding mode.

Authorization: admin

Examples

This example shows how to configure link 0 for VAS traffic.

VAS-traffic-forwarding traffic-link-0

Related Commands

[VAS-traffic-forwarding](#) (on page 2-282)

[VAS-traffic-forwarding VAS server-id](#) (on page 2-290)

[VAS-traffic-forwarding VAS server-group](#) (on page 2-286)

[VAS-traffic-forwarding VAS server-group failure](#) (on page 2-288)

[show interface linecard 0 VAS-traffic-forwarding](#) (on page 2-188)

VLAN

Configures the VLAN environment.

VLAN option

Syntax Description

option There are three options:
symmetric classify: Subscriber and flow classification use the VLAN tag. VLAN tags are symmetric.
symmetric skip: Skip the VLAN header, because subscriber and flow classification do not use the VLAN tag. VLAN tags are symmetric.
a-symmetric skip: Skip the VLAN header, because subscriber and flow classification do not use the VLAN tag. VLAN tags are asymmetric. .

Defaults

symmetric skip

Command Modes

LineCard Interface Configuration

Usage Guidelines

A symmetric environment is one in which the same VLAN tags are used for carrying a transaction in the upstream and downstream directions.

An asymmetric environment is one in which the upstream and downstream VLAN tags might not be the same.

The SCE platform is configured by default to work in symmetric environments. A specific command (*a-symmetric skip*) is necessary in order to allow correct operation of the SCE platform in an asymmetric environments, and instruct it to take into consideration that the upstream and downstream of each flow has potentially different VLAN tags.

Authorization: admin

Examples

The following example configures the VLAN environment:
SCE(config if)#vlan symmetric skip

Related Commands

vlan translation

Sets the VLAN translation constant for the network port side. The subscriber ports are doing the reverse operation. For example, if network is incrementing by 5 then subscriber port will be decremented by 5.

Use the [no] form of this command to disable vlan translation for this port (sets the value to zero).

vlan translation {increment | decrement} value *value*

no vlan translation

Syntax Description

value The value of the VLAN translation constant for the network port side.

Defaults

value = 0

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example specifies a VLAN translation constant of 16 for the network port side .
SCE(config if)#vlan translation increment value 16

Related Commands

wap

Enables or disables operating in a WAP-based environment. Use the **no** form of the command to disable operating in a WAP-based environment

wap

no wap

Syntax Description

This command has no arguments or keywords

Defaults

By default, operating in a WAP environment is disabled.

Command Modes

LineCard Interface Configuration

Usage Guidelines

Authorization: admin

Examples

The following example illustrates how to enable operating in a WAP-based environment

wap

Related Commands



Index

?

? • 2-2

A

aaa authentication accounting commands • 2-4
aaa authentication attempts • 2-5
aaa authentication enable default • 2-6
aaa authentication login default • 2-13
accelerate-packet-drops • 2-9
access-class • 2-3
access-list • 2-7
active-port • 2-10
Argument Help • 1-14
attack-detector • 2-14
attack-detector <number> • 2-15
attack-detector default • 2-11
attack-detector TCP-port-list|UDP-port-list • 2-17
attack-filter (LineCard Interface Configuration) • 2-18
attack-filter (Privileged Exec) • 2-20
attack-filter subscriber-notification ports • 2-22
Audience • xi
Authorization and Command Levels (Hierarchy) • 1-2
auto-fail-over • 2-23
auto-negotiate (GigabitEthernet only) • 2-24

B

bandwidth • 2-25
blink • 2-26
boot system • 2-27

C

calendar set • 2-28

cd • 2-29

Cisco.com • xv

clear arp-cache • 2-30

clear interface linecard • 2-31

clear interface linecard 0 VAS-traffic-forwarding VAS all counters health-check • 2-34

clear interface linecard subscriber • 2-32

clear interface linecard subscriber db counters • 2-33

clear interface linecard traffic-counter • 2-37

clear logger • 2-35

clear RDR-formatter • 2-38

CLI Authorization Levels • 1-6

CLI Command Hierarchy • 1-3

CLI Command Reference • 2-1

CLI Commands • 2-2

CLI Help Features • 1-14

CLI Scripts • 1-19

clock read-calendar • 2-39

clock set • 2-40

clock summertime • 2-41

clock timezone • 2-44

clock update-calendar • 2-45

Command History • 1-15

Command-Line Interface • 1-1

configure • 2-46

Configuring the Physical Ports • 1-9

connection-mode (SCE 1000 platform) • 2-47

connection-mode (SCE 2000 platform) • 2-48

Contacting TAC by Telephone • xvi

Contacting TAC by Using the Cisco TAC Website • xv

Conventions • xii

copy • 2-49

copy ftp

// • 2-50
 copy running-config startup-config • 2-52
 copy source-file ftp
 // • 2-53
 copy source-file startup-config • 2-54
 copy startup-config destination-file • 2-55
 copy-passive • 2-51

D

default subscriber template all • 2-56
 delete • 2-57
 dir • 2-58
 disable • 2-59
 do • 2-60
 Document Revision History • xi
 Documentation CD-ROM • xiv
 Documentation Feedback • xiv
 duplex • 2-61

E

enable • 2-62
 enable password • 2-63
 Entering and Exiting Global Configuration Mode • 1-9
 Entering Ethernet Line Interface Configuration Mode • 1-12
 Entering LineCard Interface Configuration Mode • 1-11
 Entering Management Interface Configuration Mode • 1-11
 Entering the Fast Ethernet Line Interface Configuration Mode • 1-12
 Entering the Gigabit Ethernet Line Interface Configuration Mode • 1-12
 erase startup-config-all • 2-64
 exit • 2-65
 Exiting Modes • 1-8

F

failure-recovery operation-mode • 2-66
 Filtering Command Output • 1-18
 force failure-condition (SCE 2000 only) • 2-67
 FTP User Name and Password • 1-17

G

Getting Help • 1-1

H

help • 2-68

history • 2-70
 history size • 2-71
 hostname • 2-72

I

Interface Configuration Modes • 1-9
 interface FastEthernet • 2-73
 interface GigabitEthernet • 2-74
 interface LineCard • 2-75
 interface Mng • 2-76
 ip access-class • 2-77
 ip address • 2-78
 ip advertising • 2-79
 ip default-gateway • 2-80
 ip domain-lookup • 2-81
 ip domain-name • 2-82
 ip filter fragment • 2-83
 ip filter monitor • 2-84
 ip ftp password • 2-85
 ip ftp username • 2-86
 ip host • 2-87
 ip name-server • 2-88
 ip route • 2-89
 ip rpc-adapter • 2-90
 ip rpc-adapter port • 2-91
 ip ssh • 2-92
 ip ssh access-class • 2-93
 ip ssh key • 2-94
 ip-tunnel L2TP skip • 2-95

K

Keyboard Shortcuts • 1-15

L

L2TP identify-by • 2-96
 line vty • 2-97
 link failure-reflection • 2-98
 link mode • 2-99
 logger add-user-message • 2-101
 logger device User-File-Log • 2-102
 logger device User-File-Log max-file-size • 2-103
 logger get support-file • 2-104
 logger get user-log file-name • 2-105
 logout • 2-106

M

management-agent access-class • 2-107
 management-agent sce-api logging • 2-108
 management-agent sce-api timeout • 2-110

management-agent system • 2-111
 Managing Command Output • 1-17
 mkdir • 2-112
 more • 2-113
 more user-log • 2-114
 MPLS • 2-115

N

Navigating Between Configuration Modes • 1-9
 Navigating between the Interface Configuration Modes • 1-13
 Navigational and Shortcut Features • 1-15
 no subscriber • 2-116
 no subscriber anonymous-group • 2-117
 no subscriber mappings included-in • 2-118

O

Obtaining Documentation • xiii
 Obtaining Technical Assistance • xiv
 Ordering Documentation • xiv
 Organization • xii

P

Partial Help • 1-14
 ping • 2-119
 pqi install file • 2-120
 pqi rollback file • 2-121
 pqi uninstall file • 2-122
 pqi upgrade file • 2-123
 Preface • xi
 Prompt Indications • 1-7
 pwd • 2-124

Q

queue • 2-125

R

RDR-formatter category-number • 2-126
 RDR-formatter destination • 2-127
 RDR-formatter forwarding-mode • 2-129
 RDR-formatter history-size • 2-130
 RDR-formatter protocol • 2-131
 RDR-formatter protocol RDRv2 connection-timeout • 2-132
 RDR-formatter rdr-mapping • 2-133
 Redirecting Command Output to a File • 1-18
 Related Publications • xii
 reload • 2-134

reload shutdown • 2-135
 rename • 2-136
 rmdir • 2-137

S

script capture • 2-138
 script print • 2-139
 script run • 2-140
 script stop • 2-141
 Scrolling the Screen Display • 1-17
 service password-encryption • 2-142
 service RDR-formatter • 2-143
 service telnetd • 2-144
 setup • 2-145
 show access-lists • 2-149
 show blink • 2-150
 show calendar • 2-151
 show clock • 2-152
 show failure-recovery operation-mode • 2-153
 show hostname • 2-154
 show hosts • 2-155
 show interface FastEthernet • 2-156
 show interface GigabitEthernet • 2-159
 show interface LineCard • 2-161
 show interface LineCard [VLAN|L2TP|IP-tunnel] • 2-191
 show interface LineCard application • 2-162
 show interface LineCard attack-detector • 2-163
 show interface LineCard attack-filter • 2-164
 show interface LineCard connection-mode • 2-166
 show interface LineCard counters • 2-167
 show interface LineCard link mode • 2-168
 show interface LineCard link-bypass (SCE 1000 only) • 2-169
 show interface LineCard physically-connected-links (SCE 2000 only) • 2-170
 show interface LineCard silent • 2-171
 show interface LineCard subscriber • 2-172
 show interface LineCard subscriber aging • 2-173
 show interface LineCard subscriber anonymous • 2-174
 show interface LineCard subscriber anonymous-group • 2-175
 show interface LineCard subscriber db counters • 2-176

- show interface LineCard subscriber mapping • 2-178
- show interface LineCard subscriber mapping included-in TP-IP-range • 2-183
- show interface LineCard subscriber name • 2-179
- show interface LineCard subscriber properties • 2-180
- show interface LineCard subscriber TP-IP-range • 2-182
- show interface LineCard subscriber TP-mappings statistics • 2-181
- show interface LineCard tos-marking mode • 2-184
- show interface LineCard tos-marking table • 2-185
- show interface LineCard traffic-counter • 2-186
- show interface LineCard traffic-rule • 2-187
- show interface linecard VAS-traffic-forwarding • 2-188
- show interface LineCard vlan translation • 2-192
- show interface Mng • 2-160
- show ip access-class • 2-193
- show ip advertising • 2-194
- show ip default-gateway • 2-196
- show ip filter • 2-195
- show ip route • 2-197
- show ip rpc-adapter • 2-198
- show ip ssh • 2-199
- show line vty • 2-200
- show logger device User-File-Log • 2-201
- show logger device User-File-Log counters • 2-202
- show logger device User-File-Log max-file-size • 2-202
- show logger device User-File-Log nv-counters • 2-205
- show logger device User-File-Log status • 2-204
- show management-agent sce-api • 2-206
- show pqi file • 2-207
- show pqi last-installed • 2-208
- show RDR-formatter • 2-209
- show RDR-formatter connection-status • 2-210
- show RDR-formatter counters • 2-211
- show RDR-formatter destination • 2-212
- show RDR-formatter enabled • 2-213
- show RDR-formatter forwarding-mode • 2-214
- show RDR-formatter statistics • 2-215
- show running-config • 2-216
- show snmp • 2-218
- show snmp community • 2-220
- show snmp contact • 2-221
- show snmp enabled • 2-222
- show snmp host • 2-223
- show snmp location • 2-224
- show snmp MIB • 2-225
- show snmp traps • 2-226
- show sntp • 2-227
- show startup-config • 2-228
- show system operation-status • 2-229
- show system-uptime • 2-230
- show tacacs • 2-231
- show telnet sessions • 2-232
- show telnet status • 2-233
- show timezone • 2-234
- show users • 2-235
- show version • 2-236
- show version all • 2-238
- show version software • 2-241
- silent • 2-242
- snmp-server • 2-243
- snmp-server community • 2-244
- snmp-server contact • 2-245
- snmp-server enable traps • 2-246
- snmp-server host • 2-248
- snmp-server location • 2-249
- sntp broadcast client • 2-251
- sntp server • 2-250
- sntp update-interval • 2-252
- speed • 2-253
- subscriber aging • 2-254
- subscriber anonymous-group export csv-file • 2-255
- subscriber anonymous-group import csv-file • 2-256
- subscriber export csv-file • 2-257
- subscriber import csv-file • 2-258
- subscriber sm-connection-failure • 2-259
- subscriber template export csv-file • 2-260
- subscriber template import csv-file • 2-261
- subscriber TP-IP-range • 2-264
- subscriber TP-IP-range name IP-range target-TP • 2-262
- subscriber TP-mappings • 2-263
- Syntax and Conventions • 2-1

T

Tab Completion • 1-16
tacacs-server host • 2-265
tacacs-server key • 2-266
tacacs-server timeout • 2-267
Technical Assistance Center • xv
telnet • 2-268
The • 1-13
The [no] Prefix • 1-15
timeout • 2-269
tos-marking mode • 2-270
tos-marking reset-table • 2-271
tos-marking set-table-entry • 2-272
tracert • 2-273
traffic-counter • 2-274
traffic-rule • 2-275

U

unzip • 2-278
username • 2-279
username privilege • 2-281

V

VAS-traffic-forwarding • 2-282
VAS-traffic-forwarding server-id VLAN •
2-292
VAS-traffic-forwarding traffic-link • 2-293
VAS-traffic-forwarding VAS server-group •
2-286
VAS-traffic-forwarding VAS server-group
failure • 2-288
VAS-traffic-forwarding VAS server-id • 2-
290
VAS-traffic-forwarding VAS server-id
health-check • 2-284
VLAN • 2-294
vlan translation • 2-295

W

wap • 2-296
World Wide Web • xiii