CHAPTER 2

CLI Command Reference

Revised: March 28, 2010, OL-22197-01

Introduction

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

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

Description	Description of what the command does.
Command Syntax	The general format of the command.
Syntax Description	Description of parameters and options for the command.
Default	If relevant, the default setting for the command.
Mode	The mode (command line) from which the command can be invoked.
Usage guidelines	Information about when to invoke the command and additional details.
Authorization	The level of user authorization required for using the command.
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.
Related Commands	Other commands that might be used in conjunction with the command.

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.

?

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.

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
```

aaa accounting commands

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

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

no aaa accounting commands *level* default

Syntax Description

level	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

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.

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.

Authorization: admin

Examples

The following example enables TACACS+ accounting for the admin privilege level (10).

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# aaa accounting commands 10 default stop-start group tacacs+
SCE(config)#
```

Related Commands

Command	Description
aaa authentication attempts	Sets the maximum number of login attempts that will be permitted before a Telnet session is terminated.
aaa authentication enable default	Specifies which privilege level authentication methods are to be used, and in what order of preference.
aaa authentication login default	Specifies which login authentication methods are to be used, and in what order of preference.

tacacs-server host	Defines a new TACACS+ server host that is available to the SCE platform TACACS+ client.
tacacs-server key	Defines the global default encryption key for the TACACS+ server hosts.

aaa authentication attempts

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
product>(config)# aaa authentication attempts login 5
SCE(config)#
```

Related Commands

Command	Description
aaa authentication accounting commands	Enables TACACS+ accounting.
aaa authentication enable default	Specifies which privilege level authentication methods are to be used, and in what order of preference.
aaa authentication login default	Specifies which login authentication methods are to be used, and in what order of preference.

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

Examples

This example shows how to configure privilege level authentication methods.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# aaa authentication enable default group tacacs+ enable none
SCE(config)#
```

Related Commands

Command	Description
aaa authentication login default	
aaa authentication accounting commands	

aaa authentication attempts
show tacacs

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

Examples

This example shows how to configure login authentication methods.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# aaa authentication login default group tacacs+ enable none
SCE(config)#
```

Related Commands

Command	Description
aaa authentication enable default	
aaa authentication accounting commands	

aaa authentication attempts
show tacacs

accelerate-packet-drops

Enables the drop-wred-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-wred-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-wred-packets-by-hardware mode) is enabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

By default, the SCE platform hardware drops WRED 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-wred-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-wred-packets-by-hardware mode is enabled.

Note The MIB object *tpTotalNumWredDiscardedPackets* counts dropped packets. The value in this counter is absolute only in **no accelerate-packet-drops** mode. When in **accelerate-packet-drops** mode (default mode), this MIB counter provides only a relative value indicating the trend of the number of packet drops, with a factor of approximately 1:6.

Authorization: admin

Examples

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

```
SCE>enable 10
password:<cisco>
SCE#>config
SCE(config)#interface linecard 0
SCE(config if)#no accelerate-packet-drops
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard accelerate-packet-drops	

access-class

Restricts Telnet server access to those addresses listed in the specified access list. Use the **no** form of this command to either remove a specified ACL or to set the Telnet server to accept access from any IP address.

access-class *number* in

no access-class [*number*] in

Syntax Description

number	An access-list number (1–99).

Defaults

By default, no access list is configured (Telnet access is available from any IP address).

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#line vty 0
SCE(config-line)#access-class 1 in
SCE(config-line)#
```

EXAMPLE 2

The following example removes an access class for Telnet lines.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#line vty 0
SCE(config-line)#access-class 1 in
SCE(config-line)#
```

Related Commands

Command	Description
access-list	
show access-lists	

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

number	An access-list number (1–99).
permission	Indicates whether the IP address should be allowed or denied access permission as described in the Valid Permission Values table in the Usage Guidelines.
address	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 the following:

- A permit/deny field
- An IP address
- An optional wildcard “mask” defining an IP address range

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

deny	Deny access to list member
permit	Permit access to list member.
any	All IP addresses are matched by this entry. This is equivalent to specifying the address 0.0.0.0 255.255.255.255
ip-address	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 examples illustrate the use of this command.

EXAMPLE 1

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#access-list 1 permit 10.1.1.0 0.0.0.255
SCE(config)#access-list 1 deny any
SCE(config)#
```

EXAMPLE 2

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>enable 10
Password:<cisco>
SCE#config
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

Command	Description
access-class	
snmp-server community	
show access-lists	

accurate-accounting

Controls whether the flow residual mechanism for Accurate Accounting is enabled or disabled. Use the **no** form of this command to disable flow residual mechanism for Accurate Accounting.

accurate-accounting

no accurate-accounting

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to enable the flow residual mechanism for Accurate Accounting.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>accurate-accounting
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard accurate-accounting	

active-port

Specifies which management port is currently active.

active-port

Syntax Description

This command has no arguments or keywords.

Defaults

Default Mng port is 0/1.

Command Modes

Mng Interface Configuration

Usage Guidelines

The command must be executed from the Mng interfacethat is to be defined as the active port, as follows:

- Use the **interface mng** command, specifying the desired port number (0/1 or 0/2), to enter the proper command mode.
- Execute the active-port command.

The use of this command varies slightly depending on whether the management interface is configured as a redundant interface (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>enable 10
Password:<cisco>
SCE#config
SCE (config)#interface mng 0/2
SCE (config-if)#active-port
SCE(config-if)#
```

Related Commands

Command	Description

aggregative-global-controller

Enables or configures aggregative global controllers. Use the**no** form of the command to disable aggregative global controllers.

aggregative-global-controllers

aggregative-global-controller {network | subscriber} ***agc-index*** **[(bandwidth** ***bandwidth*** **) | (link** ***link-number*** **)]**

no aggregative-global-controllers

Syntax Description

agc-index	The ID number of the aggregative global controller.
bandwidth	The bandwidth that will be enforced in Kbps.
link-number	The number of the link that the specified aggregative-global-controller will control.

Defaults

By default, aggregative-global-controller mode is disabled.

Command Modes

Linecard InterfaceConfiguration

Usage Guidelines

Use this command as follows:

- To enable the aggregative global controllers — **aggregative-global-controllers**
- To disable the aggregative global controllers — **no aggregative-global-controllers**
- To configure a specific aggregative global controller for a specific side (network or subscriber) — **aggregative-global-controller {network | subscriber}** *agc-index* **[(bandwidth** ***bandwidth*** **) | (link** ***link-number*** **)]**

Authorization: root

Examples

The following example shows how to first enable the aggregative global controllers and then configure the aggregative global controller for the network side.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#>interface linecard 0
SCE(config if)#>aggregative-global-controllers
SCE(config if)#>aggregative-global-controller network 1 bandwidth
 10000
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard aggregative-global-controller	

analysis layer

Configures the lowest layer for protocol analysis.

analysis layer {application | transport}

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Specify the appropriate layer:

- **application** — Analyze protocol information from application layers only
- **transport** — Analyze protocol information from transport layer and up

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>analysis layer application
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard analysis layer	

application

Loads the specified application. Use the **no** form of the command to unload the currently loaded application.

application ***file-name*** **[capacity-option** ***capacity-option-name*** **]**

no application

Syntax Description

file-name	The name of the SLI file.
capacity-option-name	Non-default capacity option.

Defaults

By default, the default capacity option defined in the SLI file is used to indicate the capacity (maximum number of subscribers).

Command Modes

Interface Linecard Configuration

Usage Guidelines

When loading an application, the maximum number of subscribers supported by the SCE platform must be specified using one of the following options:

- **capacity-option** — Specifies the name of a pre-defined capacity option. The maximum number of subscribers is the value defined in the SLI file for that capacity-option.

  The specified capacity-option name must be found in the SLI file.

  Use the **show applications file capacity-options** command to find out what capacity options are available in the SLI file.
- Not specifying anything — The maximum number of subscribers is determined by the SLI file default capacity-option.

When an application is loaded, traffic opens new flows, which are serviced. When the application is unloaded, all flows are closed immediately and no service is given; the SCE platform then functions as a wire.

Authorization: root

Examples

The following example shows how to load an application (application.sli) with the capacity option SubscriberlessSCE.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>application application.sli capacity-option SubscriberlessSCE
SCE(config if)#>
```

Related Commands

Command	Description
show applications file capacity-options	
capacity-option name	
show interface linecard application	

application replace

Replaces the currently loaded application.

application ***file-name*** **replace**

Syntax Description

file-name	The name of the SLI file.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

The currently loaded application is replaced by the specified application with no service downtime (hitless upgrade).

Note that support for the replacement operation can be disabled. Use the **no replace support** command (see **replace support**).

The following issues must be addressed before the actual replacement is executed:

- application compatibility
- limiting the replacement process

Application Compatibility

The new application must satisfy a few conditions with respect to the old application:

- The applications must be compatible, as signed by the SML compiler.

  Use the **application slot replace verify file** command to verify that the files are compatible.
- The new application memory requirements cannot exceed those of the old application.

  Use the **replace spare-memory** command to configure additional memory.

  Use the **show applications slot replace** command to see memory configuration for the current application.

Limiting the Replacement Process

When the **application replace** command is executed, the new application is loaded and new flows are serviced by the new application. However, the existing flows are still being serviced by the old application. Until all old flows die, the application replace is considered to be ‘in progress’, and no new application replace can begin.

In some cases, a small number of old flows may remain for some time. In order to limit the application replace process, the following criteria can be configured that trigger the explicit killing of all flows still executing on the old application:

- Time — All remaining old flows are killed after a specified amount of time has elapsed since the process started.
- Number of old flows — All remaining old flows are killed when the number of old flows goes below a specified threshold.

Use the **replace completion** command to configure these limits.

In addition, all remaining old flows can be manually killed at any time by using the **application slot replace force completion** command.

Monitoring the Replacement

The following stages can be observed when viewing the application replace status:

1. No application replace in progress, system is ready to start a new upgrade
2. Application replace in progress, completion criteria not yet met
3. Application replace in progress, one of the completion criteria has been satisfied, system is now killing all old flows.

   When the application replace is complete and no old flows exist, the status reverts to stage #1.

Use the **show applications slot replace** command to monitor the application replacement operation.

Authorization: root

Examples

The following example shows how to use the application replace functionality, including the following:

- Configuring flow time limit for kill all remaining old flows
- Verifying application compatibility
- Executing the replace
- Monitoring the replace
- Manually killing all old flows when the status shows that almost no old flows remain even though the time limit has not been reached

```
SCE>enable 15
Password:cisco
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>replace completion time 30
SCE(config if)#>do application slot 0 replace verify file newapp.sli
Replace of current application with '/tffs0/NEWAPP.SLI' is possible.
It would be an upgrade
SCE(config if)#>application replace
SCE(config if)#>exit
SCE(config)#>exit
SCE#>show applications slot replace
Application loaded, ready for replace.
Replace support is enabled (Effective on next application load).
Configured completion criterions:
Time criterion: 30 minutes.
Num-flows criterion: 0 flows.
This means that the replace process will end when no more old flows exist, or 30
minutes pass since the replace process began, whichever occurs first.
Configured spare memory parameters:
code: 3145728 bytes
global: 1000 bytes
subscriber: 0 bytes
Current spare memory sizes:
code: 5594668 bytes used out of 9970176.
global: 12961230 bytes used out of 12961280.
subscriber: 2426 bytes used out of 2426.
SCE#>application slot 0 replace force completion
SCE#>
```

Related Commands

Command	Description
application slot replace verify file	
application slot replace force completion	
replace completion	
replace spare-memory	
replace support	
show applications slot replace	
application	

application slot replace force completion

Forces the current application replace process to complete and immediately start finalization (killing all old flows).

application slot *slot-number* replace force completion

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 illustrates how to force the application replace operation to complete immediately.

```
SCE>enable 10
Password:<cisco>
SCE#application slot 0 replace force completion
SCE#
```

application slot replace verify file

Evaluates the specified application file to see whether it can replace the currently loaded application.

application slot ***slot-number*** **replace verify file** ***filename***

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
filename	The name of the new SLI file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The new application must satisfy the following conditions with respect to the old application:

- The applications must be compatible, as signed by the SML compiler.

  The following SCOS requirements are assumed to be fulfilled in addition to the applications being verified as compatible. The behaviour of the SCOS when these assumptions are false is undefined.

  - All tunables, viewables, lookup-tables, handlers, accumulators, flow-filter rules and traffic-controllers are identical in both applications.
  - RDR tags can be added or removed in the new application, but tags that are used in both applications must have the same signature (parameter types, etc).
- The new application party context memory size and graph memory size must not be larger than the respective pre-allocated sizes of these memory segments as used by the old application.

  Use the **replace spare-memory** command to configure memory.

  Use the **show applications slot replace** command to see memory configuration for the current application.

Note that if an application was compiled to be compatible with an existing application, both an upgrade (transition from current application to new application) and a downgrade (transition from new application back to previous) are supported. Based on the SLI signatures, the SCOS can tell which application was compiled later; hence it knows whether the replace operation is an upgrade or a downgrade.

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>application slot 0 replace verify file newapp.sli
Replace of current application with '/tffs0/app/NEWAPP.SLI' is possible.
It would be an samegrade
SCE#>
```

Related Commands

Command	Description
application replace	
application	

asymmetric-L2-support

Configures the system to treat flows as having asymmetric layer 2 characteristics (including Ethernet, VLAN, MPLS, and L2TP), for the purpose of packet injection.

Use the **no** form of the command to disable asymmetric L2 support.

asymmetric-L2-support

no asymmetric-L2-support

Syntax Description

This command has no arguments or keywords.

Defaults

By default, asymmetric layer 2 support is disabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

You should enable asymmetric layer 2 support in cases where the following conditions apply for any flows:

- Each direction of the flow has a different pair of MAC addresses
- The routers do not accept packets with the MAC address of the other link

Note 'Asymmetric routing topology' support and 'asymmetric tunneling support' are two separate features. Asymmetric routing topology refers to topologies where the SCE platform might see some flows only in one direction (upstream/downstream). Asymmetric tunneling support (asymmetric L2 support) refers to the ability to support topologies where the SCE platform sees both directions of all flows, but some of the flows may have different layer 2 characteristics (like MAC addresses, VLAN tags, MPLS labels and L2TP headers), which the SCE platform must specifically take into account when injecting packets into the traffic (such as in block and redirect operations). Note as well, that in order to support asymmetric layer 2, the SCE platform switches to asymmetric flow open mode, which incurs a certain performance penalty. This is NOT the case for asymmetric routing topology.

Authorization: admin

Examples

The following example shows how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)# asymmetric-L2-support
```

Related Commands

Command	Description
show inteface linecard `asymmetric-L2-support`	

asymmetric-routing-topology enabled

Enables asymmetric routing topology. Use the**no** or **default** form of the command to disable asymmetric routing topology.

[no | default] asymmetric-routing-topology enabled

Syntax Description

This command has no arguments or keywords.

Defaults

By default, asymmetric routing topology is disabled.

Command Modes

Linecard Interface Configuration

Usage Guidelines

The asymmetric routing option enables the SCE platform to handle unidirectional traffic and allows SCA BB to classify traffic based on a single direction and to apply basic reporting and global control features to unidirectional traffic.

Note that asymmetric routing cannot be used with the following Service Control capabilities:

- Subscriber redirect
- Subscriber notification
- Any kind of subscriber integration, including MPLS VPN. Use subscriber-less mode or anonymous subscriber mode instead.
- Classical open flow mode, including the following:
  - Explicit configuration of flow-open-mode classical
  - VAS traffic forwarding enabled
  - Analysis layer transport enabled
  - 'no TCP bypass-establishment' mode enabled
  - A traffic rule is configured for certain flows to use the classical open flow mode

Note The SCE platform identifies unidirectional flows by default and regardless of this mode. Enabling this mode is essential, however, for the control and reporting of the unidirectional flows by the SCA BB application. Therefore, this mode is used explicitly by the SCA BB GUI when the appropriate policy is applied.

Authorization: root

Examples

The following example illustrates how enable asymmetric routing.

```
SCE>enable 15
Password:cisco
SCE#>config
```

```
SCE(config)#>interface linecard 0
SCE(config if)#>asymmetric-routing-topology enabled
```

Related Commands

Command	Description
show interface line-card asymmetric-routing-topology	

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]*** **[suspected-flows-ratio** ***suspected-flows-ratio]*** **[notify-subscriber | dont-notify-subscriber] [alarm |noalarm]**

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

Syntax Description

protocol	TCP, UDP, IMCP, other
attack-direction	attack-source, attack-destination, both
side	subscriber, network, both
action	report, block
open-flows	Threshold for concurrently open flows (new open flows per second).
ddos-suspected-flows	Threshold for DDoS-suspected flows (new suspected flows per second).
suspected-flows-ratio	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

The following arguments must always be specified:

- protocol
- attack-direction
- side

The following arguments are optional:

- action
- open-flows
- ddos-suspected-flows
- suspected-flows-ratio

Use the optional keywords as follows:

- 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.

Use the **attack-detector <number>**command to configure a specific attack detector.

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#attack-detector default protocol TCP attack-direction attack-source side
both action report open-flows 500 ddos-suspected-flows 75 suspected-flows-ratio 50
SCE(config if)#
```

EXAMPLE 2

The following example enables subscriber notification for the specified default attack detector.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#attack-detector default protocol TCP attack-direction attack-source side
both notify-subscriber
SCE(config if)#
```

Related Commands

Command	Description
attack-detector <number>	
attack-filter subscriber-notificatio n ports	
show interface LineCard attack-detector	

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

Use the following commands to define the attack detector and the ACL:

- **attack-detector**
- **acccess-lis**t

Authorization: admin

Examples

The following example enables attack detector number "2", and assigns ACL "8".

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#attack-detector 2 access-list 8
SCE(config if)#
```

Related Commands

Command	Description
access-list	
attack-detector <number>	
show interface LineCard attack-detector	
show access-lists	

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** ***destination port*** **])|ICMP|other|all) attack-direction** ***attack-direction*** **side** ***side*** **[action** ***action]*** **[open-flows** ***open-flows*** **] [ddos-suspected-flows** ***ddos-suspected-flows*** **] [suspected-flows-ratio** ***suspected-flows-ratio*** **] [notify-subscriber|dont-notify-subscriber] [alarm|no-alarm]**

no attack-detector ***number***

attack-detector default protocol (((TCP|UDP) [dest-port ***destination port*** **])|ICMP|other|all) attack-direction** ***attack-direction*** **side** ***side*** **[action** ***action]*** **[open-flows** ***open-flows*** **] [ddos-suspected-flows** ***ddos-suspected-flows*** **] [suspected-flows-ratio** ***suspected-flows-ratio*** **] [notify-subscriber|dont-notify-subscriber] [alarm|no-alarm]**

no attack-detector default protocol (((TCP|UDP) [dest-port ***destination port*** **])|ICMP|other|all) attack-direction** ***attack-direction*** **side** ***side***

default attack-detector {all |all-numbered}

default attack-detector number protocol (((all | IMCP | other | TCP | UDP) [dest-port ***destination port*** **attack-direction** ***attack-direction*** **side** ***side***

Syntax Description

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

The following arguments must always be specified:

- protocol
- attack-direction
- side

The following arguments are optional:

- action
- open-flows
- ddos-suspected-flows
- suspected-flows-ratio

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.

If the selected protocol is either TCP or UDP, specify whether the destination port is specific, not specific, or both. If the destination port or ports are specific, the specific destination ports are configured using the attack-detector, page 2-35command.

Use the attack-detector, page 2-35command to enable a configured attack detector.

Use the attack-detector default, page 2-33command to configure a default attack detector.

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
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
SCE(config if)#
```

EXAMPLE 2

The following example deletes attack detector number "2".

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#no attack-detector 2
SCE(config if)#
```

EXAMPLE 3

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#attack-detector 2 protocol UDP dest-port not-specific attack-direction
single-side-destination side both dont-notify- subscriber
SCE(config if)#
```

Related Commands

Command	Description
attack-detector	
attack-detector TCP-port-list|UDP-port-list	
attack-filter subscriber-notification ports	
attack-detector default	
show interface LineCard attack-detector	

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
port1, port2	List of up to 15 specific port numbers.

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 (port-based). Use this command to configure 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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#attack-detector 10 TCP-port-list 100 101 102 103
SCE(config if)#
```

Related Commands

Command	Description
attack-detector <number>	
attack-filter (LineCard Interface Configuration)	

attack-filter

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 *destination port*])|ICMP|other|all) attack-direction *attack-direction*

no attack-filter protocol (((TCP|UDP) [dest-port *destination port*])|ICMP|other|all) attack-direction *attack-direction*

Syntax Description

protocol	TCP, UDP, IMCP, other
destination port	{TCP and UDP protocols only): Defines whether the default attack detector applies to specific (port-based) or not specific (port-less) detections. specific, not-specific, both
attack-direction	single-side-destination, single-side-both, dual-sided, all

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 and port-less

Command Modes

LineCard Interface Configuration

Usage Guidelines

Specific attack filtering is configured in two steps:

- Enabling specific IP filtering for the particular attack type (using this command).
- Configuring an attack detector for the relevant attack type (using the attack-detector <number>, page 2-36command). Each attack detector specifies the thresholds that define an attack and the action to be taken when an attack is detected.

In addition, the user can manually override the configured attack detectors to either force or prevent attack filtering in a particular situation (using the **attack filter force filter | don't-filter** command).

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.

If the selected protocol is either TCP or UDP, specify whether the destination port is specific (port-based), not specific (port-less), or both. If the destination port or ports are specific, the specific destination ports are configured using the attack-detector TCP-port-list|UDP-port-list, page 2-39command.

Authorization: admin

Examples

The following examples illustrate the use of this command.

EXAMPLE 1

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#attack-filter protocol TCP dest-port specific attack-direction dual-sided
SCE(config if)#
```

EXAMPLE 2

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)# attack-filter protocol ICMP attack-direction single-side-source
SCE(config if)#
```

EXAMPLE 3

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface LineCard 0
SCE(config if)#no attack-filter protocol other attack-direction all
SCE(config if)#
```

Related Commands

Command	Description
attack-detector TCP-port-list|UDP-port-list	
attack-detector <number>	
show interface LineCard attack-filter	

attack-filter dont-filter | force-filter

This 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. The**force-filter** keyword 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 force-filter protocol ((TCP|UDP) [dest-port (*port-number* |not-specific)]|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) ip *ip-address*)|(dual-sided source-ip *ip-address* destination-ip *ip-address*)) side *side*

attack-filter dont-filter protocol ((TCP|UDP) [dest-port (*port-number* |not-specific)]|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) ip *ip-address*)|(dual-sided source-ip *ip-address* destination-ip *ip-address*)) side *side*

no attack-filter dont-filter protocol ((TCP|UDP) [dest-port (*port-number* |not-specific)]|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) ip *ip-address*)|(dual-sided source-ip *ip-address* destination-ip *ip-address*)) side *side*

no attack-filter force-filter protocol ((TCP|UDP) [dest-port (*port-number* |not-specific)]|ICMP|other) attack-direction (((single-side-source|single-side-destination|single-side-both) ip*ip-address*)|(dual-sided source-ip *ip-address* destination-ip *ip-address*)) side *side*

no attack-filter force-filter all

no attack-filter dont-filter all

Syntax Description

protocol	TCP, UDP, ICMP, or Other
destination port	(TCP and UDP protocols only): Defines whether specific IP detection is forced or prevented for the specified port number or is port-less (non-specific). *port-number,* not-specific
attack direction	Defines whether specific IP detection is forced or prevented for single-sided or dual-sided attacks. • Single-sided: specify the direction (single-side-source, single-side-destination, single-side-both) and the IP address. • Dual-sided: Specify **'dual-sided'** and both the source and the destination IP addresses.

ip-address	IP address from which traffic will not be filtered. • For single-sided filtering, only one IP address is specified. • For dual-sided filtering, both a source IP address and a destination IP address are specified.
side	subscriber, network, both

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

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 protocol, direction and specified IP address
- Force filtering of an attack related to a protocol, direction and 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 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**).

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#attack-filter dont-filter protocol other attack-direction
single-side-source ip 10.10.10.10 side both
SCE(config if)#
```

EXAMPLE 2:

The following example restores all attack filtering.

```
SCE>enable 10
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no attack-filter dont-filter all
SCE(config if)#
Password:<cisco>
```

EXAMPLE 3:

The following example forces attack filtering.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#attack-filter force-filter protocol TCP dest-port not-specific
attack-direction dual-sided source-ip 10.10.10.10 destination-ip 20.20.20.20 side both
SCE(config if)#
```

EXAMPLE 4:

The following example stops all forced attack filtering.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no attack-filter force-filter all
SCE#
```

Related Commands

Command	Description
attack-filter	

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

port	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

Use this command to configure the port to be used for subscriber notification as configured using the **attack-filter** and **attack-detector <number>**commands.

Authorization: admin

Examples

The following example specifies port 100 as the subscriber notification port.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#attack-filter subscriber-notification ports 100
SCE(config if)#
```

Related Commands

Command	Description
attack-detector default	
attack-detector <number>	
show interface linecard attack-filter	

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**)

Authorization: admin

Examples

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface Mng 0/1
SCE(config if)#no auto-fail-over
SCE(config if)#
```

Related Commands

Command	Description
active-port	

auto-negotiate

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

By default, auto-negotiation is:

- On for inline connection mode
- Off for receive-only 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 (receive-only connection mode).

Authorization: admin

Examples

The following example configures GigabitEthernet line interface #1 (0/1) to perform no auto-negotiation.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface GigabitEthernet 0/1
SCE(config if)#no auto-negotiate
SCE(config if)#
```

Related Commands

Command	Description
show interface GigabitEthernet	

bandwidth

Sets Ethernet shaping for the GigabitEthernet line interfaces.

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

GigabitEthernet Interface Configuration

Usage Guidelines

This command is valid for a specified GigabitEthernet line interface only. It must be executed explicitly for each interface.

Authorization: admin

Examples

The following example sets bandwidth and burst size for a Gigabit Ethernet line interface (0/2) of a SCE 2000 4xGBE or SCE 1000 2xGBE.

```
SCEconfig
SCE(config)#interface GigabitEthernet 0/2
SCE(config-if)#bandwidth 100000 burstsize 5000
SCE(config-if)#
```

Related Commands

Command	Description
interface gigabitethernet	
queue	

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>enable 10
Password:<cisco>
SCE#no blink slot 0
SCE#
```

Related Commands

Command	Description
show blink	

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

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

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#boot system ftp://user:1234@10.10.10.10/downloads/SENum.pkg.pkg
Verifying package file…
Package file verified OK.
SCE(config)#do copy running-config startup-config
Backing –up configuration file…
Writing configuration file…
Extracting new system image…
Extracted OK.
```

Related Commands

Command	Description
copy running-config startup-config	

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

hh:mm:ss	Current local time in hours in 24-hour format, minutes and seconds (HH:MM:SS).
day	Current day (date) in the month.
month	Current month (by three-letter abbreviated name).
year	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.

Authorization: admin

Examples

The following example sets the calendar to 20 minutes past 10 AM, January 13, 2006, synchronizes the real-time clock to the calendar time, and displays the result.

```
SCE>enable 10
Password:<cisco>
SCE#calendar set 10:20:00 13 jan 2006
SCE#clock read-calendar
SCE#show calendar
10:20:03 UTC THU January 13 2006
SCE#show clock
10:20:05 UTC THU January 13 2006
SCE#
```

Related Commands

Command	Description
clock read-calendar	
clock set	
clock update-calendar	

capacity-option

Configures the SCE platform to use a specific capacity option.

capacity-option ***name*** **name**

no capacity-option

default capacity-option

Syntax Description

name	The name of the capacity option to use.

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Usage Guidelines

The purpose of the capacity option feature is to provide a choice of capacity options in the SML application, so that the user can select the proper one to be used by the SCE platform when loading the application. The use of the capacity option is application dependent; some applications will have these options while others may not.

Each capacity option is identified by a name. The SLI file always contains a default capacity option, which is used by the platform when no specific capacity option is selected. Use the **show applications file capacity-options** command to find out what capacity options are available.

The platform can be configured to use either the default capacity option or a specified capacity option. When loading an application, the configured capacity option is used by the SCE platform, if such an option is defined in the application file. If no such option is found, the application cannot be loaded.

Once the platform is configured to use a specific capacity option, it remembers this configuration via the application configuration file, (running-config-application).

Note This set of commands is used by the specific pqi file that is used at the ADMIN level for application installation. These commands allow the user to leverage additional capacity options that are not exposed by the pqi.

Do not use this command when an application is loaded.

Use either the **no** or **default** form of the command to configure the SCE platform to use the default capacity option.

Authorization: root

Examples

The following example configures the SCE platform to use the EngageDefaultSE1000 capacity option.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>capacity-option name EngageDefaultSE1000
SCE(config if)#>
```

Related Commands

Command	Description
show applications capacity-option	
show applications file capacity-options	
application	

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 (root directory) and then changes the directory to the log directory located under the root directory.

```
SCE>enable 10
Password:<cisco>
SCE>enable 10
SCE#pwd
tffs0
SCE#cd log
SCE#pwd
tffs0:log
SCE#
```

Related Commands

Command	Description
pwd	
mkdir	

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>enable 10
Password:<cisco>
SCE#clear arp-cache
SCE#
```

Related Commands

Command	Description
clear interface linecard mac-resolver arp-cache	

clear interface linecard counters

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>enable 10
Password:<cisco>
SCE#clear interface linecard 0 counters
SCE#
```

Related Commands

Command	Description
show interface linecard counters	

clear interface linecard asymmetric-routing-topology counters

Clears counters related to asymmetric routing topology.

clear interface linecard *slot-number* asymmetric-routing-topology 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

The system calculates the ratio of TCP unidirectional flows to total TCP flows per traffic processor for a requested period of time. Use this command to reset the counters used as a basis for these flow-ratio statistics.

Authorization: root

Examples

The following example show how to clear the asymmetric routing topology counters.

```
SCE>enable 15
Password:<cisco>
SCE#>clear interface linecard 0 asymmetric-routing-topology counters
SCE#>
```

Related Commands

Command	Description
show interface line-card asymmetric-routing-topology	

clear interface linecard flow-filter

Clears all flow filter rules for the specified partition.

clear interface linecard *slot-number* flow-filter partition name *name*

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
name	Name of the partition for which to clear the flow filter rules

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>clear interface linecard 0 flow-filter partition name partition_1
SCE#>
```

Related Commands

Command	Description
show interface linecard flow-filter	
flow-filter	

clear interface linecard mac-resolver arp-cache

Clears all the MAC addresses in the MAC resolver database.

clear interface linecard *slot-number* mac-resolver arp-cache

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 use this command.

```
SCE>enable 10
Password:<cisco>
SCE#clear interface linecard 0 mac-resolver arp-cache
SCE#
```

Related Commands

Command	Description
clear arp-cache	
mac-resolver arp	
show interface linecard mac-resolver arp	

clear interface linecard mpls vpn

Clears the specified MPLS VPN counter: bypassed VPNs and non-VPN-mappings

clear interface linecard *slot-number* mpls vpn [bypassed-vpns][non-vpn-mappings]

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
bypassed-VPNs	Displays all currently bypassed VPNs, grouped by downstream label
non-VPN-mappings	Displays the mappings of upstream labels that belong to non-VPN flows

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example clears the MPLS VPN counter for non-VPN-mappings.

```
SCE>enable 10
Password:<cisco>
SCE#clear interface linecard 0 mpls vpn non-vpn-mappings
SCE#
```

Related Commands

Command	Description
show interface linecard mpls	
no mpls vpn pe-database	

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>enable 10
Password:<cisco>
SCE#clear interface linecard 0 subscriber anonymous all
SCE#
```

Related Commands

Command	Description
no subscriber	
no subscriber anonymous-group	
show interface linecard subscriber anonymous	

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>enable 10
Password:<cisco>
SCE#clear interface linecard 0 subscriber db counters
SCE#
```

Related Commands

Command	Description
show interface linecard subscriber db counters	

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>enable 10
Password:<cisco>
SCE#clear interface linecard 0 traffic-counter name counter1
SCE#
```

Related Commands

Command	Description
traffic-counter	
show interface linecard traffic-counter	

clear interface linecard vas-traffic-forwarding vas 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 for which to 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.

```
SCE>enable 10
Password:<cisco>
SCE#clear interface linecard 0 vas-traffic-forwarding vas all counters health-check
SCE#
```

Related Commands

Command	Description
vas-traffic-forwarding vas server-id health-check	
show interface linecard vas-traffic-forwarding	

clear interface linecard vpn

Removes VLAN VPNs that were created automatically by the SCE platform.

clear interface linecard *slot-number* vpn automatic

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 illustrates the use of this command.

```
SCE>enable 10
Password:<cisco>
SCE#clear interface linecard 0 vpn automatic
SCE#
```

Related Commands

Command	Description

clear interface linecard vpn (ROOT option)

Removes VPNs and their subscriber mappings.

clear interface linecard ***slot-number*** **vpn [automatic] 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

The **all** option of this command is available at the root authorization level only.

This command removes all existing VPNs, including those that currently have subscriber mappings.

Use the **automatic** keyword to remove all VLAN VPNs that were created automatically by the SCE platform. (The admin-level command without the **all** option does not remove VPNs that have subscriber mappings).

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to remove all VPNs.

```
SCE>enable 15
Password:<cisco>
SCE#>clear interface linecard 0 vpn all
SCE#>
```

EXAMPLE 2

The following example illustrates how to remove all automatically created VLAN VPNs.

```
SCE>enable 15
Password:<cisco>
SCE#>clear interface linecard 0 vpn automatic all
SCE#>
```

Related Commands

Command	Description
clear interface linecard vpn	

clear interface linecard vpn name upstream-mpls all

Removes all learned upstream labels of a specified VPN.

clear interface linecard *slot-number* vpn name *vpn-name* upstream-mpls all

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
vpn-name	The name of the VPN for which to clear the learned upstream labels.

Defaults

This command has no default settings.

Command Modes

This command has no default settings.

Usage Guidelines

Authorization: admin

Examples

The following example clears all learned upstream labels for the specified VPN.

```
SCE>enable 10
Password:<cisco>
SCE#clear interface linecard 0 vpn name vpn1 upstream-mpls all
SCE#
```

Related Commands

Command	Description

clear interface range

Clears all the specified interfaces.

clear interface range ***gigabitethernet interface-range***

Syntax Description

interface-range	Specify the range of ports in the format '*port1-port2*', where the overall range of possible port numbers is as follows: • SCE 2000: 1-4 • SCE 1000: 1-2

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The **clear interface range** command allows you to clear a group of interfaces with one command, with the limitation that all the interfaces in the group must be of the same physical and logical type.

Authorization: admin

Examples

The following example clears all the traffic interfaces in the SCE platform.

```
SCE>enable 10
Password:<cisco>
SCE#clear interface range gigabitethernet 1-4
```

Related CommandsE

Command	Description
show interface linecard counters	

clear logger

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

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 user 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 in 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).

- Use the **counters** keyword to clear the counters of the SCE platform logger (user log files). These counters keep track of the number of info, warning, error and fatal messages.
- Use the **nv-counters** keyword to clear 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.

Authorization: admin

Examples

EXAMPLE 1:

The following example clears the SCE platform user log file.

```
SCE>enable 10
Password:<cisco>
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>enable 10
Password:<cisco>
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>enable 10
Password:<cisco>
SCE#clear logger device user-file-log nv-counters
Are you sure?Y
SCE#
```

Related Commands

Command	Description
show logger device	
show log	

clear logger counters

Clears counters related to the logger. You can use the**show logger counters** command to view the counters before clearing them.

clear logger {counters | counters-all}

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **counters** keyword to clear all counters related to the logger engine.

Use the **counters-all** keyword to clear all counters, both for the logger engine and all logger devices (such as debug log, user log, etc.).

Authorization: root

Examples

The following example illustrates the use of this command. Note that the request for confirmation "Are you sure?" does not actually appear twice. It is listed in the example twice to show that you must type "y" over the "N" that appears in order to confirm the clear command.

```
SCE>enable 15
Password:<cisco>
SCE#>clear logger counters
Are you sure? N
Are you sure? y (type "y" over the "N" in order to confirm)
SCE#>
```

Related Commands

Command	Description
show logger	
clear logger device counters	
clear logger nv-counters	

clear logger device

Clears the specified logger device. This means that the current contents of the specified logger device will be erased and the log will be empty.

clear logger device {debug-file-log | line-attack-file-log | sce-agent-debug-log | statistics-file-log | statistics-archive-file-log | user-file-log}

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Available logger devices are:

- Debug-File-Log
- SCE-agent-Debug-Log,
- Statistics-Archive-File-Log
- Statistics-File-Log
- User-File-Log (Available at Admin authorization level. See **clear logger**
- Line-Attack-File-Log (Available at Admin authorization level. See **clear logger**

Authorization: root

Examples

The following example illustrates how to clear the debug log file. After executing this command, the contents of the debug log file will be deleted and the debug log will be empty.

Note that the request for confirmation "Are you sure?" does not actually appear twice. It is listed in the example twice to show that you must type "y" over the "N" that appears in order to confirm the clear command.

```
SCE>enable 15
Password:<cisco>
SCE#>clear logger device debug-file-log
Are you sure? N
Are you sure? y (type "y" over the "N" in order to confirm)
SCE#>
```

Related Commands

Command	Description
clear logger device counters	

clear logger device counters

Clears the counters for the specified logger device.

clear logger device {debug-file-log | line-attack-file-log | sce-agent-debug-log | statistics-file-log | statistics-archive-file-log | user-file-log} counters

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Available logger devices are:

- Debug-File-Log
- SCE-agent-Debug-Log,
- Statistics-Archive-File-Log
- Statistics-File-Log
- User-File-Log (Available at Admin authorization level. See **clear logger**
- Line-Attack-File-Log (Available at Admin authorization level. See **clear logger**

Authorization: root

Examples

The following example illustrates how to clear the counters for the debug log file. Note that the request for confirmation "Are you sure?" does not actually appear twice. It is listed in the example twice to show that you must type "y" over the "N" that appears in order to confirm the clear command.

```
SCE>enable 15
Password:<cisco>
SCE#>clear logger device debug-file-log counters
Are you sure? N
Are you sure? y (type "y" over the "N" in order to confirm)
SCE#>
```

Related Commands

Command	Description
clear logger counters	
clear logger device	
clear logger nv-counters	

clear logger nv-counters

Clears all non-volatile counters related to the logger.

clear logger {nv-counters | nv-counters-all}

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Use the **nv-counters** keyword to clear all non-volatile counters related to the logger engine.

Use the **nv-counters-all** keyword to clear all non-volatile counters, both for the logger engine and all logger devices.

Authorization: root

Examples

The following example illustrates the use of this command. Note that the request for confirmation "Are you sure?" does not actually appear twice. It is listed in the example twice to show that you must type "y" over the "N" that appears in order to confirm the clear command.

```
SCE>enable 15
Password:<cisco>
SCE#>clear logger nv-counters
Are you sure? N
Are you sure? y (type "y" over the "N" in order to confirm)
SCE#>
```

Related Commands

Command	Description
clear logger counters	
clear logger device counters	
clear logger	

clear management-agent notifications counters

Clears the counters for the number of notifications sent to the management agent

clear management-agent notifications 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 clears the management agent notifications counters.

```
SCE>enable 10
Password:<cisco>
SCE#clear management-agent notifications counters
SCE#
```

Related Commands

Command	Description

clear rdr-formatter

Clears the RDR formatter counters and statistics.

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>enable 10
Password:<cisco>
SCE#clear rdr-formatter
SCE#
```

Related Commands

Command	Description
show rdr-formatter counters	

clear rdr-server

Clears the RDR server counters.

clear rdr-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: root

Examples

The following example illustrates the use of this command. Note that there is no request for confirmation.

```
SCE>enable 15
Password:<cisco>
SCE#>clear rdr-server
SCE#>
```

Related Commands

Command	Description
show rdr-server	

clear scmp name counters

Clears the counters for the specified SCMP peer device.

clear scmp name *name* counters

Syntax Description

name	Name of the SCMP peer device.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example clears the counters for the SCMP peer device named device_1.

```
SCE>enable 10
Password:<cisco>
SCE#clear scmp name device_1 counters
SCE#
```

Related Commands

Command	Description
show scmp	

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>enable 10
Password:<cisco>
SCE#clock read-calendar
SCE#
```

Related Commands

Command	Description
calendar set	
clock update-calendar	
show calendar	

clock set

Manually sets the system clock.

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

Syntax Description

hh:mm:ss	Current local time in hours in 24-hour format, minutes and seconds (HH:MM:SS).
day	Current day (date) in the month.
month	Current month (by three-letter abbreviated name).
year	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, January 13, 2006.

```
SCE>enable 10
Password:<cisco>
SCE#clock set 22:20:00 13 jan 2006
SCE#clock update-calendar
SCE#show clock
22:21:10 UTC THU January 13 2006
SCE#show calendar
22:21:18 UTC THU January 13 2006
SCE#
```

Related Commands

Command	Description
clock update-calendar	
show calendar	
show clock	

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 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

Syntax Description

zone	The code for the time zone for daylight savings.
week1/week2	The week of the month on which daylight savings begins (week1) and ends (week2). 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
day1/day2	The day of the week on which daylight savings begins (day1) and ends (day2). For recurrent configuration: day is a day of the week, such as Sunday. Use the keywords **first/last** 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 = second Sunday, day2 = first Sunday
month1/month2	The month in which daylight savings begins (month1) and ends (ends2). Default: month1 = March, month2 = November
year1/year2	The year in which daylight savings begins (month1) and ends (ends2). For non -recurring configuration only. Default = not used
time1/time2	The time of day (24-hour clock) at which daylight savings begins (time1) and ends (time2). Required for all configurations. Default: time1/time2 = 2:00
offset	The difference in minutes between standard time and daylight savings time. Default = 60

Defaults

recurring, offset = 60 minutes

By default, the following recurrent time changes are configured:

- Daylight savings time begins: 2:00 (AM) on the second Sunday of March.
- Daylight savings time ends: 2:00 (AM) on the first Sunday of November.

Command Modes

Global Configuration

Usage Guidelines

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 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 second Sunday of March.
- Daylight savings time ends: 2:00 (AM) on the first Sunday of November.

Use the **recurring** keyword if daylight savings time always begins and ends on the same day every year.

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 this 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>enable 10
Password:<cisco>
SCE#config
SCE(config)#clock summer-time DST
recurring last Sunday March 00:00 4 Saturday November 23:59
SCE(config)#
```

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, 2007.
- Daylight savings time ends: 23:59 October 23, 2007.
- Offset = 1 hour (default)

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#clock summer-time DST April 16 2005 00:00 October 23 2005 23:59
SCE(config)#
```

EXAMPLE 3

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no clock summer-time
SCE(config)#
```

Related Commands

Command	Description
clock set	
calendar set	
show calendar	
show clock	

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 so 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

zone	The name of the time zone to be displayed.
hours	The hours offset from UTC. This must be an integer in the range –23 to 23.
minutes	The minutes offset from 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

UTC (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 UTC.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#clock timezone PST -10
SCE(config)#
```

Related Commands

Command	Description
calendar set	
clock set	
show calendar	

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>enable 10
Password:<cisco>
SCE#clock update-calendar
SCE#
```

Related Commands

Command	Description
clock set	
calendar set	
clock read-calendar	

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, use the **exit** command.

Authorization: admin

Examples

The following example enters the Global Configuration Mode.

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE#(config) #
```

Related Commands

Command	Description
exit	

connection-mode (SCE 1000 platform)

Sets the connection mode parameters for an SCE 1000 platform.

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 an out-of-line topology using a 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 Configurati

Usage Guidelines

This command can only be used if the line card is in either **no-application** or **shutdown** mode.

Authorization: admin

Examples

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

```
SCE1000>enable 10
Password:<cisco>
SCE#config
SCE1000(config)#interface linecard 0
SCE1000(config if)#connection-mode inline on-failure cutoff
SCE1000(config if)#
```

Related Commands

Command	Description
show interface linecard connection-mode	

connection-mode (SCE 2000 platform)

Sets the connection mode parameters for an SCE 2000 platform.

connection-mode ***connection-mode*** **sce-id** ***sce-id*** **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
sce-id	A number that identifies the SCE platform in a cascaded pair. The sce-id parameter, which identifies the SCE platform, replaces the physically-connected-link parameter, which identified the link. This change was required with the introduction of the SCE8000 GBE platform, which supports multiple links. In the SCE2000, the number assigned to the sce-id parameter (0 or 1) will be defined as the of number of the physically-connected-link. Note that for backwards compatibility, the physically-connected-link parameter is currently still recognized. (cascaded SCE platform topology only) • **0** • **1**
priority	Defines the primary SCE platform. (cascaded SCE platform topologies only). • **primary** • **secondary**
on-failure	Determines system behavior on failure of the SCE platform. (inline topologies only) • **bypass** • **cutoff**

Defaults

connection mode = inline

sce-id = 0

priority = primary

on-failure = bypass

Command Modes

Linecard Interface Configuration

Usage Guidelines

Caution This command can only be used if the line card is in either **no-application** or **shutdown** mode.

Authorization: admin

Examples

The following example shows how to configure the primary SCE platform in a two-SCE platform inline topology. This device is designated as SCE platform‘0’, and the behavior of the SCE platform if a failure occurs is bypass (default).

```
SCE>enable 10
Password: <cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#connection-mode inline-cascade sce-id 0 priority primary on-failure bypass
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard connection-mode	
show interface linecard cascade **redundancy-status**	
show interface linecard cascade connection-status	
show interface linecard cascade peer-sce-information	

control-exception-traffic

Defines what actions should be assigned to the different types of exception traffic. Use the **no** form of the command to enable the TCP checksum exception (it disables the disable of the TCP checksum exception). Use the **default** form of the command to restore the default exception handling configuration for all exception types.

control-exception-traffic {(type *type* action *action*) | tcp-checksum-exception-disable}

no control-exception-traffic tcp-checksum-exception-disable

default control-exception-traffic

Syntax Description

type	Type of exception (see **Usage Guidelines** for a list of exception types).
action	Action to be taken when this exception occurs (see **Usage Guidelines** for a list of actions).
tcp-checksum-exception-disable	Keyword, disables the tcp-checksum exception.

Defaults

By default, exception traffic is handled as follows:

- TCP Checksum errors are disabled
- All exception traffic types are bypassed in HW (action = bypass), except for IP_ERR, which is passed to the traffic processor (action = pass)

Command Modes

Interface Linecard Configuration

Usage Guidelines

This setting is effective only when the SCE platform is configured to ' *inline* ' connection mode. In receive-only mode, all exception traffic is dropped by the hardware.

Exception traffic packets are marked as such by the HW for various reasons (see list of exception packet types below). The HW can pass such packets to the software for special handling, which imposes a performance burden on the traffic processor. Alternatively, the hardware can bypass such packets or drop them.

TCP checksum error is a special case of exception traffic. It can either be passed to the traffic processor for special handling, or it can be handled by the HW as a regular flow, which places less of a burden on system performance and is more resistant to attacks.

Use **no control-exception-traffic tcp-checksum-exception-disable** to cause TCP checksum error packets to be handled specifically by the traffic processor.

Exception Packet Types

Following is a list of possible exception packet types:

- ARP — ARP protocol packets
- GEN_PARSER_ERR — Generic HW parsing failure
- IP_BROD — IPv4 broadcast packet

- IP_ERR — IP Checksum Error
- L2TP_CONTROL — L2TP control packet
- L2TP_OFFSET — L2TP packet with non zero offset field
- NON_IP — Any other non IPv4 L3 protocol
- PPP_PROTOCOL_COMPR — PPP protocol with compression enabled
- TTL_ERR — Zero TTL IP packet

Possible Actions

Following is a list of possible actions:

- Bypass — HW bypass, which passes packets directly from the DP to the TX without software intervention.
- Pass — Passes the packet to the traffic processor.
- Drop — Drops the packet at the DP so that neither the traffic processor nor the intended destination of the packet will receive it, thus implementing net filtering. Note that in L2TP scenario, the drop action will take place only when the system is configured to L2TP mode.
- Classif

Authorization: root

Examples

The following example configures the SCE platform to drop all NON_IP exception packets.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>control-exception-traffic type non_ip action drop
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard control-exception-traffic	

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>enable 10
Password:<cisco>
SCE#copy analysis.sli applications/analysis.sli
SCE#
```

Related Commands

Command	Description
copy ftp://	
copy-passive	

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 eight characters, dot, then three characters.

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 10.10.10.10 with user name “user” and password “a1234”.

```
SCE>enable 10
Password:<cisco>
SCE#copy ftp://user:a1234@10.10.10.10/p:/applications/ftp.sli
SCE#
```

Related Commands

Command	Description
copy-passive	
ip ftp password	
ip ftp username	

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 password of the given username.
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>enable 10
Password:<cisco>
SCE#copy-passive appl/analysis.sli
ftp://myname:mypw@10.1.1.105/p:/applications/analysis.sli
SCE#
```

Related Commands

Command	Description
copy ftp://	
ip ftp password	
ip ftp username	

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>enable 10
Password:<cisco>
SCE#copy running-config startup-config
Backing-up configuration file...
Writing configuration file...
SCE#
```

Related Commands

Command	Description
more	
show running-config	

copy running-config startup-config (ROOT level options)

Builds a configuration file, which is used in successive boots, with the specified type of configuration commands.

copy running-config-application startup-config-application

copy running-config-all startup-config-all

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

This command builds either the current application configuration or the complete current configuration, depending on the option specified:

- copy running-config-application — Builds a configuration file (*applcfg.txt*) with application-related configuration commands.
- copy running-config-all — Builds all configuration files.

You can view the relevant running configuration before using it to build a configuration file by using the appropriate **more running-config** command.

Authorization: root

Examples

The following example saves the current configuration for successive boots.

```
SCE>enable 15
Password:<cisco>
SCE#>copy running-config-all startup-config-all
Backing-up configuration file...
Writing configuration file...
SCE#>
```

Related Commands

Command	Description
copy running-config startup-config	

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>enable 10
Password:<cisco>
SCE#copy /appl/analysis.sli ftp://myname:mypw@10.1.1.105/p:/applications/analysis.sli
SCE#
```

Related Commands

Command	Description
copy ftp://	

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/bckupcfg.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.

```
SCE>enable 10
Password:<cisco>
SCE#copy ftp://user:pass@host/drive:/dir/bakupcfg.txt startup-config
SCE#
```

Related Commands

Command	Description
copy startup-config destination-file	

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/bckupcfg.txt* • */tffs0*

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The destination 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.

```
SCE>enable 10
Password:<cisco>
SCE#copy startup-config ftp://user:pass@host/drive:/dir/bckupcfg.txt
SCE#
```

Related Commands

Command	Description
copy source-file startup-config	

debug flow-capture

Executes flow capture operations.

debug flow-capture { start | stop | create-cap ***file-destination*** **}**

Syntax Description

file-destination	Destination where the cap file should be created (may also be an FTP site path). If no absolute path is given, the file is saved in the root directory

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

The flow capture is a useful debugging capability that captures packets from the traffic stream in real time and stores them for later analysis using a standard cap format. The classification of the traffic portion to be captured is based on L4 attributes.

The following operations are available:

- **start** – start recording
- **stop** – stop recording
- **create-cap** – creates a cap file in the given destination

Note that traffic can be captured only when an application is loaded.

To perform a flow capture, complete the following steps:

1. (Optional) Configure limits to the flow capture operation using the **flow-capture controllers** command, to prevent a negative impact on traffic processing.

   You may skip this step and use the default controller values.

2. Configure an appropriate recording rule using the **traffic-rule** command. Assign the **flow-capture** action to the rule (see **traffic-rule (ROOT level options)**).

   Note the following limitations:

   – Only one recording traffic rule can be defined in the system at a time.

   – You must use the **traffic-rule** command to define the recording rule. You cannot use the **flow-filter** command.

3. Start the actual capture. The capture will not start unless a valid recording rule has been defined.

   Use the **debug flow-capture start** command.

4. Stop the capture.

   Use the **debug flow-capture stop** command.

5. Create the cap file. The captured data is saved as a CAP file in Snoop v4 format. The cap file will not be created until both a start and stop command have been executed.

   Use the **debug flow-capture create-cap** command.

At any point, you can use the **show interface linecard flow-capture** command to display the flow capture status, including whether flow capture is currently recording or is stopped, the capacity already used and the number of packets recorded.

Authorization: root

Examples

The following example shows how to perform all the steps in a flow capture:

1. Define the limits. (**flow-capture controllers capacity** and **flow-capture controllers time**)
2. Define the recording traffic rule. (**traffic-rule** with **action flow-capture** option)
3. Start the capture. (**debug flow-capture start**)

   (**show** command shows that recording is in progress.)
4. Stop the capture. (**debug flow-capture stop**)
5. Create the cap file. (**debug flow-capture create-cap**)

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-capture controllers capacity 50000
SCE(config if)#>flow-capture controllers time unlimited
SCE (config if)#>traffic-rule name FlowCaptureRule IP-addresses subscriber-side all
network-side all protocol 250 direction both traffic-counter counter2 action flow-capture
SCE(config if)#>exit
SCE(config)#>exit
SCE#>debug flow-capture start
SCE#>show interface linecard 0 flow-capture
Flow Capture Status:
--------------------
Flow Capture Status:  RECORDING
Recording Rule name:  FlowCaptureRule
Buffer Capacity (bytes): 50000
Capacity Usage:  10
Time limit (sec):  45
Number of recorded packets: 780
SCE#>debug flow-capture stop
SCE#>show interface linecard 0 flow-capture
Flow Capture Status:
--------------------
Flow Capture Status:  NOT RECORDING
Last Stop Cause:  User
Recording Rule name:  FlowCaptureRule
Buffer Capacity (bytes): 50000
Capacity Usage:  31234
Time limit (sec):  45
Number of recorded packets: 834720
SCE#>debug flow-capture create-cap
 capfile1
SCE#>
```

Related Commands

Command	Description
flow-capture controllers	
traffic-rule	

traffic-rule (ROOT level options)
show interface linecard flow-capture

debug performance aging-tuning start

Starts an aging tuning and dormant tuning measurement for the defined protocol.

debug performance aging-tuning start original-aging-time ***aging-time*** **aging-factor** ***percent*** **dormant-time** ***dormant-time***

debug performance aging-tuning start signature-id ***id*** **signature-mask** ***mask*** **aging-factor** ***percent*** **dormant-time** ***dormant-time***

Syntax Description

aging-time	Aging time of the protocol in seconds.
percent	The percentage by which to decrease the aging time (integer).
dormant-time	Dormant time of the protocol in seconds.
id	Signature-ID of the protocol.
mask	Bit mask that identifies the protocol.

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

If using the second form of the command, the protocol must match both the signature-id and the bit mask.

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>debug debug performance aging-tuning start original-aging-time 120 aging-factor 5
dormant-time 60
SCE#>
```

Related Commands

Command	Description

debug slot linecard mac-resolver ip

Performs the specified MAC resolver debug operation for the specified slot.

debug slot ***slot-number*** **linecard mac-resolver ip** ***ip-address*** **[vlan** ***vlan-id*** **]**

debug slot ***slot-number*** **linecard no mac-resolver ip** ***ip-address*** **[vlan** ***vlan-id*** **]**

debug slot ***slot-number*** **linecard mac-resolver mode active**

debug slot ***slot-number*** **linecard mac-resolver mode passive**

debug slot ***slot-number*** **linecard mac-resolver mode disable**

debug slot ***slot-number*** **linecard mac-resolver show clients**

debug slot ***slot-number*** **linecard mac-resolver show counters**

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
ip-address	The IP address to be added or removed from the MAC resolver database. In dotted notation (x.x.x.x).
vlan-id	VLAN tag that identifies the VLAN that carries this IP address (if applicable).

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

This command performs the following MAC resolver debug operations.

- **ip** — Adds the specified IP address (and optional VLAN ID) to the MAC resolver database.

  This command adds a dynamic entry to the MAC resolver database, that is, the IP address is added as an entry and the MAC address is dynamically resolved in the usual manner by listening the the ARP messages.

  Use the **no** form of the command to remove the specified IP address from the MAC resolver database.

  To add a static entry to the database, including both the IP address and the related MAC address, use the **mac-resolver arp** command.
- **mode** — Specifies the MAC resolver operation mode
  - active — MAC resolver active mode
  - disable — Disable MAC resolver
  - passive — MAC resolver passive mode
- **show** — Displays MAC resolver information:
  - clients

– counters

MAC Resolver Modes

The MAC resolver can be enabled to work in either of the following modes. Use the appropriate keyword with the **mode** option to specify the desired mode:

- **Active** — enables ARP listening, aging, and ARP injection (ARP injection requires a port with a configured pseudo IP address; see the **pseudo-ip** command.)
- **Passive** — enables ARP listening and aging, ARP injection is disabled.

Authorization: root

Examples

The following example illustrates how to add an IP address to the MAC resolver database.

```
SCE>enable 15
Password:<cisco>
SCE#>debug slot 0 linecard mac-resolver ip 10.10.10.10
SCE#>
```

Related Commands

Command	Description
mac-resolver	
mac-resolver arp	

debug slot show

Displays the specified objects.

debug slot *slot-number* show {traffic-rules | capture-rules | traffic-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

Specify the group of objects to display:

- traffic rules
- traffic counters
- capture rules

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>debug slot 0 linecard show traffic-rules

0: Rule 'Sli0', owner 'SLI':
Content of rule # 0:
Ip 1: min=0.0.0.0, max=255.255.255.255, inverse=no.
Ip 2: min=0.0.0.0, max=255.255.255.255, inverse=no.
Port 1: min=0, max=65535, inverse=no.
Port 2: min=0, max=65535, inverse=no.
TOS: min=0x0, max=0xff, inverse=no.
Protocol: value=all.
Network interface: BOTH.
TCP Flags: SYN=ignore, FIN=ignore, PSH=ignore, ACK=ignore, URG=ignore, RST=ignore
All-inverse: no.
Action fields:
Bypass-flow: Action=pass, Priority=0.
Drop-flow: Action=pass, Priority=0.
Bypass-packet: not-active.
Duplicate TP1: not-active.
Duplicate TP2: not-active.
Duplicate TP3: not-active.
Open flow to Software: disabled.
RUC Data: 0x0
Target PPC: not-active.
Default Class: not-active
Default metering type: not-active
SCE#>
```

Related Commands

Command	Description

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# default subscriber template all
SCE(config if)#
```

Related Commands

Command	Description
subscriber template import csv-file	
show interface linecard subscriber templates	
party template	

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 how to use this command:

EXAMPLE 1:

The following example deletes the *oldlog.txt* file.

```
SCE>enable 10
Password:<cisco>
SCE#delete oldlog.txt
SCE#
```

EXAMPLE 2:

The following example deletes the *oldlogs* directory.

```
SCE>enable 10
Password:<cisco>
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

Command	Description
dir	
rmdir	

delete (ROOT level option)

Interactively deletes a complete directory and its contents from the local flash file system.

delete ***directory*** **/recursive /interactive**

Syntax Description

directory	The name of the directory to be deleted.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

When the interactive switch is specified, the system prompts for confirmation of the deletion of each file in the directory.

Authorization:

- The **/recursive** switch (deletes a complete directory) is available at the admin authorization level.
- The **/interactive** switch is available only at the root authorization level.

Examples

The following example illustrates how to use this command:

```
SCE>enable 15
Password:<cisco>
SCE#>delete test /recursive /interactive
Enter directory '/tffs0/test'?y
Delete file '/tffs0/test/PORT80.SLI'?
Delete file '/tffs0/test/DEBUG.TXT'?
Delete file '/tffs0/test/BIG.CAP'?
Delete file '/tffs0/test/DEBUG2.TXT'?y
1 files and 0 directories have been deleted.
SCE#>
```

Related Commands

Command	Description
delete	

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>enable 10
Password:<cisco>
SCE#dir
File list for /tffs0/
512TUE JAN 01 00:00:00 1980LOGDBG DIR
512TUE JAN 01 00:00:00 1980LOG DIR
7653 TUE JAN 01 00:00:00 1980FTP.SLI
29 TUE JAN 01 00:00:00 1980SCRIPT.TXT
512 TUE JAN 01 00:00:00 1980SYSTEM DIR
SCE#
```

Related Commands

Command	Description
pwd	
cd	

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.

Defaults

This command has no default settings.

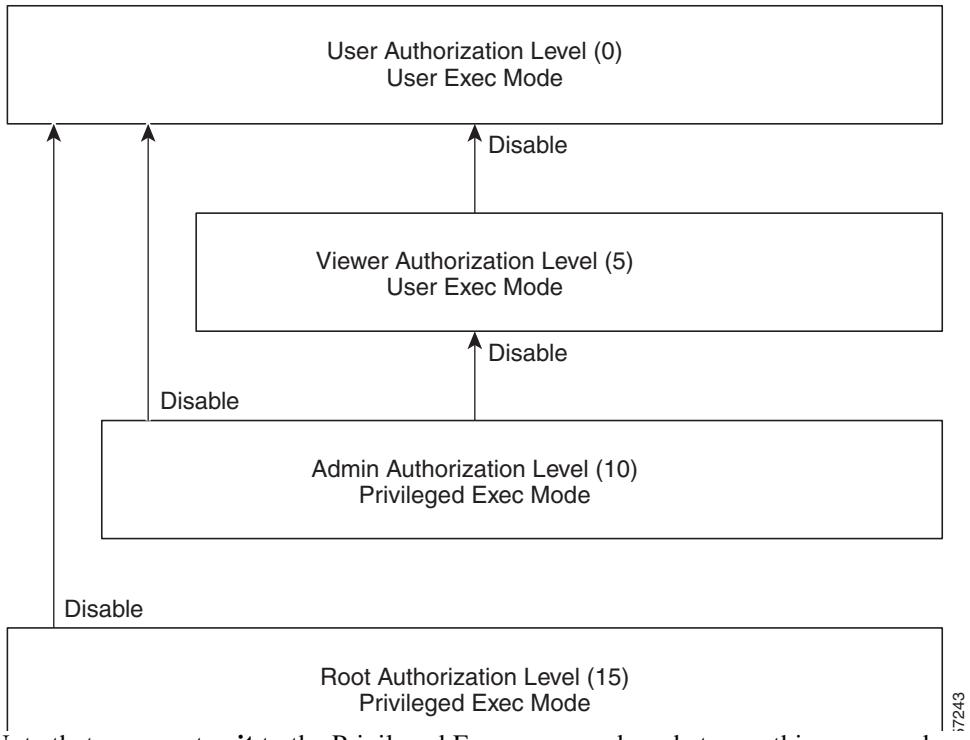
Command Modes

Privileged Exec and Viewer

Usage Guidelines

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

Figure 2-1 Disable Command



Note that you must **exit** to the Privileged Exec command mode to use this command.

Authorization: user

Examples

The following example shows how to change from root to admin mode:

```
SCE>enable 15
Password:<cisco>
SCE#>disable 10
SCE#
```

Related Commands

Command	Description
enable	

do

Use the **do** command to execute an EXEC mode command (such as a show command) or a privileged EXEC command (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 exec 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 user exec mode.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#connection-mode on-failure bypass
SCE(config if)#do show interface linecard 0 connection-mode
slot 0 connection mode
Connection mode is inline
slot failure mode is bypass
Redundancy status is standalone
SCE(config if)#
```

Related Commands

Command	Description

dropped-bytes counting-mode

Sets the dropped-bytes counting mode.

dropped-bytes counting-mode {by-queue|by-global-controller}

Syntax Description

This command has no arguments.

Defaults

default dropped-bytes counting mode = **by-global-controller**

Command Modes

Linecard Interface Configuration

Usage Guidelines

Dropped bytes (bytes dropped due to exceeding the provisioned bandwidth) are counted only by the hardware. The SCE platform can be configured to count these dropped bytes by either of the following mechanisms:

- by global controller (default)
- by queue

Note that dropped packets (as opposed to dropped bytes) can be configured to be counted either by the hardware platform or the software application (see **accelerate-packet-drops**).

Specify the appropriate keyword, **by-queue** or **by-global-controller.**

Authorization: root

Examples

The following example configures the SCE platform to count dropped bytes by queue.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>dropped-bytes counting-mode by-queue

SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard counters dropped-bytes	

duplex

Configures the duplex operation of the management interface.

duplex ***mode***

no duplex

Syntax Description

mode	Set to the desired duplex mode: • **full** : full duplex • **half** : half duplex • **auto** : auto-negotiation (do not force duplex on the link)

Defaults

mode = Auto

Command Modes

Mng Interface Configuration

Usage Guidelines

Use this command to configure the duplex mode of the Fast Ethernet management interface.

- command mode = Mng Interface Configuration
- interface designation = 0/1 or 0/2

If the speed (see **speed**) of the relevant interface is configured to **auto,** changing this configuration has no effect.

Authorization: admin

Examples

The following example configures management port #2 to auto mode.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface mng 0/2
SCE(config if)#duplex auto
SCE(config if)#
```

Related Commands

Command	Description
speed	
interface mng	
show interface mng	

duplicate-allowed

Enables duplication of packets to TP-0 for delay sensitive traffic, such as various media protocols. Use the **no** form of the command to disable packet duplication for the specified type of packets.

duplicate-allowed {set-flow [ratio *ratio*] | shortage | bundles | all}

no duplicate-allowed {set-flow | shortage | bundles | all}

Syntax Description

ratio	Set-flow duplicate ratio (percent).

Defaults

By default, packet duplication is enabled for all types of packets.

default ratio = 70

Command Modes

Interface Linecard Configuration

Usage Guidelines

Specify the option for which packet duplication is to be enabled or disabled:

- set-flow: packet duplication for flows that have been set by the application as No-Online-Control traffic
  - You can specify the set-flow duplicate ratio, which limits the ratio of duplicate flows (configuring the ratio also implicitly enables set-flow packet duplication)
- shortage: packet duplication for all UDP flows in case of shortage
- bundles: packet duplication for bundled flows that have been set by the application as No-Online-Control due to delay sensitive traffic
- all: all of the above (not all traffic)

You can enable packet duplication from a specified Traffic Processor as part of **flow-filter** rule configuration. (In the **flow-filter** command, see **duplicate-actions** under " **Actions** ".)

Authorization: root

Examples

The following example shows how to enable and configure packet duplication due to No-Online-Control traffic.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>duplicate-allowed set-flow ratio 75
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard duplicate-packets-mode	
flow-filter	

enable

Enables the user to access a higher authorization level.

enable [*level*]

Syntax Description

level	User authorization level (0, 5, 10, 15) as specified in *"CLI Authorization Levels"*.

Defaults

level = admin

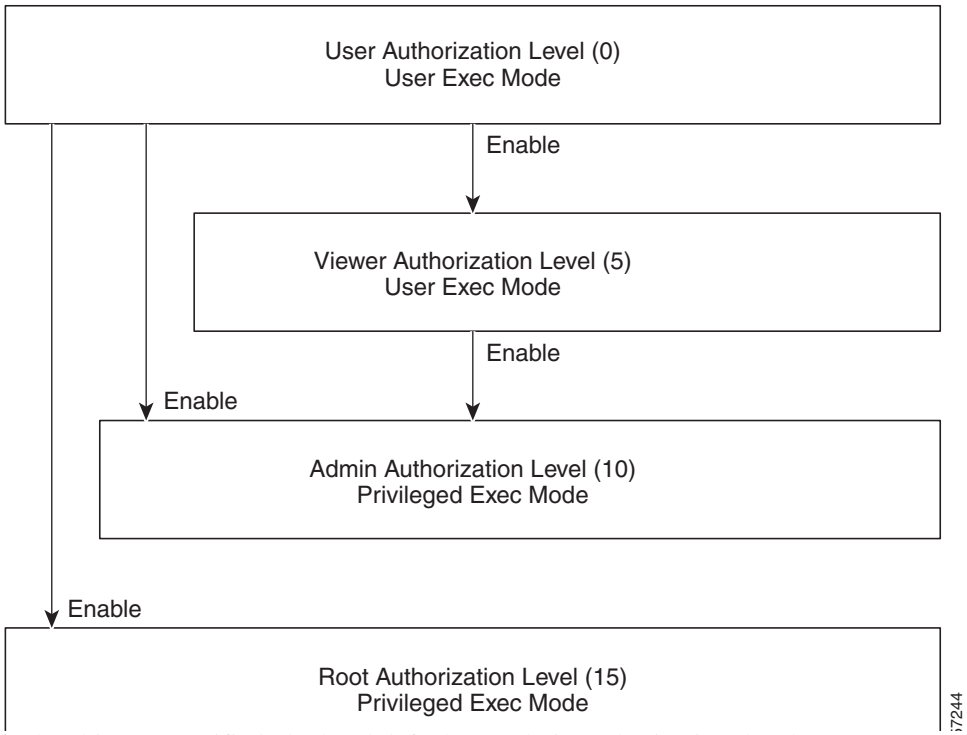
Command Modes

User Exec

Usage Guidelines

Authorization levels are illustrated in the following figure

Figure 2-2 Enable Command



If a level is not specified, the level defaults to admin authorization, level 10.

Note that you cannot use the **enable** command from the Privileged Exec or any of the configuration command modes.

Authorization: User

Examples

The following example accesses the administrator authorization level. Note that the prompt changes from **SCE>**to **SCE#,** indicating that the level is the administrator privilege level.

```
SCE>enable
Password:<cisco>
SCE#
```

Related Commands

Command	Description
disable	
enable password	

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"*. 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 = **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>enable 10
Password:<cisco>
SCE#config
SCE(config)#enable password level 10 a123*man
SCE(config)#
```

Related Commands

Command	Description

enable
service password-encryption

end

Exits from the global configuration mode or interface configuration mode to the User Exec authorization level.

end

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Global Configuration

Usage Guidelines

Use this command to exit to the User Exec authorization level in one command, rather than having to execute the **exit** command twice. The system prompt changes to reflect the lower-level mode.

Authorization: admin

Examples

The following example illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#end
SCE#
```

Related Commands

Command	Description

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

Usage Guidelines

The following data is deleted by this command:

- 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.

You can use the **copy startup-config destination-file** command to create a backup of the current configuration before it is deleted.

Authorization: admin

Examples

The following example shows how to erase the startup configuration.

```
SCE>enable 10
Password:<cisco>
SCE#erase startup-config-all
```

Related Commands

Command	Description
reload	
copy startup-config destination-file	

exit

Exits from the current mode to the next "lower" mode. When executed from Privileged Exec or User Exec, it logs out of the CLI session.

exit

Syntax Description

This command has no arguments or 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.

Tip Use the **end** command to exit directly to the User Exec authorization level.

Authorization: admin

Examples

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#exit
SCE(config)#exit
SCE#exit
Connection closed by foreign host.
```

Related Commands

Command	Description
configure	
interface gigabitethernet	
interface linecard	
interface mng	
line vty	

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

mode	**operational** or **non-operational.** Indicates whether or not the system will boot as operational 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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#failure-recovery operation-mode operational
SCE(config)#
```

Related Commands

Command	Description
show failure-recovery operation-mode	

flow-capture controllers

Configures limitations on the flow capture feature. Use the **default** form of the command to reset all options to the default values.

flow-capture controllers time (*duration* | unlimited)

flow-capture controllers max-l4-payload-length (*length* | unlimited)

default flow-capture controllers (time | max-l4-payload-length)

Syntax Description

duration	Maximum duration for the flow capture recording time in seconds. To specify unlimited duration, use the **unlimited** keyword.
length	To specify unlimited payload bytes per packet, use the **unlimited** keyword.

Defaults

duration = 3600 seconds

length = unlimited

Command Modes

Interface Linecard Configuration

Usage Guidelines

The flow capture is a useful debugging capability that captures packets from the traffic stream in real time and stores them for later analysis. The classification of the traffic portion to be captured is based on L4 attributes.

The portion of traffic that is captured does not receive service (is not processed by the application). Therefore it is important to control the capturing scenario so that service is not negatively affected. This is done by limiting certain aspects of the flow capture.

The following options are available:

- **time** (flow capture recording time) — The duration of the flow capture may be limited to the specified time limit, or it may be unlimited, so that the flow capture is stopped only by executing the explicit stop command, or when maximum file size is reached (128MB in SCE8000 platform).
- **max-l4-payload-length** (payload size)— The maximum number of L4 bytes captured from each packet may be specified. This parameter relates to each packet in the traffic stream rather than overall flow capture capacity. Using this parameter, the flow-capture throughput (in terms of captured packets) can be increased.

Authorization: admin

Examples

The following example shows how to configure the limitations to the flow capture.

```
SCE>enable 10
Password:<cisco>
SCE#>configure
SCE(config)#interface linecard 0
```

```
SCE(config if)#flow-capture controllers time 120
SCE(config if)#flow-capture controllers max-l4-payload-length 200
SCE(config if)#
```

Related Commands

Command	Description
traffic-rule	
flow-capture	
show interface linecard flow-capture	

flow-aging default-timeout

Sets the default timeout for flow aging for the specified type of flows. Use the **no** form of the command to remove the user-configured default and revert to the system default.

flow-aging default-timeout {non-TCP/UDP | non-TCP/UDP-asymmetric | TCP-data | TCP-data-asymmetric | TCP-establishment | TCP-establishment-asymmetric | UDP | UDP-asymmetric} ***timeout***

no flow-aging default-timeout {non-TCP/UDP | non-TCP/UDP-asymmetric | TCP-data | TCP-data-asymmetric | TCP-establishment | TCP-establishment-asymmetric | UDP | UDP-asymmetric}

Syntax Description

timeout	The timeout interval in seconds.

Defaults

default timeouts:

- TCP-Establishment: 10 seconds
- TCP-Data: 120 seconds
- UDP: 10 seconds
- Non-TCP/UDP: 10 seconds
- TCP-Establishment-asymmetric: 10 seconds
- TCP-Data-asymmetric: 120 seconds
- UDP-asymmetric: 20 seconds
- Non-TCP/UDP-asymmetric: 20 seconds

Command Modes

Interface Linecard Configuration

Usage Guidelines

Specify one of the following flow types:

- Non-TCP/UDP — Non-TCP/UDP flows
- TCP-Data — TCP flows on data transfer
- TCP-Establishment — TCP flows on establishment
- UDP — UDP flows
- Non-TCP/UDP-asymmetric — Non-TCP/UDP flows when asymmetric routing is enabled
- TCP-Data-asymmetric — TCP flows on data transfer when asymmetric routing is enabled
- TCP-Establishment-asymmetric — TCP flows on establishment when asymmetric routing is enabled
- UDP-asymmetric — UDP flows when asymmetric routing is enabled

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1:

The following example shows how to set the flow aging timeout value for non-TCP/UDP flows (asymmetric routing not enabled).

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-aging default-timeout Non-TCP/UDP 10
SCE(config if)#>
```

EXAMPLE 2:

The following example shows how to set the flow aging timeout value for UDP flows with asymmetric routing enabled.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-aging default-timeout UDP-asymmetric 25
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard flow-aging default-timeout	

flow-capture controllers

Configures limitations on the flow capture feature. Use the**default** form of the command to reset all options to the default values.

flow-capture controllers {(capacity *capacity*) | (time (*time* | unlimited))} | max-l4-payload-length (*length* | unlimited)

default flow-capture

Syntax Description

capacity	data capacity in bytes
time	recording time in seconds or specify **unlimited** time
length	decimal number that specifies the maximal number of L4 payload bytes captured from each packet or specify **unlimited** length

Defaults

capacity =.5 MB (500,000 bytes)

time = 60 seconds

length = unlimited

Command Modes

Interface Linecard Configuration

Usage Guidelines

The flow capture is a useful debugging capability that captures packets from the traffic stream in real time and stores them for later analysis using a standard cap format. The classification of the traffic portion to be captured is based on L4 attributes.

The portion of traffic that is captured does not receive service (is not processed by the application). Therefore it is important to control the capturing scenario so that service is not negatively affected. This is done by limiting certain aspects of the flow capture.

The following options are available:

- **capacity** (flow capture capacity) — The feature is able to store and capture only a limited amount of data. The capacity is related to the amount of raw data recorded, and reflects the size of the capturing buffer. It does not necessarily reflect the size of the capture file created.
- **time** (flow capture recording time) — The duration of the flow capture may be limited to the specified time limit, or it may be unlimited, so that the flow capture is stopped only via the explicit stop command.
- **max-l4-payload-length** (payload size)— The maximum number of L4 bytes captured from each packet may be specified. This parameter relates to each packet in the traffic stream rather than overall flow capture capacity.

Authorization: root

Examples

The following example shows how to configure the limitations to the flow capture.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-capture controllers capacity 100000
SCE(config if)#>flow-capture controllers time 120
SCE(config if)#>flow-capture controllers max-l4-payload-length 200
SCE(config if)#>
```

Related Commands

Command	Description
traffic-rule	
traffic-rule (ROOT level options)	
show interface linecard flow-capture	

flow-filter

Use this command to define a flow filter rule (**flow-filter set-ff rule**).

Following is a summary of the structure of the command:

flow-filter {set-ff | set-table} rule *rule-number* <IP addresses><port numbers>{<tos id>| <tunnel id>} <protocol><network interface><TCP flags><match inverse><actions (counters)><tos marking>

Following is the complete command:

flow-filter {set-ff | set-table} rule *rule-number* ip1-min*ip1-min* ip1-max *ip1-max* ip1-inv {false|true} ip2-min *ip2-min* ip2-max *ip2-max* ip2-inv {false|true} port1-min *port1-min* port1-max *port1-max* port1-inv {false|true} port2-min *port2-min* port2-max *port2-max* port2-inv {false|true} {tos-min *tos-min* tos-max *tos-max* tos-inv {false|true} | tid-min *tid-min* tid-max *tid-max* } protocol {all | EIGRP | ICMP | IGRP | IS-IS | OSPF | TCP | UDP | *decimal-protocol-number* } Net-If {BOTH | Subscriber | network} SYN {(0|1|ignore} FIN {(0|1|ignore} PSH {(0|1|ignore} ACK {(0|1|ignore} URG {(0|1|ignore} RST {(0|1|ignore} all-inv {false|true} action-bypass-flow {disable | (priority *priority-number* action {bypass|pass}}} action-drop-flow {disable | {priority *priority-number* action {drop|pass}}} action-bypass-packet {disable|drop|no-drop} [open-to-software {disable|enable}] [duplicate-actions duplicate-TP1 {disable|enable} duplicate-TP2 {disable|enable} duplicate-TP3 {disable|enable}] action-ruc-data *number* action-target-ppc {disable|*target-ppc* } action-default-class {disable|BE|AF2|AF3|AF4|EF} action-default-metering-type {disable|*metering-type* } action-conditional-bypass-or-drop {disable|enable} action-dont-open-flow {disable|enable} action-increment-counters {none|*counters* } [upstream-tos-id *tos-id1* downstream-tos-id *tos-id2*]

Following are the remaining command formats:

flow-filter default-mode drop {true | false} bypass {true | false}

flow-filter partition name *partition-name* first-rule *rule-number* num-rules *number-of-rules*

flow-filter execute-table

flow-filter clear-table

flow-filter (set-ff | set-table) rule *rule-number* clear

flow-filter reset

Syntax Description

rule-number	The ID number of the rule (0-127)
partition-name	Name of partition to which to assign the specified flow filter rules
number-of-rules	Total number of consecutive rules to assign to the partition, beginning with the specified rule For an explanation of the remaining arguments and keywords, refer to " **Usage Guidelines** " below.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Use this command to perform the following operations on the flow filter:

- Define default drop and bypass modes — **flow-filter default-mode drop {true | false} bypass {true | false}**
- Clear a specified rule from the flow filter — **flow-filter set-ff rule clear**
- Reset the flow filter — **flow-filter reset**
- Assign flow filter rules to a specified partition — **flow-filter partition name**

This command also performs the following operations on the temporary flow filter rule table:

- Add a rule to the temporary table — **flow-filter set-table rule**
- Copy all rules currently in the temporary table from the table to the flow-filter — **flow-filter execute-table**
- Clear a specified rule from the temporary rule table — **flow-filter set-table rule clear**
- Clear the temporary rule table — **flow-filter clear-table**

The command for defining a flow filter rule, whether directly in the flow filter or in the temporary rule table, is very complex, as it entails defining all the parameters of the rule.

- Use the **clear** option to clear the specified flow filter rule.
- Use the **set-ff** option to clear a rule from the flow filter.
- Use the **set-table** option to clear a rule from the temporary table before it has been copied from the table to the flow filter by executing the **execute-table** command.
- If the rule is removed from the flow filter, but not from the temporary table, the next **execute-table** command will copy it to the flow filter again.

Use the **reset** option to remove all flow filter rules and reset all counters. This includes all flow filter rules, as follows:

- Rules configured via these ‘ **flow-filter** ’ CLI commands
- Traffic rules and traffic counters configured via the admin level traffic-rule and traffic-counter CLI commands

Use the **default-mode** option to define the default drop and bypass actions. You must specify both actions in the command.

- False — default is not to drop/bypass
- True — default is to drop/bypass

Use the **partition** option to assign flow filter rules to a partition. You can assign an unlimited number of rules to a partition, but they must have consecutive rule numbers.

- You can assign a range of rules to a specified partition. First define the number of the first rule to be assigned (**first-rule**) and then indicate the total number of rules to be assigned (**num-rules**). (see Example 2)

Use the **set-table** option to define rules in the temporary rule table.

- Use the **flow-filter execute-table** command to copy all the rules currently in the temporary rule table to the flow filter.
- Use the **flow-filter set-table rule clear** command to remove a specific rule from the temporary table. If the **execute-table** command is then executed, the specified rule will not be copied to the flow filter.
- Use the **flow-filter clear-table** command to remove all rules from the temporary table. If the **execute-table** command is then executed, nothing will be copied to the flow filter.

The following guidelines all relate to configuring a flow filter rule (**flow-filter {set-ff | set-table} rule**).

Command form (set-ff or set-table):

- Use the **set-ff** option to set the rule directly in the flow filter.
- Use the **set-table** option to set the rule in the temporary table. To copy the rule from the table to the flow filter, use the **execute-table** command.

Rule

Rule number is an integer between 0 and 127.

IP addresses

Define the IP address range to which this flow filter rule applies for both network side and subscriber side traffic.

- **ip1** fields refer to the subscriber side
- **ip2** fields refer to the network side

For each side, define the following parameters:

- **ip-min** — The lowest IP address in the range for the specified side
- **ip-max** — The highest IP address in the range for the specified side
- **ip-inv** — This parameter indicates how to match the range of IP addresses for the specified side
  - **True** — values inside the range between **ip-min** and **ip-max** match (**ip-min** <= IP address <= **ip-max**)
  - **False** — values outside the range between **ip-min** and **ip-max** match (IP address <**ip-min** or IP address >**ip-max**)

IP addresses can be entered in one of three formats:

- decimal number
- hex number prefixed by 0x
- dotted-decimal notation (A.B.C.D)

Port numbers

Define the range of port numbers to which this flow filter rule applies for both network side and subscriber side traffic.

- **port1** fields refer to the subscriber side
- **port2** fields refer to the network side

For each side, define the following parameters:

- **port-min** — The lowest port number in the range for the specified side
- **port-max** — The highest port number in the range for the specified side

- **port-inv** — This parameter indicates how to match the range of port numbers for the specified side
  - **True** — values inside the range between **tos-min** and **tos-max** match (**tos-min** <= TOS field value <= **tos-max**)
  - **False** — values outside the range between **tos-min** and **tos-max** match (TOS field value <**tos-min** or TOS field value >**tos-max**)

For all protocol types except TCP and UDP, ports must be defined as follows:

- **port-min** must be = 0
- **port-max** must be = 65535
- **port-inv** must be = false.

TOS

You must configure either TOS or the Tunnel ID range to which this flow filter rule applies, depending upon the system mode. (Use the **no traffic-rule tunnel-id-mode** command to disable defining the traffic rule according to the tunnel ID.)

For TOS, define the following parameters:

- **tos-min** — The lowest TOS field value in the range
- **tos-max** — The highest TOS field value in the range
- **tos-inv** — This parameter indicates how to match the range of TOS field value
  - **True** — values inside the range between **tos-min** and **tos-max** match (**tos-min** <= TOS field value <= **tos-max**)
  - **False** — values outside the range between **tos-min** and **tos-max** match (TOS field value <**tos-min** or TOS field value >**tos-max**)

Tunnel ID

You must configure either TOS or the Tunnel ID range to which this flow filter rule applies, depending upon the system mode. (Use the **traffic-rule tunnel-id-mode** command to enable defining the traffic rule according to the tunnel ID.)

For Tunnel ID, define the following parameters:

- **tid-min** — The lowest tunnel ID in the range
- **tid-max** — The highest tunnel ID in the range
- The following tunnel IDs are reserved for MPLS learning: 0xff, 0xfe, 0xfd

All IP addresses, port numbers and TOS values

If all IP addresses, port numbers and TOS values are allowed for the rule, use the following option in place of configuring specific IP address range, port number range and TOS value range:

- **any-ip1-ip2-port1-port2-tos**

Protocol

Specify one of the following protocol options to which this flow filter rule applies:

- Specific protocol type: EIGRP, ICMP, IGRP, IS-IS, OSPF, TCP, or UDP
- Protocol ID number (0-255)
- ALL — any protocol

Network interface

This flow filter rule applies only to packets arriving from the specified interface:

- Subscriber
- Network
- Both

TCP flags

If protocol = TCP, this flow filter rule applies only if the TCP flags are set to the indicated value.

Set each flag to the value that must be matched:

- 0
- 1
- ignore

If protocol is not set to TCP, all TCP flags must be set to **ignore.**

Match inverse

Sometimes it is easier and more concise to define the conditions under which a rule does not apply. Use the **all-inv** option in this case:

- **all-inv = true** : inverts the entire definition, that is, when packets match the definition, the rule does NOT apply
- **all-inv = false** : normal match, when packets match the definition, the rule applies

Actions

Define the action to be taken when the conditions of the rule are matched. Actions can be either enabled or disabled. A disabled action means that the action is not triggered by the rule.

When the "drop flow" and "bypass flow" actions are enabled, they are assigned a priority between 0 (high) and 3 (low), allowing a meaningful resolution in case different rules specify different actions for the same packet.

The counters that are incremented by this rule are specified with the **increment-counters** action.

- **action-bypass-flow**

  Bypass-flow (FIF packets only) – Specify one of the following actions:

  - bypass – do not open a flow
  - pass – open a flow
- A priority (0-3) is specified.
- **action-drop-flow**

  Drop-flow (FIF packets only) – Specify one of the following actions:

  - drop – do not open a flow
  - pass – open a flow
- A priority (0-3) is specified.
- **action-bypass-packet {disable|drop|no-drop}**

  Bypass-packet (Non-FIF packets only) – Specify one of the following actions (for a packet belonging to a flow)

  - no-drop – bypassed
  - dropped
- **open-to-software** (optional)

  Open flows to software – Specify one of the following actions:
  - disable
  - enable
- **duplicate-actions** (optional)

  Allows duplicating the packets of a flow from the specified traffic processor to TP #0 for fast forwarding of delay-sensitive traffic (this is equivalent to the **quick-forwarding** action option in the **traffic-rule** command) – Specifies one of the following actions for the specified TP (TP1-TP3):
  - disable
  - enable
- **action-ruc-data**

  Specifies two bits (internally called rucInfo) that are directed to the packet descriptor header.
- **action-target-ppc**

  Target CPU (FIF packets only) – Specifies which CPU (traffic processor) should handle the flow opened by this packet. Specify either:
  - disable – do not assign a target CPU
  - CPU number (0-3)
- **action-default-class**

  Default-class (FIF packets only) – Specifies the specific class to which flows opened by this packet should be assigned. Specify one of the following:
  - EF
  - AF2
  - AF3
  - AF4
  - BE
  - disable – do not assign a default class
- **action-default-metering-type**

  Default meter type (FIF packets only) – Specifies the default metering type to which the flow opened by this packet should be assigned. Specify either:
  - disable – do not assign a default metering type
  - metering type number (1-4)
- **action-conditional-bypass-or-drop**

  Start conditional bypass (Non-FIF packets only) – Specifies that the flow should enter a state of weighted bypass. Specify one of the following actions:
  - disable
  - enable
- **action-dont-open-flow**

Don't open flow (Non-FIF packets only) – Specifies that flows corresponding to this rule will not be opened. Specify one of the following actions:

- disable
- enable

- **action-increment-counters**

  Counters (Both FIF and non-FIF packets) – Specifies which flow filter counters should count the packet. Specify one of the following:

  - none
  - list of counter numbers – specify a list of the counters (0-31), separated by commas with no spaces between (1,2,3 not 1, 2, 3). There is no limit to the number of counters that can be defined for a single rule.
  - Use the **traffic-counter** command (**traffic-counter name** *name* { **count-bytes | count-packets** }) to configure the counter mode for each counter:
  - Count packets: Each packet counted by the counter increments the counter by 1
  - Count bytes: Each packet counted by the counter increments the counter by the number of L3 bytes in the packet.

TOS Marking

You can configure a TOS marking to be applied by this flow filter rule. If you configure TOS marking, you must configure a value for both upstream and downstream traffic, although those values do not need to be the same.

TOS marking must be enabled for the relevant interfaces (see **tos-marking enabled**) and the TOS translation table defined (see **tos-marking set-table-entry**).

ToS marking cannot be used if **tunnel-id mode** is enabled (see **Tunnel ID** above).

For TOS, define the following parameters:

- **tos-id1, tos-id2** —The ID of the entry in the TOS translation table to be assigned to the traffic (one value for upstream and one for downstream)

  Range of acceptable values is 0-7. '0' indicates 'do not remark'. A value of 1-7 indicates that the DSCP value assigned to that ID in the translation table will be inserted in the TOS field.

  Default = 0 (do not remark)

Authorization: root

Examples

The following examples show how to use this command.

EXAMPLE 1

The following example shows how to define three rules in the temporary rule table, copy them to the flow filter, and clear the table.

In the first rule all IP addresses, port numbers, and TOS values are permitted, so the **any-ip1-ip2-port1-port2-tos** option is used.

In the second rule, the first command sets mode for TOS instead of Tunnel-Id, so t **unnel-id-mode** is disabled and Tunnel-Id is not defined. Since a non-TCP protocol is specified, all TCP flags are set to **ignore** and the port number ranges are both 0-65535. In addition, TOS marking values are defined.

The third rule defines a flow filter rule for all protocols except UDP. The match is defined for UDP and then the **all-inv** flag is used (set to true).

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-filter set-table rule 1 any-ip1-ip2-port1-port2-tos protocol
 TCP Net-If TH SYN 0 FIN 1 PSH 1 ACK 0 URG ignore RST 1 all-inv false action-bypass-flow
disable action-drop-flow priority 0 action pass action-bypass-packet drop action-ruc-data
0 action-target-ppc 2 action-default-class disable action-default-metering-type disable
action-conditional-bypass-or-drop enable action-dont-open-flow enable
action-increment-counters 1,2,6
SCE(config if)#>no traffic-rule tunnel-id-mode
SCE(config if)#>flow-filter set-table rule 2 ip1-min 10.10.10.10 ip1-max 10.10.10.100
ip1-inv false ip2-min 20.20.20.20 ip2-max 20.20.20.20 ip2-inv true port1-min 0 port1-max
65535 port1-inv false port2-min 0 port2-max 65535 port2-inv false tos-min 0 tos-max 0
tos-inv false protocol OSPF Net-If BOTH SYN ignore FIN ignore PSH ignore ACK ignore URG
ignore RST ignore all-inv false action-bypass-flow priority 2 action pass action-drop-flow
priority 1 action drop action-bypass-packet disable action-ruc-data 1 action-target-ppc
disable action-default-class BE action-default-metering-type 2
action-conditional-bypass-or-drop disable action-dont-open-flow disable
action-increment-counters 20,21,22,25,29,30 upstream-tos-id 0 downstream-tos-id 3
SCE(config if)#>flow-filter set-table rule 3 any-ip1-ip2-port1-port2-tos protocol UDP
Net-If BOTH SYN ignore FIN ignore PSH ignore ACK ignore URG ignore RST ignore all-inv true
action-bypass-flow priority 2 action pass action-drop-flow priority 1 action drop
action-bypass-packet disable action-ruc-data 0 action-target-ppc disable
action-default-class BE action-default-metering-type 2 action-conditional-bypass-or-drop
enable action-dont-open-flow enable action-increment-counters none
SCE(config if)#>flow-filter execute-table
SCE(config if)#>flow-filter clear-table
SCE(config if)#>
```

EXAMPLE 2

The following example shows how to assign flow filter rules 5-9 to a partition named Partition1. It is assumed that the rules have already been defined.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-filter partition name Partition1 first-rule 5 num-rules 5
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard flow-filter	
show applications slot flow-filter	
traffic-rule	
traffic-counter	

flow-open-mode

Configures the flow open mode.

flow-open-mode {classical | enhanced}

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the flow open mode is enhanced

Command Modes

Interface Linecard Configuration

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-open-mode classical
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard flow-open-mode	

flow-open-mode enhanced UDP min-packets

Sets the number of packets to pass over in between opening UDP flows. Use the **no** form of the command to remove the configured value. Use the **default** form of the command to revert to the default value (2).

flow-open-mode enhanced UDP min-packets ***number***

no flow-open-mode enhanced UDP min-packets

default flow-open-mode enhanced UDP min-packets

Syntax Description

number	The number of packets between opening a UPD flow. Range is 2—5.

Defaults

number = 2

Command Modes

Interface Linecard Configuration

Usage Guidelines

This command determines the number of packets from which a UDP flow is opened. For example, the default value of '2' means that a UDP flow will be opened for every second packet.

This command may be used when the SCE platform is very close to its performance envelop. Setting the threshold to a value higher than the default (2) will cause fewer UDP flows to be opened and thereby reduce the CPU utilization.

This command may have an impact on service classification and therefore should be used only after consulting with a Cisco technician.

Note The flow open mode must be set to *enhanced* (see the **flow-open-mode** command).

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>flow-open-mode enhanced
SCE(config if)#>flow-open-mode enhanced UDP min-packets 5
SCE(config if)#>
```

Related Commands

Command	Description
flow-open-mode	

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

When upgrading the application in a cascaded system, use this command to force failure in the active SCE 2000 platform (see 'System Upgrades' in the Chapter "Redundancy and Fail-Over" in the *Cisco Service Control Engine Software Configuration Guide*).

Authorization: admin

Examples

The following example forces a virtual failure condition.

At the displayed 'n', type 'Y' and press **Enter** to confirm the forced failure.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#force failure-condition
Forcing failure will cause a failover - do you want to continue? n
SCE(config if)#
```

Related Commands

Command	Description
pqi upgrade file	

global-controller

Configures the specified global controller.

global-controller *GC#* bandwidth *rate*

global-controller *GC#* name *GC_name*

Syntax Description

GC#	The number of the global controller (0-1023)
rate	Maximum rate in Kbps
GC_name	Logical name

Defaults

default rate = 1000000 (GigabitEthernet)

default GC_name = default

Command Modes

Interface GigabitEthernet Configuration

Usage Guidelines

Authorization: root

Examples

The following example shows how to configure the bandwidth for the specified global controller.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>Interface GigabitEthernet 0/1
SCE(config if)#>global-controller 375 bandwidth 1000
SCE(config if)#>
```

Related Commands

Command	Description
show interface global-controller	

handler name

Runs a specific handler with up to ten input parameters.

handler name ***handler-name*** **(global | default-party) [loops** ***num_of_loops*** **] [ppc** ***ppc-num*** **]**
[input-params
<value1>[<value2>[<value3>[<value4>[<value5>[<value6>[<value7>[<value8>[<value9>[
<value10>]]]]]]]]]]

handler name ***handler-name*** **party name** ***party-name*** **[loops** ***num_of_loops*** **] [ignore-output]**
[input-params
<value1>[<value2>[<value3>[<value4>[<value5>[<value6>[<value7>[<value8>[<value9>[
<value10>]]]]]]]]]]

Syntax Description

handler-name	Name of the handler to run.
value1-10	Up to ten input values
num_of_loops	Number of times to run the handler
ppc-num	Number of traffic processor on which to run the handler (global or default-party handlers only)
party-name	Name of party on which to run party handler (party handler only)
global	Keyword, global handler only
default-party	Keyword, default party handler only
ignore-output	Keyword, party handler only

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

The command options available for global or default party handlers differ slightly from those for a specific party handler.

- Use the **global** or **default-party** form of the command to run a global or default-party handler with up to ten input parameters, on a selected processor (showing handler output values, if any) or on all processors (ignoring handler output values).
- Use the **party name** form of the command to run a party handler with up to ten input parameters, on a selected party, optionally specifying that handler output values should be ignored.

The SML language allows the user to specify generic SML handlers in both party and global scope. The list of all such generic handlers, containing the name, scope and node offset of each handler, should be included in the XML section of the SLI file.

Input parameters are passed to the handlers by specifying up to ten values in the command that calls the handler. Output parameters are obtained by reading the content of global/party viewables after the handler is executed.

If the handler specifies output parameters, the Cmdl function returns only after the handler has executed and the results are known. If the handler specifies no output parameters, the Cmdl function returns immediately, enabling a high rate of such invocations.

Use the **loops** option to specify the number of times to run the handler.

For global and default party handlers, specify the traffic processor (**ppc** *ppc-num*) to enable receiving the output parameters.

If no traffic processor is specified, the handler executes on all traffic processors. This means that output parameters are not received, but the execution proceeds at a higher rate.

For party handlers, if there are no output parameters, use the **ignore-output** keyword. This also allows execution at a higher rate.

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to run a global handler with no output parameters. Since there are no output parameters, it is not necessary to specify a traffic processor to use. There are also no input parameters.

```
SCE>enable 15
Password:<cisco>
SCE#>handler name global-startup global
SCE#>
```

EXAMPLE 2

The following example illustrates how to run a default party handler. Since there are output parameters, it is necessary to specify a traffic processor to use.

```
SCE>enable 15
Password:<cisco>
SCE#>handler name quotaUpdate default-party ppc 1 input-params 0 1000
SCE#>
```

EXAMPLE 3

The following example illustrates how to run a specific party handler. There are no output parameters, so the **ignore-output** option is used for faster execution.

```
SCE>enable 15
Password:<cisco>
SCE#>handler name quotaUpdate party name subscriber_1 ignore-output input-params 0 1000
SCE#>
```

Related Commands

Command	Description
show applications slot handlers	

help

Displays information relating to all available CLI commands.

help bindings|tree

Syntax Description

This command has no arguments.

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-FMoves cursor one word to the right.
Esc-BMoves cursor one word to the left.
Ctrl-AMoves cursor to the start of the line.
Ctrl-EMoves cursor to the end of the line.
Esc F Moves cursor forward one word.
Esc BMoves cursor backward one word.
Editing
-------
Ctrl-DDeletes the character where the cursor is located.
Esc-DDeletes from the cursor position to the end of the word.
BackspaceDeletes the character before the current location of the cursor.
Ctrl-H Deletes the character before the current location of the cursor.
Ctrl-KDeletes from the cursor position to the end of the line.
Ctrl-UDeletes all characters from the cursor to the beginning of the line.
Ctrl-XDeletes all characters from the cursor to the beginning of the line.
Ctrl-WDeletes the word to the left of the cursor.
Ctrl-YRecall 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

Command	Description

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 examples illustrate how to use this command.

EXAMPLE 1

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

```
SCE>enable 10
Password:<cisco>
SCE#history
SCE#
```

EXAMPLE 2

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

```
SCE>enable 10
Password:<cisco>
SCE#no history
SCE#
```

Related Commands

Command	Description
history size	

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

size = 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>enable 10
Password:<cisco>
SCE#history size 50
SCE#
```

Related Commands

Command	Description
history	

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. Maximum length is 20 characters.

Defaults

host-name = **SCE**

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example changes the host name to MyHost.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#>hostname MyHost
MyHost(config)#>
```

Related Commands

Command	Description
show hostname	

hosts aging-timeout

Sets the hosts aging timeout. Use the **default** form of the command to reset the aging timeout to the default value.

hosts aging-timeout ***timeout***

default hosts aging-timeout

Syntax Description

timeout	The amount of time after which the hosts will timeout, in seconds.

Defaults

timeout = 600 Seconds

Command Modes

Interface Linecard Configuration

Usage Guidelines

The specified aging timeout value takes effect only after (unloading and) loading an application.

The hosts are actually terminated within one minute after the specified timeout has expired.

The **default** form of the command resets the timeout to the default value of 600 seconds.

Authorization: root

Examples

The following example illustrates how to set the host aging timeout to 300 seconds.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE (config if)#>hosts aging-timeout 300
SCE(config if)#>
```

Related Commands

Command	Description
hosts max-hosts	
show interface linecard hosts info	

hosts max-hosts

Defines the maximum number of hosts in the host context database.

hosts max-hosts*max-hosts*

default hosts max-hosts

Syntax Description

max-hosts	The maximum number of hosts in the host context database. This value must be greater than 100.

Defaults

max-hosts= 50,000

Command Modes

Interface Linecard Configuration

Usage Guidelines

The specified aging maximum hosts value takes effect only after (unloading and) loading an application.

The **default** form of the command resets the maximum hosts to the default value of 50,000.

Authorization: root

Examples

The following example illustrates how to set the maximum number of hosts to 60,000.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE (config if)#>hosts max-hosts 60000
SCE(config if)#>
```

Related Commands

Command	Description
hosts aging-timeout	
show interface linecard hosts info	

interface gigabitethernet

Enters GigabitEthernet Interface Configuration mode to configure a specified Gigabit Ethernet line interface. To configure a management port, use the **interface mng** command.

interface gigabitethernet ***slot-number/interface-number***

Syntax Description

slot-number	Enter a value of *0*.
interface-number	The GigabitEthernet line interface number. • SCE 2000 4xGBE platform: Enter a value between **1** and **4** • SCE 1000 2xGBE platform: Enter a value of either **1** or **2**

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use this command to configure the line ports for an SCE 2000 4xGBE or SCE 1000 2xGBE platform. This command is not used for configuring the management ports.

To return to the Global Configuration Mode, use the **exit** command.

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

The system prompt changes to reflect the GigabitEthernet Interface Configuration mode.

Authorization: admin

Examples

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface gigabitethernet 0/1
SCE(config if)#
```

Related Commands

Command	Description
interface mng	
exit	
end	
show interface gigabitethernet	

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, use the **exit** command.

Authorization: admin

Examples

The following example enters LineCard Interface Configuration Mode.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#
```

Related Commands

Command	Description
exit	

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, use the **exit** command.

Authorization: admin

Examples

The following example enters into Management Interface Configure Interface Mode.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface mng 0/1
SCE(config if)#
```

Related Commands

Command	Description
exit	
show interface mng	
duplex	
speed	

interface range gigabitethernet

Enters GigabitEthernet Interface Configuration mode for two or more GBE line interfaces.

interface range gigabitethernet ***slot-number/interface-range***

Syntax Description

slot-number	Enter a value of *0*.
interface-range	Specify the range of ports in the format '*port1-port2*', where the overall range of possible port numbers is as follows: • SCE 2000: 1-4 • SCE 1000: 1-2

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The **interface range** command allows you to perform a CLI operation on a group of interfaces with one command, with the limitation that all the interfaces in the group must be of the same physical and logical type.

- To return to the Global Configuration Mode, use the **exit** command.
- To return to the Use Exec authorization level, use the **end** command.

The system prompt changes to reflect the GigabitEthernet Interface Configuration mode.

The following commands will be executed on all interfaces specified in the **interface range gigabitethernet** command as long as you remain in the GigabitEthernet Interface Configuration mode:

- **auto-negotiate**
- **global-controller bandwidth**
- **global-controller name**

Authorization: admin

Examples

The following example enters the GigabitEthernet Interface Configuration mode to configure all traffic interfaces on an SCE 2000 platform.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface range gigabitethernet 0/1-4
SCE(config if range)#
```

Related CommandsE

Command	Description
exit	
show interface gigabitethernet	
interface gigabitethernet	

ip access-class

Specifies which access control list (ACL) controls global access to the SCE platform. Use the **no** form of the command to permit global access to the SCE platform from any IP address.

ip access-class*number*

no ip access-class

Syntax Description

number	The number of the access list (1–99) to use to allow global access to the SCE platform.

Defaults

none (all IP addresses can access the system)

Command Modes

Global Configuration

Usage Guidelines

The ACL specified in this command contains the definitions for all IP addresses with permission to access the SCE platform. IP addresses not permitted in this access list cannot access or detect the SCE platform; even a **ping** command will receive no response if it is not from a permitted IP address.

Authorization: admin

Examples

The following example sets access list 1 as the global ACL.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip access-class 1
SCE(config)#
```

Related Commands

Command	Description
access-list	
show access-lists	

ip address

Sets the IP address and subnet mask of the 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

Mng Interface Configuration

Usage Guidelines

When both management ports are connected, only one port is active at any given time, while the second management port provides a redundant management interface. In this case, the configured IP address acts as a virtual IP address for the currently active management interface, regardless of which port is the active port.

Since this IP address always acts as a virtual IP address for the currently active management port, this command can be executed from the Mng Interface Configuration for either management port.

Note Changing the IP address of the management interface via telnet will result in loss of the telnet connection and inability to reconnect with the interface.

Note After changing the IP address, you must reload the SCE platform (see **reload**) so that the change will take effect properly in all internal and external components of the SCE platform.

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

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface mng 0/1
SCE(config if)#ip address 10.1.1.1 255.255.0.0 SCE(config if)#
```

Related Commands

Command	Description
interface Mng	

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 [destination | interval]

Syntax Description

destination	The IP address of the destination for the ping requests
interval	The frequency of the ping requests in seconds

Defaults

By default, IP advertising is 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 this command.

EXAMPLE 1:

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

```
SCE>enable 10
Password:<cisco>
SCE#config
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>enable 10
Password:<cisco>
SCE#config
SCE(config)#default ip advertising destination
SCE(config)#
```

Related Commands

Command	Description
show ip advertising	

ip default-gateway

Configures the default gateway for the SCE platform. Use the**no** form of this command to remove the SCE platform default gateway configuration

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

no ip default-gateway

Syntax Description

x.x.x.x	The IP address of the default gateway for the SCE platform.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example sets the default gateway IP of the SCE platform to 10.1.1.1.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip default-gateway 10.1.1.1
SCE(config)#
```

Related Commands

Command	Description
show ip default-gateway	

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

By default, domain name lookup is enabled.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate how to use this command.

EXAMPLE 1:

The following example enables the domain lookup.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip domain-lookup SCE(config)#
```

EXAMPLE 2:

The following example disables the domain lookup

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no ip domain-lookup
SCE(config)#
```

Related Commands

Command	Description
ip domain-name	
ip name-server	
show hosts	

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

domain-name	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 this command.

EXAMPLE 1:

The following example configures a domain name

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip domain-name cisco.com
SCE(config)#
```

EXAMPLE 2:

The following example removes the configured domain name.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no ip domain-name
SCE(config)#
```

Related Commands

Command	Description
ip domain-lookup	
ip name-server	
show hosts	

ip filter fragment

Use this command to enable 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

Management security is defined as the capability of the SCE platform to cope with malicious management conditions that might lead to global service failure.

There are two parallel security mechanisms:

- Automatic security mechanism — monitors the TCP/IP stack rate at 200 msec intervals and throttles the rate from the device if necessary.
- User-configurable security mechanism — accomplished via two IP filters at user-configurable intervals:
  - IP fragment filter: Drops all IP fragment packets

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

  Use the **ip filter moniter** command to configure the IP filter monitor.

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

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

Authorization: admin

Examples

The following example shows how to enable IP fragment filtering.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip filter fragment enable
SCE(config)#
```

Related Commands

Command	Description
ip filter moniter	
show ip filter	

ip filter monitor

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

ip filter monitor [ip_permited | ip_not_permited] low_rate *low_rate* high_rate *high_rate* burst *burst size*

Syntax Description

low_rate	Lower threshold; the rate in Mbps that indicates the attack is no longer present
high_rate	Upper threshold; the rate in Mbps that indicates the presence of an attack
burst size	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

Defaults

low rate = 20 Mbps

high rate = 20 Mbps

burst size = 10 seconds

Command Modes

Global Configuration

Usage Guidelines

Management security is defined as the capability of the SCE platform to cope with malicious management conditions that might lead to global service failure.

There are two parallel security mechanisms:

- Automatic security mechanism — monitors the TCP/IP stack rate at 200 msec intervals and throttles the rate from the device if necessary.
- User-configurable security mechanism — accomplished via two IP filters at user-configurable intervals:
  - IP fragment filter: Drops all IP fragment packets

  Use the **ip filter fragment** command to enable the IP fragment filter.
  - IP filter monitor: Measures the rate of accepted and dropped packets for both permitted and not-permitted IP addresses.

  This command configures the IP filter monitor.

Use the **ip permitted** keyword to apply configured limits to permitted IP addresses.

Use the **ip not-permitted** keyword to apply configured limits to not-permitted IP addresses.

If neither keyword is used, it is assumed that the configured limits apply to both permitted and not-permitted IP addresses.

Authorization: admin

Examples

The following example shows how to configure the rates for permitted IP addresses.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# ip filter monitor ip permitted low_rate 25 high_rate 30 burst 15
SCE(config)#
```

Related Commands

Command	Description
ip filter fragment	
show ip filter	

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>enable 10
Password:<cisco>
SCE#ip ftp password mypw
SCE#
```

Related Commands

Command	Description
copy ftp://	
copy-passive	
ip ftp username	

ip ftp-server

Enables the ftp server and configures the ports for the FTP server. Use the **default** form of the command to revert to the specified default port setting.

ip ftp-server {(passive-port-range max *max_port#* min *min_port#*) | port *port#* }

default ip ftp-server {passive-port-range | port}

Syntax Description

max_port#	Highest port number of the range of ports assigned to passive FTP
min_port#	Lowest port number of the range of ports assigned to passive FTP
port#	FTP port number (not passive)

Defaults

port# = 21000

Command Modes

Global Configuration

Usage Guidelines

The following options are available

- **passive-port-range** — assign a minimum and a maximum port number to define the range of ports used by passive FTP.

  Use the **default** command to remove the port range configuration.
- **port** — assign the port number for FTP (not passive).

  Use the **default** command to revert to the default FTP port.

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>ip ftp-server passive-port-range max 150 min 115
SCE(config)#>
```

Related Commands

Command	Description
show ip (ROOT level options)	

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>enable 10
Password:<cisco>
SCE#ip ftp username myname
SCE#
```

Related Commands

Command	Description
copy ftp://	
copy-passive	
ip ftp password	

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 or removed.
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>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip host PC85 10.1.1.1
SCE(config)#
```

Related Commands

Command	Description
show hosts	

ip http-tech-if

Enables and configures the HTTP adaptor. Use the**no** form of the command to disable the HTTP adaptor. Use the**default** form of the command to revert to the default HTTP adaptor port setting.

ip http-tech-if [port *port#*]

no ip http-tech-if

default ip http-tech-if port

Syntax Description

port#	HTTP adaptor port number

Defaults

port# = 8082

Command Modes

Global Configuration

Usage Guidelines

The following options are available

- **ip http-tech-if** — enables the HTTP adaptor
- **no ip http-tech-if** — disables the HTTP adaptor
- **ip http-tech-if port** — assigns the HTTP adaptor port
- **default ip http-tech-if port** — assigns the default port (port 8082) to the HTTP adaptor

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>ip http-tech-if port 100
SCE(config)#>
```

Related Commands

Command	Description
show ip (ROOT level options)	

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 10.1.1.1 and 10.1.1.2 to the configured servers list.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip name-server 10.1.1.1 10.1.1.2
SCE(config)#
```

Related Commands

Command	Description
ip domain-lookup	
show hosts	

ip radius-client retry limit

Configures the parameters for retransmitting unacknowledged RADIUS client messages.

ip radius-client retry limit ***times*** **[timeout** ***timeout*** **]**

Syntax Description

times	The maximum number of times the RADIUS client can try unsuccessfully to send a message.
timeout	Timeout interval for retransmitting a message, in seconds

Defaults

times = 3

timeout = 5 second

Command Modes

Global Configuration

Usage Guidelines

Due to the unreliable nature of UDP, the RADIUS client retransmits requests to the SCMP peer device if they were not acknowledged within the configured number of seconds. Messages that were not acknowledged can be retransmitted up to the configured maximum number of retries.

The optional timeout parameter limits the time interval for retransmitting a message.

Authorization: admin

Examples

The following example illustrates how to configure the retransmission parameters.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# ip radius-client retry limit 5 timeout 5
SCE(config)#
```

Related Commands

Command	Description
scmp name	
show ip radius-client	

ip route

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

ip route ***ip-address mask [next-hop]***

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

no ip route all

Syntax Description

ip-address	The IP address of the new entry.
mask	The relevant subnet mask.
next-hop	The 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 this command:

EXAMPLE 1:

The following example sets the next-hop to 20.2.2.2 for IP addresses in the range 10.10.10.0 to 10.10.10.255.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip route 10.10.10.0 255.255.255.0 20.2.2.2
SCE(config)#
```

EXAMPLE 2:

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no ip route 10.10.10.0 255.255.255.0 S
CE(config)#
```

Related Commands

Command	Description
show ip route	

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 this command.

EXAMPLE 1:

The following example enables the RPC adapter.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip rpc-adapter
SCE(config)#
```

EXAMPLE 2:

The following example disables the RPC adapter.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no ip rpc-adapter
SCE(config)#
```

Related Commands

Command	Description
ip rpc-adapter port	
show ip rpc-adapter	
ip rpc-adaptor security-level	

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

port number = 14374

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following examples illustrate the use of this command:

EXAMPLE 1:

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

```
SCE>enable 10
Password:<cisco>
SCE#config
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>enable 10
Password:<cisco>
SCE#config
SCE(config)#default ip rpc-adapter port
```

Related Commands

Command	Description
ip rpc-adapter	
show ip rpc-adapter	

ip rpc-adaptor security-level

Sets the PRPC server security level.

ip rpc-adaptor security-level {full|semi|none}

Syntax Description

	full, semi, none

Defaults

default = semi

Command Modes

Global Configuration

Usage Guidelines

Specify the desired PRPC server security level:

- **full** : all PRPC connections require authentication
- **semi** : PRPC connections that supply a user-name and password during connection establishment are authenticated. Connections that do not supply a user-name and password are accepted with no authentication
- **none** : no authentication is performed

Authorization: admin

Examples

The following example illustrates how to set the PRPC server security level.

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE(config)#ip rpc-adaptor security-level full
SCE>
```

Related Commands

Command	Description
ip rpc-adapter	
show ip rpc-adapter	

ip ssh

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

ip ssh [SSHv1]

no ip ssh [SSHv1]

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

If the SSHv1 keyword is not specified, both SSHV1 and SSHv2 are enabled. If you wish to enable only SSHv2, use the **no** form of the command to disable SSHv1, as explained in Example 3. Use the **ip ssh SSHv1** command to re-enable SSHv1.

When using an SSH server, you should also do the following:

- Generate an SSH key set (**ip ssh key** command). A set of keys must be generated at least once before enabling the SSH server
- Assign an ACL to the SSH server (**ip ssh access-class** command)

Authorization: admin

Examples

The following examples illustrate the use of this command:

EXAMPLE 1:

The following example enables the SSH server. Both SSHV1 and SSHv2 are enabled.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip ssh
SCE(config)#
```

EXAMPLE 2:

The following example disables the SSH server.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no ip ssh
SCE(config)#
```

EXAMPLE 3:

The following example shows how to disable SSHv1 so that only SSHv2 is enabled.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip ssh
SCE(config)#no ip ssh SSHv1
SCE(config)#
```

Related Commands

Command	Description
ip ssh access-class	
ip ssh key	
show ip ssh	

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 **access-list**.) Use the **no** option 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

When using an SSH server, you should also do the following:

- Enable the SSH server (**ip ssh** command).
- Generate an SSH key set (**ip ssh key** command).

Authorization: admin

Examples

The following examples illustrate how to use this command.

EXAMPLE 1:

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip ssh access-class 4
SCE(config)#
```

EXAMPLE 2:

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no ip ssh access-class
SCE(config)#
```

Related Commands

Command	Description
ip ssh	

ip ssh key
show ip ssh

ip ssh key

Generates or removes the SSH key set. A set of keys must be generated at least once before enabling the SSH server.

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

Each SSH server should define a set of keys (DSA2, RSA2 and RSA1) to be used when communicating with various clients. The key sets are pairs of public and private keys. The server publishes the public key while keeping the private key in non-volatile memory, never transmitting it to SSH clients.

Note that the keys are kept on the *tffs0* file system, which means that a person with knowledge of the ' *enable* ' password can access both the private and public keys. The SSH server implementation provides protection against eavesdroppers who can monitor the management communication channels of the SCE platform, but it does not provide protection against a user with knowledge of the ' *enable'* password.

When using an SSH server, you should also do the following:

- Enable the SSH server (**ip ssh** command).
- Assign an ACL to the SSH server (**ip ssh access-class** command).

Authorization: admin

Examples

The following examples illustrate how to use this command.

EXAMPLE 1:

The following example generates a new SSH key set.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip ssh key generate
SCE(config)#
```

EXAMPLE 2:

The following example removes the SSH key set,

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#ip ssh key remove
SCE(config)#
```

Related Commands

Command	Description
ip ssh	
ip ssh access-class	
show ip ssh	

ip-tunnel IPinIP DSCP-marking-skip

Configures the SCE platform to perform DSCP marking on the internal IP header of IPinIP traffic.

Use the **no** form of the command to perform DSCP marking on the external IP header.

ip-tunnel IPinIP DSCP-marking-skip

no ip-tunnel IPinIP DSCP-marking-skip

Syntax Description

This command has no arguments or keywords.

Defaults

By default, DSCP marking of IPinIP traffic is done on the external IP header (**no** form of the command).

Command Modes

Interface Linecard Configuration

Usage Guidelines

DSCP marking modifies the DSCP bits of the IPv4 header. In IPinIP tunnels there are at least two IP headers. By default, DSCP marking is performed only on the external IP header. Use this command to mark the DSCP bits of the internal IP header.

This command takes effect only when **IPinIP skip** is enabled (see the **ip-tunnel IPinIP skip** command).

Note DSCP marking should be enabled and configured through SCA BB console. Refer to the section "How to Manage DSCP ToS Marker Values" in the chapter "Using the Service Configuration Editor: Traffic Control" in the *Cisco Service Control Application for Broadband User Guide* for further information.

Authorization: admin

Examples

The following example shows how to configure the SCE platform to perform DSCP marking on the internal IP header of an IPinIP flows.

```
SCE>enable 10
Password:<cisco>
SCE# configure
SCE(config)#interface linecard 0
SCE(config if)#>ip-tunnel IPinIP DSCP-marking-skip
```

ip-tunnel IPinIP skip

Enables the recognition of IPinIP tunnels and skipping into the internal IP packet. Use the **no** form of this command to disable IPinIP skip.

ip-tunnel IPinIP skip

no ip-tunnel IPinIP skip

Syntax Description

This command has no arguments or keywords.

Defaults

By default, IPinIP skip is disabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

- IPinIP and other tunnels: IPinIP is supported simultaneously with plain IP traffic and any other tunneling protocol supported by the SCE platform.
- Overlapping IP addresses: There is no support for overlapping IP addresses within different IPinIP tunnels.
- DSCP marking: For IPinIP traffic, DSCP marking can be done on either the external or the internal IP header exclusively.

  See the **ip-tunnel IPinIP DSCP-marking-skip** command.

Authorization: admin

Examples

The following example shows how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE# configure
SCE(config)#interface linecard 0
SCE(config if)#>ip-tunnel IPinIP skip
```

Related Commands

Command	Description
ip-tunnel IPinIP DSCP-marking-skip	
show interface linecard ip-tunnel IPinIP	

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 and classify traffic by the external IP address.

ip tunnel L2TP skip

no ip tunnel

Syntax Description

This command has no arguments or keywords.

Defaults

By default, IP tunnel recognition is disabled.

Command Modes

Linecard Interface Configuration

Usage Guidelines

L2TP is an IP-based tunneling protocol. Therefore, the system must be specifically configured to recognize the L2TP flows, given the UDP port used for L2TP. The SCE platform can then skip the external IP, UDP, and L2TP headers, reaching the internal IP, which is the actual subscriber traffic. If L2TP is not configured, the system treats the external IP header as the subscriber traffic, thus all the flows in the tunnel are seen as a single flow.

The IP tunnel mode is mutually exclusive with other MPLS- or VLAN-based classification.

Use the **L2TP identify-by** command to configure the port number that the LNS and LAC use for L2TP tunnels.

Authorization: admin

Examples

The following example enables recognition of L2TP tunnels.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#ip tunnel L2TP skip
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard ip-tunnel	
L2TP identify-by	
MPLS	
VLAN	

jvm input-string

Sets the input string argument for the jvm.

jvm input-string ***input-string*** **[cold-start|warm-start]**

no jvm input-string input-string [cold-start|warm-start|all]

Syntax Description

input-string	Specify the input string to use. Specify whether to set or reset (to default) the *cold-start* or *warm-start* input string. The *all* option is available only with the **no** form (reset to default) of the command.

Defaults

Default input string for warm-start = *Dcom.pcube.WarmStart StartSE*

Default input string for cold-start = *StartSE*

Command Modes

Global Configuration

Usage Guidelines

ROOT users can disable and enable the management agent. However, without special handling, this results in the loss of the management agent configuration. In order for the management agent to preserve its configuration in such a situation, it must be able to differentiate between a normal startup that is part of a normal boot process (cold-start) and a startup initiated by the user (warm-start). This is accomplished by using a unique input string for each type of startup, resulting in the use of the appropriate configuration file.

When shutting down, the management agent saves its current configuration to a file. During warm start, it reads this file to restore the last known configuration. During cold start, it does not read this file, but instead relies on the last configuration exported to the embedded config.txt file.

This solution has the following advantages:

- During cold-start, the *config.txt* file is the only source of configuration commands.
- During warm-start (which is a ROOT-only feature), the management agent configuration is automatically preserved.

If no keyword is included, the warm-start jvm input string is set or reset.

Use the **no** form of the command to reset the input string for the specified option (cold-start, warm-start, or both) to the default input string.

Authorization: root

Examples

The following example illustrates how reset both cold-start and warm-start input strings to the default.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>no jvm input-string all
SCE(config)#>
```

Related Commands

Command	Description
service management-agent	
show jvm	

l2tp identify-by

Configures the port number that the LNS and LAC use for L2TP tunnels.

l2tp identify-by port-number ***port-number***

l2tp identify-by default port

Syntax Description

port-number	The port number to be configured for L2TP tunnels.

Defaults

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.

Note that if external fragmentation exists in the L2TP environment, it is required to configure a *quick-forwarding-ignore* Traffic Rule (see the section "Configuring Traffic Rules and Counters" in the *Cisco SCE Software Configuration Guide*) that bypasses all IP traffic targeted to either the LNS or LAC IP address. This will make sure that any packets not having the L2TP port indication (i.e. non-first fragments) will not require handling by the traffic processors.

In addition, in order to prevent reordering of L2TP tunneled fragments, it is advised to define a *quick-forwarding* traffic-rule for all the L2TP traffic. This can be done based on the IP ranges in use by the internal IPs in the tunnel (as allocated by the LNS), or simply for all of the traffic passing through the SCE platform.

Note that flow redirection and flow blocking cannot be performed on the quick-forwarded traffic.

Authorization: admin

Examples

The following example configures port# 1000 as the L2TP port.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#l2tp identify-by port-number 1000
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard l2tp	
ip tunnel	

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, use the **exit** command.

Authorization: admin

Examples

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

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#line vty 0
SCE(config-line)#
```

Related Commands

Command	Description
show line vty	
exit	

link failure-reflection

Enables/disables the link failure reflection.

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

no link failure-reflection [linecard-aware]

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** 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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#link failure-reflection on-all-ports S
CE(config if)#
```

link mode

Configures the link mode. The link mode allows the user to force the specified behavior on the link. This may be useful during installation and for debugging the network.

link mode ***link mode***

Syntax Description

link	Use this parameter for SCE 2000 platforms only • GBE: – **GBE1-GBE2** – **GBE3-GBE4** • FE: – **LINK1** – **LINK2** • **all-links**
mode	• **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** mode 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.

```
SCE2000GBE>enable 10
Password:<cisco>
SCE2000GBE#config
```

```
SCE2000GBE(config)#interface linecard 0
SCE2000GBE(config if)#link mode GBE1-GBE2 bypass
SCE2000GBE(config if)#
```

EXAMPLE 2:

The following example configures "forwarding" as the link mode for the SCE 1000 GBE platform.

```
SCE1000GBE>enable 10
Password:<cisco>
SCE1000GBE#config
SCE1000GBE(config)#interface linecard 0
SCE1000GBE(config if)#link mode forwarding
SCE1000GBE(config if)#
```

EXAMPLE 3:

The following example configures "sniffing" as the link mode on all links for the SCE 2000 GBE platform.

```
SCE2000GBE>enable 10
Password:<cisco>
SCE2000GBE#config
SCE2000GBE(config)#interface linecard 0
SCE2000GBE(config if)#link mode all-links sniffing
SCE2000GBE(config if)#
```

Related Commands

Command	Description
show interface linecard link mode	

logger (ROOT level options)

Performs the specified operation on the debug log file.

logger add-dbg-message*message-text*

logger add-sce-agent-log-message ***message-text***

logger get debug-log file-name ***target-file***

Syntax Description

message-text	Text of the message to write to the debug log file
target-file	Name of the output file. Can be any of the following filename types: • local • full path • host ftp • full ftp path

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The following operations can be performed on the debug log file:

- **add-dbg-message** — Adds a message to the file
- **add-sce-agent-log-message** — Adds a message to the SCE agent log file
- **get debug-log** — Outputs the current debug log to a target file

For information concerning operations on the user log file, see the following commands:

- **logger add-user-message**
- **logger get user-log file-name**

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to retrieve the current debug log file:

```
SCE>enable 15
Password:<cisco>
SCE#>logger get debug-log file-name ftp://myname:mypw@10.1.1.205/d:/log.txt
SCE#>
```

EXAMPLE 2

The following example illustrates how to add "testing 123" as the message to the debug log file:

```
SCE>enable 15
Password:<cisco>
SCE#>logger add-dbg-message testing 123
SCE#>
```

Related Commands

Command	Description
logger add-user-message	
logger get user-log file-name	

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>enable 10
Password:<cisco>
SCE#logger add-user-message testing 123
SCE#
```

Related Commands

Command	Description
logger (ROOT level options)	

logger device

Disables or enables the specified logger device.

logger device {line-attack-file-log | statistics-file-log | user-file-log} ***status***

Syntax Description

status	**enabled** or **disabled,** indicating whether to turn on or off logging.

Defaults

By default, the log devices are enabled.

Command Modes

Global Configuration

Usage Guidelines

Available logger devices are:

- Line-Attack-File-Log
- SCE-agent-Statistics-Log
- User-File-Log

Authorization: admin

Examples

The following example disables the User-File-Log device.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#logger device user-file-log disabled
SCE(config)#
```

Related Commands

Command	Description
logger device user-file-log max-file-size	
logger get user-log file-name	
clear logger	
logger device (ROOT level options)	

logger device (ROOT level options)

logger device {debug-file-log | line-attack-file-log | statistics-file-log | statistics-archive-file-log | sce-agent statistics-log | user-file-log} enabled

logger device {debug-file-log | line-attack-file-log | statistics-file-log | statistics-archive-file-log | sce-agent statistics-log | user-file-log} disabled

logger device {debug-file-log | line-attack-file-log | statistics-file-log | statistics-archive-file-log | sce-agent statistics-log | user-file-log} max-file-size *size*

logger device debug-file-log min-severity {fatal | error | warning | info}

logger device debug-file-log module *module-number*

logger device sce-agent-debug-log category *category-name* {clear | priority {debug | info | warn | error | fatal}}

logger device statistics-archive-file-log message-timeout *timeout*

Syntax Description

size	Maximum size of the log file in bytes.
module-number	Number of the module to log (in HEX). To log all modules, use '0xffff'.
category-name	Name of the category to clear priority or set new priority
timeout	The time period between archiving of the same message, in seconds

Defaults

By default, all logger devices are enabled.

default for SCE-agent-Debug-Log category = warning

default min-severity for the Debug-File-Log = warning

default file sizes:

- debug log file = 4 MB
- statistics log file = 19MB
- archive statistics log file = 3MB

Global Configuration

Command Modes

Global Configuration

Usage Guidelines

Available logger devices are:

- Debug-File-Log
- SCE-agent-Debug-Log
- Statistics-File-Log

- Statistics-Archive-File-Log
- SCE-agent Statistics-Log (Available at Admin authorization level. See **logger device**)
- User-File-Log (Available at Admin authorization level. See **logger device**)
- Line-Attack-File-Log (Available at Admin authorization level. See **logger device**)

The following types of information can be configured for the logger devices:

- status (enabled or disabled)
- module (debug devices only): Logged module. Set the module ID to be logged. The device can either log a specific module by ID or all modules. Module ID is in hex, for all modules use 0xffff..
- min-severity: Minimum logged severity level (fatal, error, warning, info). This option sets the severity of the messages that are logged. In general, 'info' messages are not logged for debug. Selecting a lower severity level impacts performance.
- max-file-size: Maximum size of the specified log file in binary form in bytes. This option limits the binary log file only; it has no effect on the size of the interpreted output file.
- category clear/priority: Clear (set to default) or set the minimum severity level for the specified category that will be logged to the SCE-agent-Debug-Log (fatal, error, warning, info, debug)
- message timeout: The time period between archiving of the same message in seconds

The configurable options available for the various logger devices vary somewhat. Refer to the following table for a summary of what options can be configured for each logger device.

Table 2-2 Logger Device Configuration Options

Logger Device	Configuration Options
Debug-File-Log	status, module, min-severity, max-file-size
Statistics-File-Log	
Statistics-Archive-File-Log	status, status, max-file-sizemax-file-size, message timeout
SCE-agent-Debug-Log	category clear/priority

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to configure the maximum file size for the Statistics-Archive-File-Log.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>logger device statistics-archive-file-log max-file-size 8000000 S
CE(config)#>
```

EXAMPLE 2

The following example illustrates how to set the minimum severity level for category "Category1" to be logged to the SCE-agent-Debug-Log.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>logger device sce-agent-debug-log category category1 priority info
SCE(config)#>
```

Related Commands

Command	Description
logger device	
logger device User-File-Log max-file-size	

logger device user-file-log max-file-size

Sets the maximum log file size.

logger device User-File-Log max-file-size ***size***

Syntax Description

size	The maximum size for the user log (in bytes).

Defaults

size = 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>enable 10
Password:<cisco>
SCE#config
SCE(config)#logger device user-file-log max-file-size 65000
SCE(config)#
```

Related Commands

Command	Description
logger device	
show logger device	

logger get support-file

Generates a log file for technical support via FTP. Note that this operation may take some time.

logger get support-file *filename*

Syntax Description

filename	Name of the generated log file. The specified file must be located on an FTP site, not on the local file system.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example generates a technical support log file (via FTP) named *support.zip*.

```
SCE>enable 10
Password:<cisco>
SCE#logger get support-file ftp://user:1234@10.10.10.10/c:/support.zip
SCE#
```

Related Commands

Command	Description

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 name of the output file to which 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>enable 10
Password:<cisco>
SCE#logger get user-log file-name ftp://myname:mypw@10.1.1.205/d:/log.txt
SCE#
```

Related Commands

Command	Description
logger get support-file	

logger track flows

Specifies the subscriber and service to track and for which to generate debug information and starts flow tracking for the specified flows. Use the **no** form of the command to terminate flow tracking currently in progress.

logger track flows [subscriber name *name* | subscriber IP-Range *range*] { signature-id*id* | (protocol *protocol-name* min-port *min-port#* max-port *max-port#*)} [stop-after *number*]

logger track flows any [stop-after *number*]

no logger flow-tracking

Syntax Description

name	Name of the subscriber to be tracked.
range	IP range that defines an anonymous subscriber to be tracked.
id	The signature ID of the service to be tracked.
protocol-name	The name of the protocol to be tracked. The port number range must also be defined (min-port and max-port)
min-port#	Lowest port number of the range of port numbers that defines the protocol.
max-port#	Highest port number of the range of port numbers that defines the protocol.
number	Number of flows to track.

Defaults

stop-after number = 1

Command Modes

Global Configuration

Usage Guidelines

This command allows a network administrator to define a specific problematic area (a subscriber-service combination). The system will then track flows fitting that particular definition and generate debug information for these flows. The information gathered is written to the debug log. This provides the network administrator with specific problem-solving information when service to a particular subscriber or for a particular service in unsatisfactory.

The flows to be tracked are described by two general parameters:

- subscriber (optional) — The subscriber specification is not required. The flow to be tracked may be defined by the relevant service only.

  A subscriber can be defined in one of two ways:

  - subscriber name — the name of a specific subscriber (subscriber-aware mode)
  - IP address range — range of subscriber IP addresses (anonymous subscriber mode)
- Service (required) — The service specification is required. (See the *Cisco SCA BB Protocol Reference Guide* for signature IDs, protocol names and port ranges.)

  A service can be defined in one of two ways:

  - signature ID — the signature ID of the service

- protocol — the protocol name and port range (minimum port number and maximum port number)

Possible legal subscriber/service formats are as follows:

logger track flows subscriber *name* name signature-id *id*

logger track flows subscriber name *name* protocol *protocol-name* min-port *min-port#* max-port *max-port#*

logger track flows subscriber IP-Range *range* signature-id *id*

logger track flows subscriber IP-Range *range* protocol *protocol-name* min-port *min-port#* max-port *max-port#*

logger track flows signature-id *id*

logger track flows protocol *protocol-name* min-port *min-port#* max-port *max-port#*

Use the stop-after option to specify how many flows to track. Flow tracking will then stop after the specified number of flows. If this option is not specified, flow tracking will continue until a **no logger flow-tracking** command is executed.

Use the **any** keyword to track all flows.

Note that you cannot issue a new flow tracking command while flow tracking is currently in progress. You must either wait for the current flow tracking to end or execute a **no logger flow-tracking** command.

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>logger track flows subscriber name John Smith protocol MSN Messenger min-port
1863 max-port 1863 stop-after 5 S
CE(config)#>
```

Related Commands

Command	Description
show logger flow-tracking	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#exit
SCE>logout
Connection closed by foreign host.
```

Related Commands

Command	Description

lookup

Performs the specified operation on the specified lookup table to add or remove entries.

lookup ***lookup-name*** **insert-key** ***key*** **value** ***value***

lookup ***lookup-name*** **replace-key** ***key*** **value** ***value***

lookup ***lookup-name*** **overwrite-key** ***key*** **value** ***value***

lookup ***lookup-name*** **remove-key** ***key***

lookup ***lookup-name*** **remove-all**

Syntax Description

lookup-name	Table lookup name.
key	Specific key to perform the operation on (insert, remove, etc.). Keys have the following characteristics: • permitted formats: string, uint32, int32 • case sensitive • can be exact or include a wildcard ('*') • use \char to declare the character after the slash to be literal. For example, to define a slash, use \\
value	Value to assign to the specified key.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

The **lookup** command can be used to assist in updating certain lookup tables used by the application for various purposes, such as classification. You can execute this command either manually or by automated scripts.

The following operations are available:

- **insert-key** — If the specified key is not currently in the table, inserts both the key and the specified value.
- **replace-key** — If the specified key is currently in the table, replaces the current value with the specified value.
- **overwrite-key** — Inserts both the specified key and the specified value, regardless of whether the key is currently in the table or not.
- **remove-key** — Removes the specified key with its value.
- **remove-all** — Removes all keys from table.

Before using this option, you should know the name of the lookup table as given by the application and its format (use the **show applications slot lookup** command).

Lookups can be defined in one of the following formats:

- Suffix string lookup
- Prefix string lookup
- Suffix_prefix string lookup

Make sure the key format is appropriate for the lookup type.

Authorization: root

Examples

The following example shows how to use this command. The output of the **show** commands demonstrates the difference between insert, replace, and overwrite.

Note that when the **replace** option is used for a key that does not exist, an error message appears.

Both the **insert** and the **overwrite** options can be used successfully with keys that do not exist.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>show applications slot 0 lookup StreamingUserAgentsList all-key
Table keys and values:
key = Windows-Media-Player
value = 0
key = RealPlayer
value = 0
SCE(config if)#>lookup StreamingUserAgentsList replace-key QuickTime value 0
Error - Key 'QuickTime' not found.More info: in func 'CmdlLut::replaceCfg',
lutName='PL_StreamingUserAgentsList', key='QuickTime', value='0'..
SCE(config if)#>lookup StreamingUserAgentsList insert-key QuickTime value 0
SCE(config if)#>show applications slot 0 lookup StreamingUserAgentsList all-key
Table keys and values:
key = Windows-Media-Player
value = 0
key = QuickTime
value = 0
key = RealPlayer
value = 0
SCE(config if)#>lookup StreamingUserAgentsList replace-key QuickTime value 1
SCE(config if)#>show applications slot 0 lookup StreamingUserAgentsList all-key
Table keys and values:
key = Windows-Media-Player
value = 0
key = QuickTime
value = 1
key = RealPlayer
value = 0
SCE(config if)#>lookup StreamingUserAgentsList overwrite-key Nullsoft value 1
SCE(config if)#>show applications slot 0 lookup StreamingUserAgentsList all-key
Table keys and values:
key = Windows-Media-Player
value = 0
key = Nullsoft
value = 1
key = QuickTime
value = 1
key = RealPlayer
value = 0
SCE(config if)#>
```

Related Commands

Command	Description
show applications slot lookup	

mac-resolver

Enables the MAC resolver. Use the **no** form of the command to disable the MAC resolver.

mac-resolver {active | passive}

no mac-resolver

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The MAC resolver provides a mechanism that allows software modules ("clients") in the SCOS to find the MAC address associated with a specific IP address.

Each client registers the IP addresses it needs to resolve in the MAC resolver database and receives the resolved MAC addresses and any future updates regarding those addresses. If an IP address has not been resolved or refreshed within a specified time interval, the database entry is marked as aged, and all clients are informed that this MAC address is no longer valid.

The MAC addresses are learned by listening to ARP messages. The MAC resolver does not respond to ARP requests, however, it will, in some cases, inject an ARP request in order to resolve or refresh a MAC address.

You can manually add an IP address to the MAC resolver database using one of the following commands:

- **debug slot linecard mac-resolver ip** — inserts a dynamic entry
- **mac-resolver arp** — inserts a static entry with the related MAC adddress

Note The MAC resolver injects the ARP request packet only to ports that have a pseudo IP address configured (see **pseudo-ip**).

The MAC resolver can be enabled to work in either of the following modes. Use the appropriate keyword to specify the desired mode:

- **Active** — enables ARP listening, aging, and ARP injection (ARP injection requires a port with a configured pseudo IP address; see **pseudo-ip.**)
- **Passive** — enables ARP listening and aging, ARP injection is disabled.

Authorization: root

Examples

The following example illustrates how to enable the MAC resolver to operate in active mode. Note that port #3 is configured with a pseudo IP address to support ARP injection.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface GigabitEthernet 0/3
SCE(config if)#>pseudo-ip 10.10.10.10
SCE(config if)#>exit
SCE(config)#>mac-resolver active
SCE(config)#>
```

Related Commands

Command	Description
pseudo-ip	
clear interface linecard mac-resolver arp-cache	
show interface linecard mac-resolver arp	
show interface linecard mac-mapping	
mac-resolver arp	
debug slot linecard mac-resolver ip	

mac-resolver arp

Adds a static IP entry to the MAC resolver database. Use the**no** form of the command to remove the static IP entry from the data base.

mac-resolver arp*ip_address* **[vlan** *vlan_tag] mac_address*

no mac-resolver arp *ip_address* **[vlan** *vlan_tag] mac_address*

Syntax Description

ip address	IP address entry to be added to the database.
vlan tag	VLAN tag that identifies the VLAN that carries this IP address (if applicable).
mac address	MAC address assigned to the IP address, in xxxx.xxxx.xxxx format.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

When adding an entry, if a client has previously registered a dynamic entry with the same IP address and VLAN tag, the entry receives the MAC address specified in the CLI command, and the entry is changed to static.

When removing an entry, if an entry has been added both as a dynamic entry and a static entry, it exists in the database as a static entry only (as explained in the preceding paragraph). Removing the static configuration changes the entry from a static entry to a dynamic entry and deletes the corresponding user-configured MAC address.

Authorization: admin

Examples

The following example assigns the MAC address 1111.2222.3333 to the IP address 10.20.30.40.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#mac-resolver arp 10.20.30.40 1111.2222.3333
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard mac-resolver arp	

management-agent access-class

Restricts management agent access to those addresses listed in the specified access list. The configuration applies to all services provided by the management agent (such as RPC, HTTP, etc.). IP addresses not included in this access list cannot access the management agent. (Use the **access-list** command to create the appropriate access control list.) Use the **no** form of the command to set the management agent to accept access from any IP address.

management-agent access-class ***acl-id***

no management-agent access-class

Syntax Description

acl-id	The number of the access list (1–99) containing the IP addresses that are permitted management agent access. (See the **access-list** command for information on creating an access list)

Defaults

By default, no access list is configured (management agent access is available from any IP address).

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following examples illustrates how to use this command.

EXAMPLE 1:

The following example assigns an existing ACL to the management agent.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#>management-agent access-class 4
SCE(config)#>
```

EXAMPLE 2:

The following example removes the ACL assignment from the management agent.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#>no management-agent access-class
SCE(config)#>
```

Related Commands

Command	Description
access-list	
show management-agent	

management-agent notifications

Enables sending notifications to the management agent that a dynamic CLI command was invoked. The 'notifications' in this context refer to an asynchronous notification mechanism that is internal for the SCOS and the management agent. The notification IDs are part of the code base of the SCOS/Management agent and in order to control specific IDs, an intimate knowledge of the code base is required. Use either the **no** or the **default** form of the command to disable sending notifications about dynamic CLI commands to the management agent.

management-agent notifications {all | module-list*module-list* **| notification-list** ***notification-list*** **}**

no management-agent notifications

default management-agent notifications

Syntax Description

module-list	List of module numbers to be enabled. All notifications in each listed module will be enabled.
notification-list	List of specific notification numbers to be enabled.

Defaults

By default, all notifications are enabled.

Command Modes

Global Configuration

Usage Guidelines

Each notification is assigned an ID number. In addition, each notification is assigned to a module, which also has an ID number. Therefore, you can enable either specific notifications or entire notification modules.

Authorization: root

Examples

The following example enables dynamic CLI notifications to the specified modules.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>management-agent notifications module-list 5 7 11
SCE(config)#>
```

Related Commands

Command	Description

management-agent sce-api ignore-cascade-violation

Configures the agent to ignore the errors issued when logon operations are performed on a standby SCE platform. Use the **no** form of this command to configure the agent to issue an error when a logon operation is performed on a standby SCE platform. Use the**default** form of this command to set the value to the default (the default behavior is to issue an error when a logon operation is performed on a standby SCE platform).

management-agent sce-api ignore-cascade-violation

no management-agent sce-api ignore-cascade-violation

default management-agent sce-api ignore-cascade-violation

Syntax Description

This command has no arguments or keywords.

Defaults

By default, an error is issued when a logon operation is performed on a standby SCE platform (**no** form of the command).

Command Modes

Global Configuration

Usage Guidelines

Starting in release 3.1.0, the SCE platform issues an error message when a logon operation is performed on the standby SCE platform in a cascaded system. This behavior is not backward compatible for previous versions of the SCE Subscriber API.

Use this command with SCOS release 3.1.0 to provide backward-compatible behavior to previous releases in which such errors were not issued.

Authorization: admin

Examples

The following example illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# management-agent sce-api ignore-cascade-violation
SCE(config)#
```

Related Commands

Command	Description

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>enable 10
Password:<cisco>
SCE#config
SCE(config)# management-agent sce-api logging
SCE(config)#
```

Related Commands

Command	Description

management-agent sce-api quota-buffer-size

Configures the size of the quota buffer. This is a queue that stores the QM notification messages if the link between the SCE platform and the QM fails.

management-agent sce-api quota-buffer-size *buffer-size*

Syntax Description

buffer-size	The size of the quota message buffer in bytes. (100-5000)

Defaults

.buffer-size = 1000

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#> management-agent sce-api quota-buffer-size 2000
SCE(config)#>
```

management-agent sce-api quota-rate-control

Defines the limit on the rate of the quota indications sent from the SCE platform to the Quota Manager.

management-agent sce-api quota-rate-control ***quota-rate***

Syntax Description

quota-rate	The maximum number of quota indications that the SCE platform can send to the Quota Manager per second.

Defaults

quota-rate = 125 per second

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following examples illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#>management-agent sce-api quota-rate-control 150
SCE(config)#>
```

Related Commands

Command	Description

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# management-agent sce-api timeout 10
```

Related Commands

Command	Description

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#management-agent system mng45.pkg
Verifying package file…
Package file verified OK.
SCE(config)#do copy running-config startup-config
Backing –up configuration file…
Writing configuration file…
Extracting new management agent…
Extracted OK.
```

Related Commands

Command	Description
copy running-config startup-config	

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>enable 10
Password:<cisco>
SCE#mkdir mydir
CE#
```

Related Commands

Command	Description
dir	

more

Displays the contents of a file.

more {*file-name* | running-config [all-data] | startup-config}

Syntax Description

file-name	The name of the file to be displayed.
all data	Displays defaults as well as non-default settings (running-config option only)

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The **running-config** option displays the running configuration file. You can use the **all data** switch with this option to see sample usage for many CLI configuration commands.

The **startup-config** option displays the startup configuration file.

Authorization: admin

Examples

The following sample output displays the contents of the running configuration file.

```
SCE>enable 10
Password:<cisco>
SCE#more running-config
#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 "cisco"
enable password level 15 0 "cisco"
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

Command	Description
show running-config	
show startup-config	

more (ROOT level options)

Displays the specified configuration file.

more startup-config-application

more startup-config-all

more running-config-application

more running-config-all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

This command displays either the startup or current configuration, depending on the option specified:

- more startup-config-application — Displays the startup application configuration.
- more startup-config-all — Displays the complete startup configuration.
- more running-config-application — Displays the current application configuration.
- more running-config-all — Displays the complete current configuration.

Authorization: root

Examples

The following sample output displays a portion of the startup application configuration.

```
SCE>enable 15
Password:<cisco>
SCE#>more startup-config-application
#This is an application configuration file (running-config-application).
#Created on 09:54:48 GMT WED April 26 2006
#cli-type 1
#version 1
interface linecard 0
application /tffs0/app/eng30102.sli capacity-option "EngageDefaultSE100"
tunable "GT_GLB_currentMonth" v "4"
tunable "GT_SubsNotificationDismissMethod[0]" v "2"
lookup "GT_NotificationLUT[0]" remove-all
lookup "GT_NotificationLUT[1]" remove-all
lookup "GT_NotificationLUT[2]" remove-all
lookup "GT_NotificationLUT[3]" remove-all
--More--
SCE#>
```

Related Commands

Command	Description
show startup-config	
show running-config	
more	

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>enable 10
Password:<cisco>
SCE#more user-log
<INFO>| 01/28/97 22:29:22 | CPU #000 | Logger: Task Initialized successfully
```

Related Commands

Command	Description
logger get user-log file-name	
show log	

mpls

Configures the MPLS environment. MPLS labels are supported up to a maximum of 15 labels per packet.

mpls traffic-engineering skip

mpls vpn skip

mpls vpn auto-learn

default mpls

Syntax Description

See "Usage Guidelines"..

Defaults

By default, **traffic-engineering skip** is enabled.

Command Modes

Linecard Interface Configuration

Usage Guidelines

Use the **traffic-engineering skip** form of the command when all IP addresses are unique and MPLS labels are not mandatory (a non-MPLS/VPN environment).

Use the **VPN skip** form of the command when all IP addresses are unique, but MPLS labels are used.

Use the **VPN auto-learn** form of the command in an MPLS/VPN environment where auto-learning is required due to the existence of private IP addresses and/or VPN based subscribers.

Use the **default** keyword to set the MPLS configuration to the default value.

CHANGING VPN MODES

VPNs can only exist in either **VLAN symmetric classify** or **MPLS VPN auto-learn,** but these two modes cannot be enabled simultaneously. When changing from one of these VPN-related modes to another, keep the following guidelines in mind:

- All VPN-based subscribers must be cleared in order to change the tunneling mode. If the connection with the SM is down, use the **no subscriber all with-vpn-mappings** CLI command.
- All VPN mappings must also be removed. This can only be done via the SM CLU (which means that the connection with the SM must be up).

Authorization: admin

Examples

The following examples illustrate the use of this command.

EXAMPLE 1

The following example illustrates the use of this command in a non-MPLS/VPN environment.

```
SCE>enable 10
Password:<cisco>
SCE#config
```

```
SCE(config)#interface linecard 0
SCE(config if)#mpls traffic-engineering skip
SCE(config if)#
```

EXAMPLE 2

The following example illustrates the use of this command in an MPLS/VPN environment with VPN-based subscribers.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#mpls vpn auto-learn
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard mpls	

mpls vpn pe-id

Defines a PE router, with the interface IP address of that PE router. Use the **no** form of the command to remove a router definition.

mpls vpn pe-id ***pe-id-ip*** **interface-ip** ***if-ip*** **[vlan** ***vlan-id*** **] [interface-ip** ***if-ip*** **[vlan** ***vlan-id*** **]]**

no mpls vpn pe-id ***pe-id-ip*** **interface-ip** ***if-ip***

no mpls vpn pe-id ***pe-id-ip***

Syntax Description

pe-id-ip	IP address that identifies the PE router
if-ip	Interface IP address for the PE router. This is used for MAC resolution. See "Usage Guidelines" for more information.
vlan-id	A VLAN tag can optionally be provided for each interface IP.

Defaults

By default, no PE routers are defined.

Command Modes

Linecard Interface Configuration

Usage Guidelines

Refer to the following guidelines when defining the PE router and its interfaces.

- At least one interface IP address must be defined per PE router.
- Multiple interface IP addresses may be defined for one PE router.
- Only one MAC address is configured per PE router. Therefore, if the PE router has multiple interfaces, some or all of which have the same MAC address, only one interface IP address is configured.
- Two interfaces cannot be defined with the same IP address, even if they have different VLAN tags. If such a configuration is attempted, it will simply update the VLAN tag information for the existing PE interface.

Refer to the following guidelines when removing a PE router or its interfaces.

- You cannot remove a PE if it retains any MPLS mappings. You must logout the VPN before removing the router it uses.
- Removing the last interface of a PE router removes the router as well. Therefore, you must logout the relevant VPN in order to remove the last interface.

Use the **no MPLS VPN PE-ID** *pe-id-ip* **interface-IP** *if-ip* form of the command to remove an interface from the PE router.

Use the **no MPLS VPN PE-ID** *pe-id-ip* form of the command to remove a PE router.

Authorization: admin

Examples

The following examples illustrate the use of this command.

EXAMPLE 1

The following example illustrates how to define a PE router with two interfaces.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#mpls vpn pe-id 10.10.10.10 interface-ip 10.10.10.20 interface-ip
10.10.10.30
SCE(config if)#
```

EXAMPLE 2

The following example illustrates how to remove the above PE router.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no mpls vpn pe-id 10.10.10.10
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard mpls	
mpls	
no mpls vpn pe-database	

mpls vpn validity-checks

Enables or configures the MPLS/VPN validity check mechanisms. Use the **no** form of the command to disable the specified MPLS/VPN validity check mechanism.

mpls vpn validity-checks

no mpls vpn validity-checks

mpls vpn validity-checks upstream-aging [aging-timeout *time*]

no mpls vpn validity-checks upstream-aging

mpls vpn validity-checks bypassed-vpns-aging aging-timeout *time*

mpls vpn validity-checks invalidity-threshold *threshold*

mpls vpn validity-checks unidirectional-tcp-detection

no mpls vpn validity-checks unidirectional-tcp-detection

Syntax Description

time	The timeout interval for either upstream aging and bypassed VPN aging, in minutes. Range is 5–120 minutes.
threshold	The maximum number of failed checks allowed for a label. If this threshold is exceeded, the label is removed

Defaults

By default, all MPLS/VPN validity check mechanisms are enabled.

Command Modes

By default, all MPLS/VPN validity check mechanisms are enabled.

Default time = 10 minutes

Default threshold = 20

Usage Guidelines

Validity checks clear mappings that are no longer relevant, so that the tables do not overflow due to irrelevant information. There are several validity check mechanisms:

- Upstream labels aging — Upstream label pairs learned through TCP are aged if no healthy flow is opened on them. This includes both subscriber labels and non-vpn labels.
- Bypassed VPN aging – Label mappings that belong to bypassed VPNs are cleared after a specific aging time, regardless of the traffic. If the label is still active, it will be relearned after removal.
- Unidirectional TCP detection — Detects erroneous situations where TCP flows have data only on one direction.
- Other built in validity checks for labels.

  Since none of the validity checks is 100% accurate, there is a threshold that is used to accumulate validity check failures before the labels are cleared.

Use the appropriate keyword to enable or disable the desired option:

- **upstream-aging** — Enables the aging of upstream labels. Use the **aging-timeout** option with this keyword to set the timeout interval for upstream aging. Note that the actual aging time may be anything between the configured value and double the configured value.
- **bypassed-VPNs-aging aging-timeout** – Specifies the aging time for labels of bypassed VPNs. Note that bypassed VPNs are removed after the exact time that is configured.
- **unidirectional-tcp-detection** — Enables the unidirectional TCP flow detection mechanism.
- Use the **no** form of the command to disable the specified option.
- If no keyword is used, all MPLS/VPN validity check mechanisms are enabled or disabled.

Use the **invalidity-threshold** option to set the threshold for all the validity check failures.

Authorization: root

Examples

The following example shows how to enable the aging of upstream labels and set the timeout interval.

```
SCE>enable 10
Password:<cisco>
SCE#>config
SCE(config)#>interface linecard 0
SCE(config if)#>mpls vpn validity-checks upstream-aging aging-timeout 5
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard mpls vpn (ROOT level options)	

no bursty-input

Disables the bursty-input 'debug' mode.

no bursty-input

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Usage Guidelines

The SCOS has a 'debug' mode for congestion handling that was implemented for use in artificial traffic generation scenarios, such as throughput or benchmark testing done by Ixia/Adtech/etc.

This mode can be useful in SCOS versions prior to 2.5.10 and 3.0.3 (on the relevant trains) and is usually described in the documents that explain how to perform benchmarking testing with the SCE platform.

With newer releases, the use of this command is not required and may cause less than optimal behavior.

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>no bursty-input
SCE(config if)#>
```

Related Commands

Command	Description

no more

By default, the **show** commands act the same as the **more** commands; that is, the output is displayed interactively a single screen at a time. Use this command to disable this feature so that **show** commands display the complete output all at one time.

no more

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>no more
SCE#>
```

Related Commands

Command	Description
All show commands, especially those with a long output.	

no mpls vpn pe-database

Removes all configured PE router enties.

no mpls vpn pe-database

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Usage Guidelines

All MPLS VPNs must be logged out before using this command, since it removes all PE routers.

Authorization: admin

Examples

The following example illustrates the use of this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no mpls vpn pe-database
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard mpls	
show interface linecard mpls vpn (root level options)	
mpls vpn pe-id	

no party db

Removes all data from the party database.

no party db

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to remove all data from the party database.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>no party db
SCE(config)#>
```

Related Commands

Command	Description
party load-database	
party save-database	

no party name

Removes the specified party from the database.

no party name ***party-name*** **[remove-ip-mappings]**

Syntax Description

party-name	The name of the party to remove.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

A party that has existing IP mappings will not be removed. Use the **remove-ip-mappings** flag to automatically remove any existing mappings, so that the party will be removed even if there are currently IP mappings for the party.

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates that a party cannot be removed if there are any existing IP mappings for the party. Use the **remove-ip-mappings** flag to remove the IP mappings so that the party will be successfully removed.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>no party name newparty
Error - Cannot remove party from DB because it has addresses mapped to it.
SCE(config)#>no party name newparty remove-ip-mappings S
CE(config)#>
```

EXAMPLE 2

The following example illustrates the use of the **no party mapping all** command, which removes the mappings, followed by the **no party name** command to actually remove the party. This requires two steps, while using the **remove-ip-mappings** flag removes the mappings and the party in one step.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>no party mapping all name newparty
SCE(config)#>no party name newparty
SCE(config)#>
```

Related Commands

Command	Description
show party name	
party mapping	
no subscriber	

no subscriber

Removes a specified subscriber from the system. Use the**all** option to remove all introduced subscribers.

no subscriber name ***subscriber-name***

no subscriber scmp name ***scmp-name*** **all**

no subscriber sm all

no subscriber all [with-vpn-mappings]

Syntax Description

subscriber-name	The specific subscriber name to be removed from the system.
scmp-name	Name of an SCMP peer device.

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Usage Guidelines

Use the **all with-vpn-mappings** keywords to remove all the subscribers that have VPN-based subscribers from the SCE platform.

This option allows you to switch out of MPLS/VPN mode when the SM is down.

Note Use the **with-vpn-mappings** option ONLY when the SCE platform is disconnected from the SM.

Use the **scmp name all** option to remove all subscribers managed by the specified SCMP peer device.

Use the **sm all** option to remove all subscribers managed by the SM.

Authorization: admin

Examples

The following example removes all subscribers.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0

SCE(config if)# no subscriber all SCE(config if)#
```

Related Commands

Command	Description
show interface linecard subscriber	

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*

no subscriber mappings included-in ip-range *IP-range*

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

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# no subscriber mappings included-in TP-IP-range name CMTS1
```

Related Commands

Command	Description
show interface linecard subscriber mapping included-in tp-ip-range	

party aging

Enables party aging for the specified party type (anonymous or introduced). Also configures the aging timeout for the specified party type. Use the **no** form of the command to disable party aging for the specified party type or to reset the aging timeout to the default value for the specified party type.

party aging {anonymous | introducedl} [timeout *timeout*]

no party aging {anonymous | introduced | all} [timeout *timeout*]

Syntax Description

timeout	The aging timeout value in minutes.

Defaults

Default party aging:

- Anonymous parties — party aging is enabled
- Introduced — party aging is disabled

Default timeout = 30 minutes for both anonymous and introduced parties

Command Modes

Global Configuration

Usage Guidelines

The most common usage for aging is for anonymous subscribers, since this is the easiest way to ensure that anonymous subscribers who have logged-out of the network are removed from the SCE platform and are no longer occupying resources.

Note that the **all** option is only available for the **no** form of the command.

When the **timeout** option is specified, the timeout value for the specified party type is configured, but the status (enabled/disabled) is unchanged.

When the **timeout** option is not specified, the status (enabled/disabled) for the specified party type is configured, but the timeout value is unchanged.

Note Introduced party aging is not supported when using VPN-based subscribers.

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to configure the timeout to 15 minutes for both party types. Note that this does not change the status of party aging for either party type (aging would still be disabled for introduced parties, assuming default aging configuration).

```
SCE>enable 15
Password:<cisco>
SCE#>configure
```

```
SCE(config)#>party aging anonymous timeout 15
SCE(config)#>party aging introduced timeout 15
SCE(config)#>
```

EXAMPLE 2

The following example illustrates how to reset the timeout to the default value for both party types. Note that this does not change the status of party aging for either party type (aging would still be enabled for anonymous parties, assuming default aging status configuration).

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>no party aging all timeout
SCE(config)#>
```

Related Commands

Command	Description
show party	
subscriber aging	

party autoflush-mode

Enables party database operation in autoflush-mode, which saves the database on every operation. Use the **no** form of the command to disable auto-flush mode for the party database. (use the **party save-database** command to manually save the party database).

party autoflush-mode

no party autoflush-mode

Syntax Description

This command has no arguments or keywords.

Defaults

By default, auto-flush mode is enabled.

Command Modes

Privileged Exec

Usage Guidelines

This is a CLI session parameter. It is not saved in the configuration.

Authorization: root

Examples

The following example illustrates how to enable autoflush-mode.

```
SCE>enable 15
Password:<cisco>
SCE#>party autoflush-mode
SCE#>
```

Related Commands

Command	Description
party save-database	

party default-name

Changes the name of the default party.

party default-name ***default-party-name***

Syntax Description

default-party-name	The name of the default party.

Defaults

default-party-name = DefaultParty

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to configure the name of the default party.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>party default-name plainVanilla
SCE(config)#>
```

Related Commands

Command	Description
show party	

party mapping

Maps the specified IP address, range of addresses, or VLAN tag to the specified party. Use the **no** form of the command to remove the specified mapping.

party mapping IP-address*ip-address* **name** ***party-name***

party mapping IP-range ***ip-address:mask*** **name** ***party-name***

party mapping vlan-id ***vlan-id*** **name***party-name*

no party mapping IP-address ***ip-address***

no party mapping IP-range*ip-address:mask*

no party mapping vlan-id ***vlan-id***

no party mapping all name ***party-name***

Syntax Description

party-name	The name of the party.
ip-address	Specific IP address to be mapped, specified in one of the following formats: • long decimal (e.g. 8733346) • long hexadecimal (e.g. 0x15624362) • IP address (e.g. 1.2.3.4)
ip-address:mask	Range of IP addresses specified in one of the following formats: • A.B.C.D • A.B.C.D/E • A.B.C.D:0xMASK where A,B,C,D are in the range [0,255], E is in the range [0,32] and MASK is the IP mask in 8 hexadecimal characters
vlan-id	Specific VLAN tag number, specified in of the following format: • hexadecimal number not larger than 0x0fff

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use the **all** keyword with the **no** form of the command to remove all mappings of the specified party.

Authorization: root

Examples

The following example illustrates how use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>party mapping ip-range 10.10.10.10:0xffffffff name newparty
SCE(config)#>
```

Related Commands

Command	Description
show party mapping	
show party name mappings	

party load-database

Loads the specified party database information from the backup.

party load-database subscribers backup

party load-database mappings backup

party load-database variables backup

party load-database all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

Specify appropriate keyword to load the desired party database information from the backup:

- subscribers
- mappings
- variables
- all

Authorization: root

Examples

The following example illustrates how to load all party database information from the backup.

```
SCE>enable 15
Password:<cisco>
SCE#>party load-database all
Party names database loaded
Party mappings database loaded
Party variables database loaded
SCE#>
```

Related Commands

Command	Description
party save-database	
party autoflush-mode	

party name tunables

Updates party tunables.

party name ***party-name*** **tunables name** ***party-tunable-name*** **value** ***party-tunable-value*** **name** ***party-tunable-name*** **value** ***party-tunable-value***

Syntax Description

party-name	The name of the party.
party-tunable-name	The name of the specific party tunable.
party-tunable-value	Value to assign to the tunable.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

The party is created if it does not exist.

Tunables can only be specified if an application is loaded.

Authorization: root

Examples

The following example illustrates how to update the tunable "packageId".

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>party name partyall tunables name packageId value 1
SCE(config)#>
```

Related Commands

Command	Description
show party name	
no party name	
subscriber name property	

party name cpu-mapping

Statically sets the slot and traffic processor to which the party should be mapped. Usually the parties are load-balanced between the traffic processors; this commands allows the user to bypass the system party-to-cpu mapping if the mapping has not already been decided (therefore this command can only be executed when there are no IP mappings to the party). Use the **no** form of the command to reset the static cpu mapping of the specified party.

party name ***party-name*** **cpu-mapping slot** ***slot-number*** **cpu** ***cpu-number***

no party name ***party-name*** **cpu-mapping**

Syntax Description

party-name	The name of the party.
slot-number	The number of the identified slot. Enter a value of 0.
cpu-number	The number of the CPU in the designated slot. Must be one of the traffic processors (1-3).

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Be sure that all mappings to the party are removed before executing this command. (Use the **no party mapping all name** command.)

Authorization: root

Examples

The following example illustrates how to set the cpu mapping for a party. Note the use of the **no party mapping all** command to remove all mappings first.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>no party mapping all name newparty
SCE(config)#>party name newparty cpu-mapping slot 0 cpu 1
SCE(config)#>
```

Related Commands

Command	Description
party mapping	
show party name	

party pull-retries-till-trap

Defines the number of pull requests permitted before a trap is issued. Use the **default** form of the command to revert to the default number of pull requests permitted before a trap is issued.

party pull-retries-till-trap ***number***

default party pull-retries-till-trap

Syntax Description

number	Number of pull requests retries before sending a trap. This number is limited by the number of total tries the control card performs.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>party pull-retries-till-trap 10
SCE(config)#>
```

Related Commands

Command	Description

party save-database

Saves the party database for backup (in case the SCE platform reloads).

party save-database

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to manually save the party database.

```
SCE>enable 15
Password:<cisco>
SCE#>party save-database
SCE#>
```

Related Commands

Command	Description
party autoflush-mode	
party load-database	

party template

Configures a template context, defining the set of tunable or meter values for this context.

party template index *index* tunables name *tunable-name* value*tunable-value* name *tunable-name* value *tunable-value*...

party template index meters name *meter-name* value *meter-values* name *meter-name* value *meter-values*...

default party template index *index*

Syntax Description

index	The index number of the party template (1-199).
tunable-name	The name of the specific party tunable.
meter-name	The name of the specific party meter.
tunable-value	Value to assign to the tunable.
meter-values	Indicate the relevant meter parameters separated by a slash in the following order: committed/peak/direction/qos/assuranceLevel/totalIdx

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

A party (subscriber) template is assigned to each group of anonymous subscribers to define the properties of that anonymous subscriber group s. If no subscriber template has been assigned, the default template is used.

Party (subscriber) templates are identified by a number from 0-199. Party templates 1-199 are defined in csv formatted subscriber template files. Template #0 is the default template and cannot be edited.

Note that party templates can also be imported from csv files (see **subscriber template import csv-file**). In addition, you can export existing party templates to a csv file (see **subscriber template export csv-file**).

Use the **default** form of the command to configure the specified party template to the default tunable / meter values.

Authorization: root

Examples

The following example illustrates how to configure a party template.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>party template 1 tunables name packageId value 1 name monitor value 0
SCE(config)#>
```

Related Commands

Command	Description
show party template	
subscriber template export csv-file	
subscriber template import csv-fil	
default subscriber template all	

party unmapped-group

Creates an unmapped party group entry based on the specified IP range. Use the **no** form of the command to remove the specified unmapped party group.

party unmapped-group name ***name*** **ip-range** ***ip-address:mask*** **[template-index** ***index*** **]**

no party unmapped-group name ***name*** **ip-range*****ip-address:mask*** **[template-index** ***index*** **]**

no party unmapped-group all

Syntax Description

name	The name of the group.
ip-address:mask	Range of IP addresses specified in the format x.x.x.x:y.
index	The index number of the party template.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use the optional **template-index** parameter to add the unmapped group to, or remove it from, the specified template context.

Use the **all** keyword with the **no** form of the command to remove all unmapped groups.

The SCE platform can support a maximum of 1000 unmapped party groups.

Authorization: root

Examples

The following example illustrates how use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>party unmapped-group name unmappedGroup ip-range 10.10.10.10:0xffffffff
template-index 1
SCE(config)#>
```

Related Commands

Command	Description
show party	
clear interface linecard subscriber	
no subscriber anonymous-group	

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

host	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>enable 10
Password:<cisco>
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

Command	Description

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

filename	The filename of the pqi application file to be installed.
options	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

Always run the **pqi uninstall file** command before installing a new pqi file to prevent accumulation of old files on the disk.

Authorization: admin

Examples

The following example installs the Subscriber Manager anr10015.pqi file. No options are specified.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#pqi install file anr10015.pqi
SCE(config if)#
```

Related Commands

Command	Description
show pqi file	
pqi uninstall file	

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. Use the **show pqi last-installed** command.

Authorization: admin

Examples

The following example reverses the upgrade for the Subscriber Manager using the anr100155.pqi file.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#pqi rollback file anr100155.pqi
SCE(config if)#
```

Related Commands

Command	Description
show pqi last-installed	

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. Use the **show pqi last-installed** command.

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#pqi uninstall file anr10015.pqi
SCE(config if)#
```

Related Commands

Command	Description
show pqi last-installed	
pqi install file	

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

filename	The filename of the *pqi* application file to be used for the upgrade.
options	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.

When upgrading the application in a cascaded system, use the **force failure-condition** command to force failure in the active SCE 2000 platform (see 'System Upgrades' in the Chapter "Redundancy and Fail-Over" in the *Cisco Service Control Engine Software Configuration Guide*).

Authorization: admin

Examples

The following example upgrades the Subscriber Manager using the anr100155.pqi file. No options are specified.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#pqi upgrade file anr100155.pqi
SCE(config if)#
```

Related Commands

Command	Description
show pqi file	
force failure-condition (SCE 2000 only)	

pseudo-ip

Configures a dummy IP address for the interface. Use the**no** form of the command to remove the specified dummy IP address.

pseudo-ip ***ip-address [subnet-mask]***

no pseudo-ip ***ip-address [subnet-mask]***

Syntax Description

ip-address	Specific IP address to be assigned in dotted decimal format.
subnet-mask	Range of IP addresses (used for VAS over 10G with 7600 as dispatcher)

Defaults

By default, no pseudo IP address is assigned.

Command Modes

GigaBit Ethernet Interface Configuration

Usage Guidelines

The dummy IP address is used by the SCE platform for operations that require a unique IP address while retaining the transparent nature of the SCE platform; that is the SCE platform acquires a useable IP address without becoming a network entity.

Two examples of the use of the pseudo IP address are:

- MAC resolver — requires a port with a pseudo IP address to support ARP injection (see **mac-resolver**)
- VAS over 10G — requires a port with eight dummy IP addresses (IP addresses that are not used in the network) for the sending of health check packets. This IP address range is then configured as the source IP address for the health check packets. This option, using a Cisco 7600 router, requires that the subnet mask be specified in the command to configure a range of IP addresses.

Authorization: root

Examples

The following example illustrates how to configure port #3 with a range of pseudo IP addresses to be used as the destination for the VAS health check packets, as configured in the **vas-traffic-forwarding vas health-check ip-address** command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface GigabitEthernet 0/3
SCE(config if)#>pseudo-ip 20.20.20.20. 255.255.255.0
SCE(config if)#>exit
SCE(config)#>interface linecard 0
SCE(config if)#>vas-traffic-forwarding vas health-check ip-address source 20.20.20.20/28
destination 10.10.10.10
SCE(config if)#>
```

Related Commands

Command	Description
mac-resolver	
vas-traffic-forwarding **vas health-check**	

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>enable 10
Password:<cisco>
SCE#pwd
tffs0:
SCE#
```

Related Commands

Command	Description
cd	

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. BE is the best effort queue, that is the lowest priority. • 2, 3=AF. 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. • 4=EF. EF is the Expedited Forwarding queue, that is the highest priority forwarding
bandwidth	Bandwidth measured in kbps. The maximum bandwidth is determined by the line rate. 0 disables packet transmission from the queue. 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

GigabitEthernet Interface Configuration

Usage Guidelines

This command is valid for a specified GigabitEthernet line interface only. It must be executed explicitly for each interface.

Use the **interface gigabitethernet** command to access the configuration mode for the desired interface.

Authorization: admin

Examples

The following example configures queue shaping for queue 1 for GBE port #4.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface GigabitEthernet 0/4
SCE(config if)#queue 1 bandwidth 20000 burstsize 1000
```

Related Commands

Command	Description
bandwidth	
interface gigabitethernet	

rdr-formatter buffer-size

Sets the buffer size for the specified RDR category.

rdr-formatter ***category number*** **category-number buffer-size** ***size***

default rdr-formatter category number ***category-number*** **buffer-size**

default rdr-formatter buffer-size all

Syntax Description

category-number	Number of the RDR category (1-4)
size	Size of the buffer allocated to the specified category in bytes

Defaults

Default buffer size varies by category and SCE platform type (see **Usage Guidelines**).

Command Modes

Global Configuration

Usage Guidelines

This command can be executed only when the RDR-formatter service is disabled (Use the **no service RDR-formatter command**).

Use the **default** option to set the buffer size for the specified category to the default value.

Use the **all** keyword with the **default** option to set the buffer size for the all categories to the default value.

Total memory assigned to all RDR categories is:

- SE1000: 20MB
- SE2000: 40MB

The total memory available for the RDR formatter cannot be changed. This command specifies how much of the total available memory is allocated to each RDR category.

Default memory allocations (% of total memory) to each RDR category, assuming the following standard categories:

- **Category 1 – 50%** : Usage RDRs to Data Collector \ mediation system
- **Category 2 – 30%** : Quota RDRs to Pre-Paid Server (e.g. Comverse) \ Subscriber Controller OSS (e.g. Tazz)
- **Category 3 – 10%** : External events RDR \ RT Signaling to various systems such as a Packet Cable Multi Media Policy Server
- **Category 4 - 10%** : URL Query RDR to URL Filtering DB (e.g. surfControl)

Authorization: root

Examples

The following example illustrates how to set the buffer for category 2 to the default size. Note that the RDR formatter is disabled before changing the buffer size and then enabled after the command is executed.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE#>no service rdr-formatter
SCE(config)#>default rdr-formatter category number 2 buffer-size
SCE#>service rdr-formatter
SCE(config)#>
```

Related Commands

Command	Description
service rdr-formatter	

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. 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.

rdr-formatter category number ***[1-4]*** **name** ***category name***

no rdr-formatter category number ***[1-4]*** **name** ***category name***

Syntax Description

category name	The user-defined name to be assigned to the category.

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#rdr-formatter category number 1 name prepaid
SCE(config)#
```

Related Commands

Command	Description
show rdr-formatter	
service rdr-formatter	
rdr-formatter buffer-size	

rdr-formatter destination

Configures an RDRV1 or Netflow destination. This is where the RDR formatter sends the records (RDRs or export packets) it produces. Use the**no** form of the command to remove the mappings of a 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* **] [category …] protocol {RrdrV1 | NetflowV9} [transport {udp | tcp}]**

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	(Optional) The priority of the destination. The priority value may be any number between 1 (lowest) to 100 (highest).
protocol	The protocol configured for this destination. Specify either of the following: • **RDRv1** • **NetflowV9**
transport	(Optional) The transport type configured for this destination. Specify either of the following: • **UDP** when protocol = Netflow • **TCP** when protocol = RDRv1.

Defaults

Default protocol = RDRv1

Command Modes

Global Configuration

Usage Guidelines

Up to eight destinations can be configured. Multiple destinations over the same category must have distinct priorities. In redundancy mode, the entry with the highest priority is used by the RDR formatter; in multicast mode or load-balancing mode priorities have no meaning.

In its simplest form, this command specifies only the IP address and port number of the destination and the protocol being used. In addition, a global priority may be assigned to the destination. Or a specific priority may be assigned to any or all of the four categories for the specified destination. If a global priority is not explicitly configured, the highest priority is assigned automatically.

Categories may be identified by either name or number.

A certain destination may be configured to one or more categories on the same time. A maximum of three destinations may be assigned to a specific category.

Note RDRv1 may only be configured with transport type of TCP and NetflowV9 may only be configured with transport type of UDP.

PRIORITIES

Following are some guidelines for configuring priorities for the report destinations:

- In redundancy mode, the entry with the highest priority is used by the RDR formatter, provided that a connection with this destination can be established
- Priority configuration is not relevant in multicast mode, since all reports are sent to all destinations.
- Priority configuration is not relevant in load-balancing mode, since all destinations are used for load balancing
- For the first destination defined, if no priority is set, the highest priority is automatically assigned.
- For all subsequently defined destinations, the priority must be explicitly defined, otherwise it will collide with the first destination priority.
- 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 all categories for that destination.
- The same priority cannot be assigned to the same category for two different destinations.

Authorization: admin

Examples

The following examples illustrate the use of this command:

EXAMPLE 1:

The following example configures a Netflow destination with the default priority (highest) to be used by all categories.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#rdr-formatter destination 10.1.1.205 port 33000 protocol NetflowV9 transport
udp
SCE(config)#
```

EXAMPLE 2:

The following example configures an RDR formatter destination for two categories with a different priority for each category. This configuration will send RDRs from category 2 to this destination, but generally not RDRs from category 1.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#rdr-formatter destination 10.1.1.206 port 34000 category number 1 priority 10
category number 2 priority 90 protocol RrdrV1
SCE(config)#
```

Related Commands

Command	Description
show rdr-formatter destination	
service rdr-formatter	
rdr-formatter protocol NetflowV9 dscp	
rdr-formatter destination protocol netflowv9 template data timeout	

rdr-formatter destination protocol NetflowV9 template data timeout

Configures the interval after which all Netflow templates must be exported to the specified destination (refreshed). Use the**no** or the **default** form of the command to disable the template refresh mechanism.

rdr-formatter destination ***ip-address*** **port** ***port-number*** **protocol NetflowV9 template data timeout** ***timeout-value***

no rdr-formatter destination ***ip-address*** **port** ***port-number*** **protocol NetflowV9 template data**

default rdr-formatter destination ***ip-address*** **port** ***port-number*** **protocol NetflowV9 template data**

Syntax Description

ip-address	The destination IP address.
port-number	The destination port number.
timeout-value	The time interval, in seconds,.between exporting the Netflow templates to the specified destination. Valid range is 1 – 86400 seconds.

Defaults

By default, the refresh mechanism is disabled.

Command Modes

Global Configuration

Usage Guidelines

A template record defines the structure of each Netflow data record. The RDR formatter transmits the templates only along with their matching data records. The RDR formatter refreshes the templates on the collector by resending them at configured intervals.

The **no** form of the command disables the refresh mechanism.

The **default** form of the command also disables the refresh mechanism, since the default state is disabled.

Authorization: admin

Examples

The following example illustrates the use of this command:

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#rdr-formatter destination 10.1.1.205 port 33000 protocol NetflowV9 template
data timeout 240
SCE(config)#
```

Related Commands

Command	Description
show rdr-formatter destination	
rdr-formatter destination	

rdr-formatter destination reconnect

Attempts to reconnect to the specified RDR formatter destination.

rdr-formatter destination {all-disconnected | (*host-name* port *port-number*)} reconnect

Syntax Description

host-name	Specific destination. Specify hostname or IP address.
port-number	Number of port at destination.

Defaults

Command Modes

Privileged EXEC

Usage Guidelines

You can define a specific RDR formatter destination, using the hostname or IP address and the port number. If the specified destination is currently connected, it will first disconnect and then reconnect.

Use the **all-disconnected** keyword to cause all connections that are currently down to attempt to reconnect.

Authorization: root

Examples

The following example illustrates how to reconnect to a specific destination.

```
SCE>enable 15
Password:<cisco>
SCE#>rdr-formatter destination 10.10.10.10 port 33000 reconnect
SCE#>
```

Related Commands

Command	Description
show rdr-formatter connection-status	

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	Each successive record is sent to a different destination, one destination after the other, in a round robin manner.

Authorization: admin

Examples

The following example sets the RDR formatter mode to “redundancy”.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#rdr-formatter forwarding-mode redundancy
SCE(config)#
```

Related Commands

Command	Description
show rdr-formatter forwarding-mode	

rdr-formatter history-size

Configures the size of the history buffer. This command is currently not supported.

rdr-formatter history-size ***size***

Syntax Description

size	Size of the history buffer in bytes. Must be = 0 only (default)

Defaults

Default size = 0

Command Modes

Global Configuration

Usage Guidelines

Do not change the size of the history buffer from the default value.

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.

Authorization: admin

Examples

Related Commands

Command	Description
show rdr-formatter history-size	

rdr-formatter protocol (ROOT level option)

Resets the RDR formatter.

rdr-formatter protocol rdrv1 force-reset

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Use this command to force a reset (disable and then enable) of the RDR formatter.

Authorization: root

Examples

The following example illustrates how to reset the RDR formatter.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>rdr-formatter protocol rdrv1 force-reset
SCE(config)#>
```

Related Commands

Command	Description
show rdr-formatter protocol	

rdr-formatter protocol NetflowV9 dscp

Defines the DSCP value to be assigned to the Netflow packets.

rdr-formatter protocol NetflowV9 dscp ***dscp-value***

Syntax Description

dscp-value	DSCP value to be assigned to the Netflow packets, in HEX format. Accepted range is 0-63.

Defaults

Default dscp-value = 0

Command Modes

Global Configuration

Usage Guidelines

You can assign a DSCP value to specify the diffserv value of the Netflow traffic exported from your SCE platform.

Authorization: admin

Examples

The following example illustrates the use of this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#rdr-formatter protocol NetflowV9 dscp 0x20
SCE(config)#
```

Related Commands

Command	Description
show rdr-formatter protocol NetflowV9 dscp	

rdr-formatter protocol NetflowV9 mapping

Loads a mapping of Raw Data Records (RDR) to Netflow records.

rdr-formatter protocol NetflowV9 mapping file ***filename***

Syntax Description

filename	Name of the XML file containing the Netflow record mapping.

Defaults

Command Modes

Global Configuration

Usage Guidelines

The mapping file specified must be a valid XML file with a valid format and values.

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#>rdr-formatter protocol NetflowV9 mapping file xml_mapping
SCE(config)#>
```

Related Commands

Command	Description
[root]show rdr-formatter protocol NetflowV9 mapping	

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 all categories are removed from a tag, this tag will be ignored and will not be formatted and sent – this is ‘ignore mapping'.

Authorization: admin

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

This example shows how to add a mapping to a category.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#rdr-formatter rdr-mapping tag-id 0xf0f0f000 category-number 1
SCE(config)#
```

EXAMPLE 2

This example shows how to restore the default mapping for a specified RDR tag.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#default rdr-formatter rdr-mapping tag-id 0xf0f0f000
SCE(config)#
```

Related Commands

Command	Description
show rdr-formatter rdr-mapping	

rdr-server

Configures the RDR server port number. Use the**default** form of the command to revert to the default rdr-server port.

rdr-server port ***port*** **#**

default rdr-server port

Syntax Description

port#	Number of the port to be used by the RDR server.

Defaults

port = 33001

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>rdr-server port 100
SCE(config)#>
```

Related Commands

Command	Description
show rdr-server	

reload

Note In order not to lose the current configuration, use the **copy running-config-all startup-config-all** command before using the **reload** command.

Reboots the SCE platform.

reload

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>enable 10
Password:<cisco>
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

Command	Description
copy running-config startup-config	
reload shutdown	

reload shutdown

Shuts down the SCE platform, 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 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>enable 10
Password:<cisco>
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

Command	Description
reload	

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>enable 10
Password:<cisco>
SCE#rename test1.pkg test3.pkg
SCE#
```

Related Commands

Command	Description

replace completion

Sets the criterion for completing the application replace operation (see **application replace**) and killing all old flows (flows associated with the old or replaced application). Use the**no** form of the command to disable the specified criterion. Use the **default** form of the command to set the specified criterion to the default value. Since the default value for the number of flows is "0", the **no** and the **default** forms of the command produce the same result for the number of flows option.

replace completion time ***minutes***

no replace completion time

default replace completion time

replace completion num-flows ***num***

no replace completion num-flows

default replace completion num-flows

Syntax Description

minutes	Maximum time period for completion of the application replace operation, in minutes. After this amount of time, all old flows are killed. Specifying a value of "0" disables this criterion, meaning that with respect to this criterion, the application replace operation is completed only after all old flows have naturally died. This is the same as using the **no** form of the command.
num	Number of flows criterion for completing the replace operation. When the number of remaining old flows has gone below this threshold, all old flows are killed. Specifying a value of "0" disables this criterion, meaning that with respect to this criterion, the application replace operation is completed only after all old flows have naturally died. This is the same as using the **no** or the **default** form of the command.

Defaults

minutes = 60

num = 0

Command Modes

Interface Linecard Configuration

Usage Guidelines

If both criteria are enabled, the replace operation is completed and all old flows killed as soon as either one of the criteria is met.

If only one criterion is enabled, the replace operation is completed and all old flows killed when that criterion is met.

If both criteria are disabled, the replace operation is completed only after all old flows have naturally died.

Authorization: root

Examples

The following example illustrates how to configure both completion criteria. In this case, the replace operation will be completed as soon as either criterion is met.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>replace completion time 30
SCE(config if)#>replace completion num-flows 100
SCE(config if)#>
```

Related Commands

Command	Description
application replace	
show applications slot replace	

replace spare-memory

Sets the amount of spare memory allocated for the specified element when loading an application. Use the **default** form of the command to reset the memory allocation for the specified element to the default value.

replace spare-memory {code | subscriber} {percent|bytes} ***value***

default replace spare-memory {code |subscriber} {percent|bytes}

Syntax Description

value	Amount of spare memory to be allocated for the specified element. Can be specified in percent or in bytes.

Defaults

Code spare memory = 50 percent

Subscriber spare memory = 0 bytes

Command Modes

Interface Linecard Configuration

Usage Guidelines

This command reserves additional memory so that the currently loaded application can be replaced with future applications having larger memory requirements.

The following memory elements can be configured:

- code — graph; nodes and construction memory
- subscriber — party memory

The settings of this command take effect only during an original application load (not replace).

Authorization: root

Examples

The following example illustrates how to configure the spare memory. allocations.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>replace spare-memory code percent 45
SCE(config if)#>replace spare-memory subscriber bytes 5000 SCE(config if)#>
```

Related Commands

Command	Description
show applications slot replace	
application replace	

replace support

Enables support for the application replace operation (see**application replace**). Use the **no** form of the command to disable support for the replace operation.

replace support

no replace support

Syntax Description

This command has no arguments or keywords.

Defaults

By default, replace support is enabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

The settings of this command take effect only during an original application load (not replace).

Authorization: root

Examples

The following example illustrates how to enable support for future replace operations.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>replace support
SCE(config if)#>
```

Related Commands

Command	Description
application replace	

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 removed.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

You can only remove an empty directory. Use the **dir** command to verify that no files are listed in this directory.

Authorization: admin

Examples

The following example deletes the code directory.

```
SCE>enable 10
Password:<cisco>
SCE#rmdir code
SCE#
```

Related Commands

Command	Description
dir	
delete	
delete (ROOT level option)	

salt

Configures the value of the salt to be applied to the Personally Identifying Field of Extended Transaction Usage RDRs prior to hashing it.

Use the **default** form of the command to reset the salt to the default value.

salt ***salt-value1 salt-value2 salt-value3 salt-value4***

default salt

Syntax Description

salt-value1 - salt-value4	Four 4-byte salt values in HEX

Defaults

0x12345678 0x12345678 0x12345678 0x12345678

Command Modes

Interface Linecard Configuration

Usage Guidelines

When generating Extended Transaction Usage RDRs for analyzing subscriber browsing patterns, it is necessary to hash the Personally Identifying Field to protect the identity of the subscriber. This command configures the salt to be applied to the field before hashing.

Always make sure to save the running configuration using the **copy running-config startup-config** command.

Authorization: admin

Examples

The following example shows how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)#salt 0xfafafafa 0xfafafafa 0xfafafafa 0xfafafafa
SCE(config if)#
```

sanity-checks

Enables or configures the specified sanity check. Use the **no** form of the command to disable the specified sanity check or option.

sanity-checks {*sanity-check-name* |all}

sanity-checks attack-filter [memory threshold *memory-threshold-value*]

sanity-checks attack-filter [times filtering-cycle *cycle-time-value* max-attack-time *max-time-value*]

sanity-checks event-counters {all | Flow-ID-Allocations-Failed | HW-Interrupts | Master-Processor-Logger-Errs | Traffic-Processor-Logger-Errs} [normalizer-validation-value *delta-value* | threshold *event-threshold-value*]

sanity-checks intensive-cpu-consuming-flows action [block | bypass]

sanity-checks intensive-cpu-consuming-flows aggregated-packet-rate *packet-rate*

sanity-checks intensive-cpu-consuming-flows max-packets-threshold *max-packets*

sanity-checks intensive-cpu-consuming-flows min-packets-threshold *min-packets*

sanity-checks intensive-cpu-consuming-flows trigger [always | shortage-only]

no sanity-checks {*sanity-check-name* | all}

no sanity-checks attack-filter [memory threshold]

no sanity-checks event-counters all

no sanity-checks event-counters (Flow-ID-Allocations-Failed | HW-Interrupts | Master-Processor-Logger-Errs | Traffic-Processor-Logger-Errs) [normalizer-validation-value | threshold]

no sanity-checks intensive-cpu-consuming-flows action

no sanity-checks intensive-cpu-consuming-flows aggregated-packet-rate

no sanity-checks intensive-cpu-consuming-flows max-packets-threshold

no sanity-checks intensive-cpu-consuming-flows min-packets-threshold

no sanity-checks intensive-cpu-consuming-flows trigger

Syntax Description

sanity-check-name	Name of the sanity check to be enabled or disabled: • attack-filter—There are further options for configuring this sanity check. See '**Usage Guidelines'.** • classifier-aging • control-watchdog-monitor • counters-test • disk-rw-test • event-counters—There are further options for configuring this sanity check. See '**Usage Guidelines'.** • intensive-cpu-consuming-flows—There are further options for configuring this sanity check. See '**Usage Guidelines'.** • test-packets
memory-threshold	Threshold for declaring memory shortage (percentage of memory)
cycle-time-value	Filtering cycle time in seconds
max-time-value	Maximum attack time in seconds
delta-value	Number of events per measurement period required for the specified event counter measure to be valid.
event-threshold-value	Threshold in seconds for determing that the measured rate for the specified event counter fails the sanity check. Sanity check fails if the measured rate exceeds this threshold per second. The actual threshold applied is the specified value divided by 10000 (accuracy up to four digits after the decimal point)
packet-rate	Threshold, in packets per second aggregated over the life of the flow, for determining that a flow is cpu consuming. Flows that exceed this rate, aggregated over the life of the flow, fail the intensive-cpu-consuming-flows sanity check.
max-packets	Upper threshold, in packets per second, for monitoring flow rate. Flows that exceed this maximum number of packets per second will not be monitored.
min-packets	Lower threshold, in packets per second, for monitoring flow rate. Flows that exceed this minimum number of packets per second will be monitored.

Defaults

filter-cycle-time = 1 hour (3600 seconds)

max-attack-time = 24 hours (86400 seconds)

Default values for delta-value and event-threshold-value vary depending on the specific event counter

By default, all flows are monitored for the intensive-cpu-consuming-flows sanity check, (no values configured for packet-rate, max-packets, or min-packets).

Command Modes

Interface Linecard Configuration

Usage Guidelines

The following sanity check options are available:

- **all** — Enables or disables all sanity checks.
- **attack-filter** — Enables or disables the attack filter mechanism, or configures one of the following options:
  - memory threshold
  - filtering-cycle
  - max-attack-time
- **classifier-aging** — Enables or disables the classifier aging mechanism
- **control-watchdog-monitor** — Enables or disables the control watchdog monitoring mechanism
- **counters-test** — Enables or disables the input/output counters tests
- **disk-rw-test** — Enables a sanity check that constantly reads/writes to the disk to make sure that it is working properly.
- **event-counters** — Enables or disables the specified event counter or configures one of the following options:
  - normalizer-validation-value
  - threshold
- The following event counter options are available:
  - all — (enable/disable only)
  - Flow-ID-Allocations-Failed
  - HW-Interrupts
  - Master-Processor-Logger-Errs
  - Traffic-Processor-Logger-Errs
- **intensive-cpu-consuming-flows** — Enables or disables the intensive-cpu-consuming-flows sanity check, or configures one of the following options:
  - action — Action to apply to flows that have failed the check (*block* or *bypass*)
  - aggregated-packet-rate
  - max-packets-threshold
  - min-packets-threshold
  - trigger — Event that triggers the intensive-cpu-consuming-flows sanity check (*always* or *shortage-only*)
- **test-packets** — Enables or disables the test packet mechanism.

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>no sanity-checks all
SCE(config if)#>
```

EXAMPLE 2

The following example shows how to enable and configure the sanity check for the hardware interrupt event counter.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>sanity-checks event-counters HW-Interrupts
SCE(config if)#>sanity-checks event-counters HW-Interrupts normalizer-validation-value
1000
SCE(config if)#>sanity-checks event-counters HW-Interrupts threshold 2500
SCE(config if)#>
```

EXAMPLE 3

The following example shows how to enable and configure attack filter sanity checks.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>sanity-checks attack-filter
SCE(config if)#>sanity-checks attack-filter times filtering-cycle 30 max-attack-time 60
SCE(config if)#>sanity-checks attack-filter memory threshold 90 S
CE(config if)#>
```

Related Commands

Command	Description
show interface linecard sanity-checks	

sce-url-database add-entry

Adds a single entry to the protected URL database

sce-url-database add-entry url-wildcard *URL-wildcard-format* **flavor-id** *flavor-id*

Syntax Description

URL-wildcard-format	(* | [*] [Host-Suffix] | [*] [Host-Suffix] / [URL-Prefix [*]] [URL suffix] [? Params-prefix]) See Table 2-4 for examples of how to define the URL.
flavor-id	The ID of the flavor to be applied to the entry. The specified flavor must be the one that was designated for the black list in the pqb file that was applied, other wise the operation will fail.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Use this command to add only a few new entries to the database. Add a large number of new URLs by importing an updated protected URL database file.

Refer to the following table for URL examples..

Table 2-4 Examples for Defining URLs

URL Input	LUT Key Output	Result
*	*:*:*:*	blocks all URLs
*.com	*.com:*:*:*	blocks all URLs in which the host ends with .com
*/media	*:/media:*:*	blocks all URLs in which the path contains only media
*/media*mp3	*:/media*:*mp3:*	blocks all URLs in which the path starts with media and ends with mp3
/?key	*:/*:*:key*	blocks all URLs in which the parameters start with key
*.com/media*mp4?download	*.com:/media*:*mp4:download*	blocks all URLs in which: • the host ends with .com • the path starts with media and ends with mp4 • the parameters start with download

The user executing the command must have write permission for the protected URL database.

.Authorization: admin

Examples

The following example shows how to add an entry to the database. Since the flavor-ID is included in the command, this indicates that it is not present in the import file.

```
SCE>enable 10
Password:<cisco>
SCE#>configure
SCE(config)#interface linecard 0
SCE(config if)#sce-url-database add-entry url-wildcard *.com/media*mp4?download flavor-id
50
SCE(config if)#
```

Related Commands

Command	Description
sce-url-database protection	
sce-url-database import	
show interface linecard sce-url-database	

sce-url-database import

Imports entries from an encrypted or cleartext file into the protected URL database.

sce-url-database import (cleartext-file | encrypted-file *file-name)* **[flavor-id** *flavor-id]*

Syntax Description

file-name	Path and filename of the protected URL database import file.
flavor-id	The ID of the flavor to be applied to all entries in the file. The specified flavor must be the one that was designated for the black list in the pqb file that was applied, otherwise the operation will fail. • If the import file does not contain the flavor per entry, you must specify the flavor in this command. • If the import file does contain the flavor per entry, you may not specify the flavor in this command.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Specify the type of file:

- Clear text file
- Encrypted file: An encrypted file can be imported only if a matching encryption key has been configured. (See **sce-url-database protection.**)

Guidelines for Managing the Protected URL Database

- The user executing the command must have write permission for the protected URL database.
- When a new file is imported, the existing database is cleared before the import. Incremental update is not supported via the import command. Therefore the import file must contain all the relevant URLs, not only new ones to be added to the database.
- Add a large number of new URLs by importing an updated protected URL database file. Typically, if the database is protected this option is used with an encrypted file.
- Add a few new URLs by adding the new URLs using the **sce-url-database add-entry** command.

Protected URL Database Import File

The database import file may either contain cleartext or be encrypted. If the file is encrypted, the matching encryption key must be configured by the database owner.

If the file is encrypted, it must be prefixed with a cleartext header. The encrypted file header format must be exactly as follows:

Encrypted file version: 0x01

Block cipher index: 0x01

Mode of operation index: 0x02

Padder index: 0x02

IV length: 0x10

IV: *<16 unformatted bytes which form the 128 bits IV of the encrypted data >*

Following the header, the following data should appear in AES 128, CFB mode, encrypted format:

A random number (in the range [16…31]) of random bytes, followed by the word "Signed", and then again 32 random bytes.

Each following line represents a single URL.

Protected URL Database Import File Format

[Flavor <tab>] URL

Where:

- Flavor: Flavor-id. The flavor ID must either be included for every line in the file or none of the lines. The flavor must be separated from the URL by a <tab>.
- URL: (* | [*] [Host-Suffix] | [*] [Host-Suffix] / [URL-Prefix [*]] [URL suffix] [? Params-prefix])

  See Table 2-4 for examples of how to define the URL.

Results

- The sce-url-database is first cleared.
- The entries from the file are written to the database.
- Duplicate keys in the file are overwritten with no warning.
- In case of a failure, writing continues to the next entry.

  The total number of failures and a listing of the failed file line numbers are reported when the import is finished.

Authorization: admin

Examples

The following example shows how to import the protected URL database from an encrypted file. Since the flavor-ID is included in the command, this indicates that it is not present in the import file.

```
SCE>enable 10
Password:<cisco>
SCE#>configure
SCE(config)#interface linecard 0
SCE(config if)#sce-url-database import encrypted-file blacklist-file flavor-id 50
SCE(config if)#
```

Related Commands

Command	Description
sce-url-database protection	
sce-url-database add-entry	
show interface linecard sce-url-database	

sce-url-database protection

Configures user authorization for the protected URL database.

Use the **no** form of the command to either remove all protection settings, or to remove only the encryption key.

sce-url-database protection owner (myself | (name *user-name***))**

sce-url-database protection allow-write (all-users | owner-only)

sce-url-database protection allow-lookup (owner-only | no-user)

sce-url-database protection encryption-key *encryption-key*

no sce-url-database protection

no sce-url-database protection encryption-key

Syntax Description

user-name	Username that is defined as the owner of the protected URL database. Cannot be the default username.
encryption-key	The AES encryption key – either 128-, 192-, or 256-bits long. The key is supplied in hexadecimal format and is 32, 48, or 64 hexadecimal digits respectively.
all-users	All users can perform the specified action.
owner-only	Only the owner of the protected URL database can perform the specified action.
no-user	No user can perform the specified action.

Defaults

- By default there is no designated owner.
- Read permission—no-user. This setting is not configurable
- Write permission
  - If no owner has been assigned, the default is **all-users.**
  - If an owner has been assigned, the default is **owner-only.**
- Lookup permission
  - If no owner has been assigned, the default is **all-users**.
  - If an owner has been assigned, the default is **no-user**.
- Encryption key—no key.

Command Modes

Interface Linecard Configuration

Usage Guidelines

When the protected URL database is protected, one user is designated as the owner of the database and only that user can execute the protection CLI commands on the database; the database manipulation commands then being restricted according to the owner configuration. This requires defining the AAA authorization method (either based on local users or based on a TACACS+ server, etc.) and defining at least one user who should be assigned to be the owner of the database.

If the database is defined to be protected, none of the database information (including the owner, the database entries, and the authorization information itself) is accessible to any users, including the relevant saved configuration in the log files and in the relevant SCA BB reports. The database-owner user may change the authorizations using the CLI; however, when any of the protections are relaxed (or all of the protections are relaxed by removing the protections entirely) the database is reset.

In order to ensure the secrecy of the database information, the database entries may be imported to the SCE (using the CLI) in an encrypted form using 128-, 192-, or 256-bit key length AES. The key may be set or updated using the appropriate CLI command; typically, this command should be run over a secure Telnet session.

User Authorization Guidelines:

- The default user cannot be the owner.
- When there is no designated owner, the sce-url-database is unprotected and the contents can be read and modified by any user.
- Only the owner can configure the protection settings. If there is no owner, the database is unprotected and any user has read and write permissions. A user may be configured to be the owner of the database only while no owner user is designated for the database.
- When any protection setting is relaxed, the database is reset. Protection is relaxed in the following cases:
  - Protection is removed completely using the **no sce-url-database protection** command.
  - Write permission is changed from owner-only to all-users.
  - Lookup permission is changed from no-user to owner-only.
- The sce-url-database configuration information is not accessible as part of the running config and startup config files.
  - Protected information is not displayed when a **show** or **more** command is executed on the config files.
  - Protected information is included when a **copy** command is executed on the config files.

Authorization: admin

Examples

The following example shows how to configure protected URL database protection.

```
SCE>enable 10
Password:<cisco>
SCE#>configure
SCE(config)#interface linecard 0
SCE(config if)#sce-url-database protection owner myself
SCE(config if)#sce-url-database protection allow-write all-users
SCE(config if)#sce-url-database protection allow-lookup no-user
SCE(config if)#sce-url-database protection encryption-key AABBCCDDEEFF11223344556677889900
SCE(config if)#
```

Related Commands

Command	Description
sce-url-database import	
show interface linecard sce-url-database protection	
sce-url-database remove-all	
sce-url-database add-entry	

sce-url-database remove-all

Clears the protected URL database

sce-url-database remove-all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

The user executing the command must have write permission for the protected URL database.

.Authorization: admin

Examples

The following example shows how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#>configure
SCE(config)#interface linecard 0
SCE(config if)#sce-url-database remove-all
SCE(config if)#
```

Related Commands

Command	Description
sce-url-database protection	
sce-url-database import	
show interface linecard sce-url-database	

scmp

Enables the Service Control Management Protocol functionality. Use the **no** form of the command to disable the SCMP.

scmp

no scmp

Syntax Description

This command has no arguments or keywords.

Defaults

By default, SCMP is disabled.

Command Modes

Global Configuration

Usage Guidelines

SCMP is a protocol by which an SCE platform communicates with peers such as Cisco routers running ISG to manage subscriber sessions.

SCMP performs the following functions:

- Manages the connection status to all SCMP peer devices
- Encodes and decodes the SCMP messages
- Orders northbound messages per subscriber

When the SCMP is disabled, all subscribers provisioned via this interface are removed.

Authorization: admin

Examples

The following example illustrates how to disable the SCMP.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no scmp
SCE(config)#
```

Related Commands

Command	Description
scmp keepalive-interval	
scmp loss-of-sync-timeout	
scmp name	
scmp reconnect-interval	

scmp subscriber force-single-sce
scmp subscriber id append-to-guid
scmp subscriber send-session-start
no subscriber
show scmp

scmp keepalive-interval

Defines interval between keep-alive messages to the SCMP peer device.

scmp keepalive-interval ***interval***

Syntax Description

interval	Interval between keep-alive messages from the SCE platform to the SCMP peer device.

Defaults

interval = 5 seconds

Command Modes

Global Configuration

Usage Guidelines

The SCE platform sends keep-alive messages to all connected SCMP peer device at the defined interval.

- If a response is received within the defined interval, the keep-alive time-stamp is updated.
- If a response is not received within the defined interval, the connection is assumed to be down; the connection state is changed to not-connected, and the SCMP begins attempts to reconnect.

Authorization: admin

Examples

The following example illustrates how to define the SCMP keepalive message interval.

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE(config)#scmp keepalive-interval 10
SCE(config)#
```

Related Commands

Command	Description
show scmp	

scmp loss-of-sync-timeout

Defines the loss of sync timeout interval; that is the amount of time between loss of connection between the SCE platform and an SCMP peer device and the loss-of-sync event.

scmp loss-of-sync-timeout ***interval***

Syntax Description

interval	Loss of sync timeout interval in seconds

Defaults

interval = 90 seconds

Command Modes

Global Configuration

Usage Guidelines

If the connection between an SCE platform and an SCMP peer device fails, a timer starts. If the configured loss of sync timeout interval is exceeded, the connection is assumed to be not-in-sync, a loss-of-sync event occurs, and the following actions are performed:

- connection status is set to not-in-sync
- all messages are removed from the SCMP buffers
- all subscribers associated with the SCMP peer device are removed

Authorization: admin

Examples

The following example illustrates how to define loss of sync timeout interval.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# scmp loss-of-sync-timeout 120
SCE(config)#
```

Related Commands

Command	Description
show scmp	
scmp reconnect-interval	

scmp name

Adds an SCMP peer device. Use the **no** form of the command to delete the specified SCMP peer device.

scmp name ***name*** **radius** ***host-name*** **secret** ***secret*** **[auth-port** ***auth-port#*** **acct-port** ***acct-port#*** **]**

no scmp name ***name***

Syntax Description

name	Name of the SCMP peer device
host-name	IP address or name of the RADIUS host
secret	RADIUS shared secret
auth-port#	authentication port number
acct-port#	accounting port number

Defaults

Default: Ports configuration as specified in RFC #2865 and RFC #2866

Authentication port = 1812

Accounting port = 1813

Command Modes

Global Configuration

Usage Guidelines

After defining an SCMP peer device, you must associate it with one or more unmapped anonymous groups (see **subscriber anonymous-group name scmp name**). This provides the ability to query the SCMP peer regarding unmapped IP addresses in cases where the SCE platform is not updated when the subscriber session has started (see **scmp subscriber send-session-start**) or in recovery scenarios.

You cannot delete an SCMP device that has anonymous groups assigned to it. Use the **no** form of the **subscriber anonymous-group name scmp name** command to remove all associated anonymous groups before deleting the device.

Authorization: admin

Examples

The following example illustrates how to define an SCMP peer device.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)# scmp name peer_device1 radius radius1 secret abcdef
SCE(config)#
```

Related Commands

Command	Description
subscriber anonymous-group name scmp name	

no subscriber	Use the 'scmp name scmp-name all' option to remove subscribers managed by a specified SCMP peer device
ip radius-client retry limit	
show scmp	

scmp reconnect-interval

Defines the SCMP reconnect interval; that is the amount of time between attempts by the SCE platform to reconnect with an SCMP peer.

scmp reconnect-interval ***interval***

Syntax Description

interval	Interval between attempts by the SCE platform to reconnect with an SCMP peer, in seconds

Defaults

interval = 30 seconds

Command Modes

Global Configuration

Usage Guidelines

The SCE platform attempts to reconnect to the SCMP peer device at the defined intervals by sending an establish peering request message. If a valid reply is received, the SCMP connection state for the SCMP peer is changed, and the SCMP performs the required reconnection operations, such as the following:

- Re-querying the peer regarding all subscribers provisioned by this device
- Querying the peer regarding all anonymous subscribers created using the anonymous group assigned to this peer

Authorization: admin

Examples

The following example illustrates how to define the SCMP reconnect interval.

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE(config)#scmp reconnect-interval 60
SCE(config)#>
```

Related Commands

Command	Description
show scmp	
scmp loss-of-sync-timeout	

scmp subscriber force-single-sce

Configures the SCMP to make the SCMP peer device verify that each subscriber is only provisioned for one SCE platform. This configuration must be enabled in MGSCP deployments. Use the **no** form of the command to disable verifying each subscriber is only provisioned for one SCE platform.

scmp subscriber force-single-sce

no scmp subscriber force-single-sce

Syntax Description

This command has no arguments or keywords.

Defaults

Default is disabled.

Command Modes

Global Configuration

Usage Guidelines

This command takes effect only if it is set before the connection with the SCMP peers is established. Use the **no scmp** and **scmp** commands to stop and then restart the SCMP if active connections exist.

Authorization: admin

Examples

The following example illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#scmp subscriber force-single-sce
SCE(config)#
```

Related Commands

Command	Description
show scmp	
scmp	

scmp subscriber id append-to-guid

Defines the subscriber ID structure for subscribers provisioned via the SCMP interface. Use the **no** form of the command to clear the subscriber ID structure setting.

scmp subscriber id append-to-guid radius-attributes Calling-Station-Id | NAS-Port-Id | User-Name [Calling-Station-Id | NAS-Port-Id | User-Name] [Calling-Station-Id | NAS-Port-Id | User-Name]

no scmp subscriber id append-to-guid

Syntax Description

This command has no arguments.

Defaults

By default, all settings are cleared.

Command Modes

Global Configuration

Usage Guidelines

The GUID is a global unique ID assigned to each subscriber session by the SCMP peer device.

The user can define the structure of the subscriber ID via this command by specifying which of the following RADIUS attributes to include and in which order:

- Calling-Station-Id
- NAS-port
- User-Name

The GUID is always appended at the end of the subscriber ID as defined by this command.

The **no** form of the command clears the subscriber ID structure setting,resulting in no other elements being used with the GUID to form the subscriber ID.

You must disable the SCMP interface before executing this command. (Use the command **no scmp.**)

Authorization: admin

Examples

The following example illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no scmp
SCE(config)#scmp subscriber id append-to-guid radius-attributes User-Name
Calling-Station-Id NAS-Port-Id
SCE(config)#scmp
SCE(config)#
```

Related Commands

Command	Description
scmp	
show scmp	

scmp subscriber send-session-start

Configures the SCMP to make the SCMP peer device push sessions to the SCE platform immediately when the session is created on the peer device. Use the **no** form of the command to disable pushing of sessions from the SCMP peer device to the SCE platform.

scmp subscriber send-session-start

no scmp subscriber send-session-start

Syntax Description

This command has no arguments or keywords.

Defaults

Default is disabled.

Command Modes

Global Configuration

Usage Guidelines

This command takes effect only if it is set before the connection with the SCMP peers is established. Use the **no scmp** and **scmp** commands to stop and then restart the SCMP if active connections exist.

This feature must be disabled in MGSCP deployments.

Authorization: admin

Examples

The following example illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#scmp subscriber send-session-start
SCE(config)#
```

Related Commands

Command	Description
show scmp	

script capture

Begins the recording of a script. It tracks all commands typed until the **script stop** command is used.

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

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.

Authorization: admin

Examples

The following example shows the script capture for the script1.txt.

```
SCE>enable 10
Password:<cisco>
SCE#script capture script1.txt
SCE#cd log
SCE#cd..
SCE#pwd
SCE#script stop
```

Related Commands

Command	Description
script stop	

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>enable 10
Password:<cisco>
SCE#script print script1.txt cd log
cd..
pwd
script stop
SCE#
```

Related Commands

Command	Description
script capture	
script run	

script run

Runs a script. The script may be created using the **script capture** command, or it may be created as a text file containing the appropriate commands.

script run ***script-file-name*** **[halt]**

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

Use this command to run a script that you have previously created using the **script capture** command.

Use the **halt** keyword to break script on errors.

Authorization: admin

Examples

The following example runs the script named monitor.txt, which contains commands to enable the generation of the real-time subscriber usage RDRs for the specified subscribers.

Following is the contents of the file:

```
configure
interface linecard 0
subscriber name Jerry property monitor value 1
subscriber name George property monitor value 1
subscriber name Elaine property monitor value 1
subscriber name Kramer property monitor value 1
```

The following show how to run the script:

```
SCE>enable 10
Password:<cisco>
SCE#script run monitor.txt
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)#subscriber name Jerry property monitor value 1
SCE(config if)#subscriber name George property monitor value 1
SCE(config if)#subscriber name Elaine property monitor value 1
SCE(config if)#subscriber name Kramer property monitor value 1
SCE(config if)#
```

Related Commands

Command	Description
script capture	
script print	

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

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example stops the capturing of a script.

```
SCE>enable 10
Password:<cisco>
SCE#script capture script1.txt
SCE#cd log
SCE#cd..
SCE#pwd
SCE#script stop
SCE#
```

Related Commands

Command	Description
script capture	

service-bandwidth-prioritization-mode

Defines the service bandwidth prioritization mode.

service-bandwidth-prioritization-mode {global | subscriber-internal}

Syntax Description

This command has no arguments.

Defaults

default = subscriber-internal

Command Modes

Interface Linecard Configuration

Usage Guidelines

This parameter configures how bandwidth controllers compete for bandwidth by specifying which assurance level (AL) value is used when allocating bandwidth between bandwidth controllers. The AL can either be taken from either of the following:

- **global** prioritization mode — the global controller AL is taken from current bandwidth controller Assurance Level.
- **subscriber-internal** prioritization mode — the global controller AL of each bandwidth controller is taken from the Primary BWC Relative Priority (the party or "total" bandwidth-controller Relative-Priority value)

Authorization: admin

Examples

The following example shows how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)#service-bandwidth-prioritization-mode global
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard service-bandwidth-prioritization-mode	

service logger

Enables the logger. Use the **no** form of the command to disable the logger. These commands affect all logging activity.

service logger

no service logger

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global Configuration

Usage Guidelines

Authorization: root

Examples

The following example illustrates how to enable the logger.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>service logger
SCE(config)#>
```

Related Commands

Command	Description
show logger	
logger device	
logger device (ROOT level options)	

service management-agent

Enables the management agent. Use the **no** form of this command to disable the management agent.

service management-agent

no service management-agent

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the management agent is enabled.

Command Modes

Global Configuration

Usage Guidelines

Disabling the management agent results in the loss of all functionality supplied by the management agent. Use the **jvm input-string command** to specify a warm-start input string that will save the management agent configuration.

Authorization: root

Examples

The following example illustrates how to disable the management agent.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>no service management-agent
SCE(config)#>
```

Related Commands

Command	Description
jvm input-string	
show management-agent	

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

Passwords that were configured in an encrypted format are not deciphered when password encryption is disabled.

Authorization: admin

Examples

The following example shows the effect of enabling password encryption.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#enable password abcd
SCE(config)#do 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(config)#service password-encryption
SCE(config)#do 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 0 "e2fc714c4727ee9395f324cd2e7f331f"
…
SCE(config)#
```

Related Commands

Command	Description
	enable password

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#service rdr-formatter
SCE(config)#
```

EXAMPLE 2:

The following example disables the RDR-formatter.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no service rdr-formatter
SCE(config)#
```

Related Commands

Command	Description
show rdr-formatter enabled	
rdr-formatter category-number	
rdr-formatter destination	

service telnetd

Enables the 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>enable 10
Password:<cisco>
SCE#config
SCE(config)#service telnetd
SCE(config)#
```

EXAMPLE 2:

The following example disables the Telnet daemon.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#no service telnetd
SCE(config)#
```

Related Commands

Command	Description
show telnet status	
telnet	

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

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 the parameter values that are necessary to complete the initial configuration. It is recommended that you obtain all these values before beginning the setup.

Parameter	Description
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. Maximum length is 20 characters.
admin password	Admin level password. Character string from 4-100 characters beginning with an alpha character.
root password	Root level password. Character string from 4-100 characters beginning with an alpha character.
password encryption status	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 2007
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).
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	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.
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: • 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	Trap manager IP address, community string, and SNMP version (maximum 20).
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 a optical splitter (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)	
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 • 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 links are designated as follows: • The link connected to port1-port2 is by default link-0 • 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?

Command Modes

Privileged EXEC

Usage Guidelines

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
- SNTP 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 *Cisco SCE Platform Installation and Configuration Guide.*

Authorization: admin

Examples

The following example runs the setup utility.

```
SCE>enable 10
Password:<cisco>
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
```

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

Default access list number = 1.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: admin

Examples

The following example displays the configuration of access-list 5.

```
SCE>enable 5
Password:<cisco>
SCE#show access-lists 5
Standard IP access list 5
Permit 10.1.1.0, wildcard bits 0.0.0.255
deny any
SCE#
```

Related Commands

Command	Description
access-list	

show applications file capacity-options

Displays a list of the capacity options available inside an SLI file.

show applications file *filename* capacity options

Syntax Description

filename	The name of the SLI file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

If a capacity option is to be specified in the **application** command, use this command to obtain a listing of the capacity options available for the specified SLI file.

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show applications file application.sli capacity-options
Capacity options defined in file "application.sli ":
"Default" : Default configuration.
"EngageDefaultSE100" : Engage default configuration (typical broadband topology)
"SubscriberLessSE100" : Subscriberless installation topology configuration
SCE#>
```

Related Commands

Command	Description
capacity-option name	
application	

show applications file configuration-data

Displays the configuration data for the specified application (SLI) file.

show applications file *filename* configuration-data

Syntax Description

filename	The name of the SLI file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show applications file application.sli configuration-data
SCE#>
```

Related Commands

Command	Description

show applications file info

Displays information about the specified application (SLI) file.

show applications file *filename* info

Syntax Description

filename	The full path of the SLI file.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show applications file /tffs0/app/eng30102.sli info
Information for file /tffs0/app/eng30102.sli:
Application name: Engage SML Version 3.0 build 35
Using Lib - PL_3.0b31
Using Lib - Classifier_3.0b21
Application help: Entry point of Engage
Originalsource file: H:\work\App\SML\Engage\v3.0\dev\src\com\pcube\apptemplate
main\template_app_main.san
Compilation date: Thu, December 15, 2005 at 12:53:33
Compiler version: SANc v3.00 Build 37 gcc_codelets=true
built on: Tue 08/28/200 04:25:39.;SME plugin v1.1
Object format : 17
Nodes section : 2238864 (=0x222990) bytes, begining at 0xc0
Global section : 112768 (=0x1b880) bytes, begining at 0x222a50
Const section : 5308101 (=0x50fec5) bytes, begining at 0x321cec
Flow filter section : 68 (=0x44) bytes, begining at 0x23e2d0
Xml section : 919756 (=0xe08cc) bytes, begining at 0x23e314
Info section : 338 (=0x152) bytes, begining at 0x31ebe0
Party section : 704 (=0x2c0) bytes, begining at 0x31ed32
Report types section : 3312 (=0xcf0) bytes, begining at 0x31eff2
Alloc nodes section : 7716 (=0x1e24) bytes, begining at 0x31fce2
Capacity options section : 269 (=0x10d) bytes, begining at 0x321b06
Signatures section : 217 (=0xd9) bytes, begining at 0x321c13
Signature section content:
1 signatures:
#0:Thu, December 15, 2005 at 12:53:33SANc v3.00 Build 37 gcc_codelets=true
built on: Tue 08/28/2005 04:25:39.;SME plugin v1.1Engage SML Version 3.0 build 35
Using Lib - PL_3.0b31
Using Lib - Classifier_3.0b21
Report types section content:
There are 53 tags:
-1294967295(=0xb2d05e01), -1294967294(=0xb2d05e02), -1294967292(=0xb2d05e04), -
294967291(=0xb2d05e05), -1294967256(=0xb2d05e28), -1294967255(=0xb2d05e29),
```

```
-124967253(=0xb2d05e2b), -1294967252(=0xb2d05e2c), -1294967251(=0xb2d05e2d),
-129467249(=0xb2d05e2f), -1294967248(=0xb2d05e30), -1294967247(=0xb2d05e31),
-129496246(=0xb2d05e32), -1294967226(=0xb2d05e46), -1294967225(=0xb2d05e47),
-129496724(=0xb2d05e48), -252645376(=0xf0f0f000), -252645374(=0xf0f0f002),
-252645372(=0f0f0f004), -252645371(=0xf0f0f005), -252645360(=0xf0f0f010),
-252645354(=0xf0f0016), -252645353(=0xf0f0f017), -252645352(=0xf0f0f018),
-252645351(=0xf0f0f019) -252645350(=0xf0f0f01a), -252645342(=0xf0f0f022),
-252645328(=0xf0f0f030), -25645327(=0xf0f0f031), -252645312(=0xf0f0f040),
-252645310(=0xf0f0f042), -25264539(=0xf0f0f043), -252645296(=0xf0f0f050),
-252644296(=0xf0f0f438), -252644292(=0f0f0f43c), -252644288(=0xf0f0f440),
-252644246(=0xf0f0f46a), 40(=0x28), 44(=0x2), 77771(=0x12fcb), 77772(=0x12fcc),
88881(=0x15b31), 88882(=0x15b32), 1000000(0xf4240), 11110001(=0xa98671),
11110002(=0xa98672), 11110003(=0xa98673), 1111004(=0xa98674),
11111001(=0xa98a59), 11120001(=0xa9ad81), 11140001(=0xa9fba1),
1150001(=0xaa22b1), 11160001(=0xaa49c1)
SCE#>
```

Related Commands

Command	Description

show applications slot capacity-option

Displays the name of the currently selected capacity option.

show applications slot *slot-number* capacity-option

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: root

Examples

The following example illustrates the use of this command:

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 capacity-option
Configured capacity option is EngageDefaultSCE1000
SCE#>
```

Related Commands

Command	Description
capacity-option name	

show applications slot flow-filter

Displays information related to flow filter rules.

show applications slot ***slot-number*** **flow-filter rule** ***rule number***

show applications slot ***slot-number*** **flow-filter min rule** ***min-rule number*** **max rule** ***max-rule number***

show applications slot ***slot-number*** **flow-filter max-rules**

show applications slot ***slot-number*** **flow-filter default-mode**

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
rule number	Number of the specific flow filter rule. To specify a range of flow filter rules, the first *rule number* is the beginning of the range (use with **min rule**) and the second rule number (use with **max rule**) is the end of the range.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

The following information related to flow filter rules can be displayed:

- Configuration of a specified flow filter rule
- All flow filter rules in a specified range
- Maximum number of flow filter rules
- Default flow filter modes

When one rule number is specified with the **rule** keyword, the configuration (parameter values) of that filter rule is displayed.

Use the **min rule** and **max rule** options together to specify a range of flow filter rules to display.

Use the **max-rules** keyword to display the maximum number of flow filter rules.

Use the **default-mode** keyword to display the default flow filter modes (Drop-true/false, Bypass-true/false)

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to display a specific flow filter rule:

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 flow filter 0
Content of rule # 0:
Ip 1: min=0.0.0.0, max=255.255.255.255, inverse=no.
Ip 2: min=0.0.0.0, max=255.255.255.255, inverse=no.
Port 1: min=0, max=65535, inverse=no.
Port 2: min=0, max=65535, inverse=no.
TOS: min=0x0, max=0xff, inverse=no.
Protocol: value=all.
Network interface: BOTH.
TCP Flags: SYN=ignore, FIN=ignore, PSH=ignore, ACK=ignore,
URG=ignore, RST=ignore.
All-inverse: no.
Action fields:
Bypass-flow: not-active.
Drop-flow: not-active.
Bypass-packet: not-active.
Duplicate TP1: not-active.
Duplicate TP2: not-active.
Duplicate TP3: not-active.
Open flow to Software: disabled.
RUC Data: 0x0
Target PPC: not-active.
Default Class: not-active
Default metering type: not-active
Start Conditional bypass-drop: not-active
Stop Conditional bypass-drop: not-active
Increment-counters: none
SCE#>
```

EXAMPLE 2

The following example illustrates how to display the maximum number of flow filter rules:

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 flow filter max-rules
Flow-filter max rules: 128
This means that valid rule numbers are in the range 0 - 127.
SCE#>
```

Related Commands

Command	Description
flow-filter	

show applications slot handlers

Displays all existing global and party handlers.

show applications slot *slot-number* handlers

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: root

Examples

The following example illustrates the use of this command:

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 handlers
There are 13 handlers.
#0: Global handler 'afterApply' has 0 input, and 0 output params:
name=afterApply, offset=2234732, scope=Global, index=10.
#1: Global handler 'G_linkReportHandler' has 0 input, and 0 output params:
name=G_linkReportHandler, offset=2235576, scope=Global, index=1.
#2: Global handler 'G_linkReportInitHandler' has 0 input, and 0 output params:
name=G_linkReportInitHandler, offset=2234860, scope=Global, index=3.
#3: Global handler 'G_linkReportPeriodicHandler' has 0 input, and 0 output params:
name=G_linkReportPeriodicHandler, offset=2234948, scope=Global, index=0.
#4: Global handler 'G_linkReportWraparoundHandler' has 0 input, and 0 output params:
name=G_linkReportWraparoundHandler, offset=2235060, scope=Global, index=2.
#5: Global handler 'G_packageReportHandler' has 0 input, and 0 output params:
name=G_packageReportHandler, offset=2236820, scope=Global, index=5.
#6: Global handler 'G_packageReportInitHandler' has 0 input, and 0 output params:
name=G_packageReportInitHandler, offset=2236088, scope=Global, index=7.
#7: Global handler 'G_packageReportPeriodicHandler' has 0 input, and 0 output params:
name=G_packageReportPeriodicHandler, offset=2236212, scope=Global, index=4.
#8: Global handler 'G_packageReportWraparoundHandler' has 0 input, and 0 output params:
name=G_packageReportWraparoundHandler, offset=2236340, scope=Global, index=6.
#9: Global handler 'httpContentFilteringKeepAliveHandler' has 0 input, and 0 output
params:
name=httpContentFilteringKeepAliveHandler, offset=2238752, scope=Global, index=11.
#10: Global handler 'insertToHTTPContentFilteringCacheHandler' has 2 input, and 0 output
params:
name=insertToHTTPContentFilteringCacheHandler, offset=2238700, scope=Global, index=12.
Input parameters:
name=keyInP1, scope=Global, variableId=189.
name=categoryIdInP2, scope=Global, variableId=2.
#11: Party handler 'ongoingHandler' has 0 input, and 0 output params:
name=ongoingHandler, offset=2237880, scope=Party, index=8.
#12: Party handler 'set_classification_policy_handler' has 1 input, and 0 output params:
name=set_classification_policy_handler, offset=2238676, scope=Party, index=9.
```

```
Input parameters:
name=new_classification_policy, scope=Party, variableId=2.
SCE#>
```

Related Commands

Command	Description
handler name	

show applications slot lookup

Displays the value of the specified lookup name. Can also be used to display a listing of all existing lookup names or to display information regarding a specific lookup table.

show applications slot ***slot-number*** **lookup** ***lookup-name*** **key** ***key***

show applications slot ***slot-number*** **lookup** ***lookup-name*** **match** ***key***

show applications slot ***slot-number*** **lookup** ***lookup-name*** **first-key**

show applications slot ***slot-number*** **lookup** ***lookup-name*** **next-key** ***key***

show applications slot ***slot-number*** **lookup** ***lookup-name*** **all-key**

show applications slot ***slot-number*** **lookup** ***lookup-name*** **info**

show applications slot ***slot-number*** **lookup-all**

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
lookup-name	Name of the lookup table.
key	Value of the key.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Use the **lookup-all** keyword to display the names of all existing lookup tables (see Example 1).

For a specific **lookup** table, the following key options are available:

- key — display the member of the lookup table with the specified key value
- match — display the members of the lookup table whose keys match the specified key pattern
- first-key — display the first member of the lookup table (no key value is specified in the command)
- next-key — display the member whose key comes after the specified key
- all-key — display all members of the lookup table (no key value is specified in the command)

Use the **info** keyword to display the following information regarding the specified lookup table (see Example 2).

- key type
- value type
- capacity
- number of current inserted items

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to display the names of all existing lookup tables. (Partial output only)

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 lookup-all
Lookup tables names list:
GT_NotificationLUT[0]
GT_NotificationLUT[1]
GT_NotificationLUT[2]
GT_NotificationLUT[3]
GT_NotificationLUT[4]
GT_NotificationLUT[5]
GT_NotificationLUT[6]
GT_NotificationLUT[7]
GT_NotificationLUT[8]
GT_NotificationLUT[9]
GT_NotificationLUT[10]
GT_NotificationLUT[11]
GT_NotificationLUT[12]
GT_NotificationLUT[13]
GT_NotificationLUT[14]
GT_NotificationLUT[15]
GT_NotificationLUT[16]
GT_NotificationLUT[17]
GT_NotificationLUT[18]
GT_NotificationLUT[19]
GT_NotificationLUT[20]
GT_NotificationLUT[21]
GT_NotificationLUT[22]
GT_NotificationLUT[23]
GT_NotificationLUT[24]
GT_NotificationLUT[25]
GT_NotificationLUT[26]
GT_NotificationLUT[27]
GT_NotificationLUT[28]
GT_NotificationLUT[29]
GT_NotificationLUT[30]
GT_NotificationLUT[31]
GT_LUT_ServiceID
GT_LUT_ZoneID
GT_LUT_RuleMap
PL_StreamingUserAgentsList
--More--
SCE#>
```

EXAMPLE 2

The following example illustrates how to display information about a specified lookup table.

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 lookup GT_LUT_PortBasedProtocols info
Lookup name = GT_LUT_PortBasedProtocols
Key type = ip-range
Value type = Uint32
Total capacity = 15
Number of inserted items = 10
SCE#>
```

EXAMPLE 3

The following example illustrates how to find the values for the first two members of a table.

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 lookup GT_LUT_PortBasedProtocols first-key
key = 0.6.1.187:0xffffffff
value = 4
SCE#>show applications slot 0 lookup GT_LUT_PortBasedProtocols next-key
0.6.1.187:0xffffffff
key = 0.6.6.184:0xffffffff
value = 1
SCE#>
```

Related Commands

Command	Description
lookup	

show applications slot replace

Displays information about the configuration and status of the application replace operation, as well as spare memory allocations.

show applications slot *slot-number* replace

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: root

Examples

The following example illustrates the use of this command:

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot replace
Application loaded, ready for replace.
Replace support is enabled (Effective on next application load).
Configured completion criterions:
Time criterion: 60 minutes.
Num-flows criterion: 0 flows.
This means that the replace process will end when no more old flows exist, or 60
minutes pass since the replace process began, whichever occurs first.
Configured spare memory parameters:
code: 1000 bytes
global: 1000 bytes
subscriber: 0 bytes
Current spare memory sizes:
code: 7546965 bytes used out of 7548160.
global: 8362074 bytes used out of 8363264.
subscriber: 2426 bytes used out of 2426.
```

Related Commands

Command	Description
application replace	
replace completion	
replace spare-memory	

show applications slot tunable

Displays the value of the specified tunable or tunables. Can also be used to display a listing of all existing tunables and the format in which the value for each one is displayed.

show applications slot *slot-number* tunable *tunable-name*

show applications slot *slot-number* tunables name *tunable-name* name *tunable-name*

show applications slot *slot-number* all-tunables

show applications slot *slot-number* all-tunables names

show applications slot *slot-number* changed-tunables

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Use the **all-tunables** keyword to display the values of all existing tunables (see Example 1).

Use the **all-tunables names** keyword phrase to display the names of all existing tunables and the format in which the value for each one is displayed (see Example 3).

Use the **changed-tunables** keyword to display all tunables that currently have non-default values (see Example 4).

To display the values for a list of tunables, use the **tunables** form of the command (plural) and then use the **name** keyword before the name of each specific tunable in the list (see example 2). Maximum number of tunables that can be listed is 37.

To display the value of a single tunable, use the tunable form of the command (singular).

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to display current values for all existing tunables. (Partial output only)

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 all-tunables
Application at slot 0 has 319 tunables:
APP_PT_ReportingLevel=10
```

```
APP_PT_ShowDebugReportForModule[0..8]=TRUE,FALSE*8
categoryIdInP2=0
CLS_PT_ReportingLevel=10
CLS_PT_ShowDebugReportForModule[0..5]=TRUE,FALSE*5
FTP_OR_SMTP_CONFLICT_DECISION_USE_FTP=TRUE
GT_CheckSkypeTrafficRate=TRUE
GT_CLS_HTTP_CONTENT_FILTERING_DBAllowCaching=TRUE
GT_CLS_HTTP_CONTENT_FILTERING_DBCacheRefreshThreshold=100
GT_CLS_HTTP_CONTENT_FILTERING_DBCheckKeepAlive=TRUE
GT_CLS_HTTP_CONTENT_FILTERING_DBClassificationPolicy2boolean[0..4999]=FALSE*500
GT_CLS_HTTP_CONTENT_FILTERING_DBDepthPath=0
GT_CLS_HTTP_CONTENT_FILTERING_DBKeepAliveResponseTime=0
GT_CLS_HTTP_CONTENT_FILTERING_DBKeepAliveTimeInterval=30
GT_CLS_HTTP_CONTENT_FILTERING_DBKeepAliveTimeThreshold=10
GT_CLS_HTTP_CONTENT_FILTERING_DBOperationMode=0
GT_CLS_HTTP_CONTENT_FILTERING_DBRepeatWaitingMethod=1
GT_CLS_HTTP_CONTENT_FILTERING_DBWaitingMethod=1
GT_DBG_clsType=0
GT_DBG_packetDumpNumBytes=255
GT_DBG_packetDumpNumOfPackets=1
GT_DBG_packetDumpPort=0
--More--
SCE#>
```

EXAMPLE 2

The following example illustrates how to find the values for a list of a specific tunables:

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 tunables name GT_DBG_packetDumpNumBytes name
GT_DBG_packetDumpNumOfPackets name GT_DBG_packetDumpPort
255
1
0
SCE#>
```

EXAMPLE 3

The following example illustrates how to display a listing of all tunables and their value format. (Partial output only)

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 all-tunables names
Application at slot 0 has 319 tunables:
"APP_PT_ReportingLevel" : Uint8.
"APP_PT_ShowDebugReportForModule" : bool[9].
"categoryIdInP2" : Uint32.
"CLS_PT_ReportingLevel" : Uint8.
"CLS_PT_ShowDebugReportForModule" : bool[6].
"FTP_OR_SMTP_CONFLICT_DECISION_USE_FTP" : bool.
"GT_CheckSkypeTrafficRate" : bool.
"GT_CLS_HTTP_CONTENT_FILTERING_DBAllowCaching" : bool.
"GT_CLS_HTTP_CONTENT_FILTERING_DBCacheRefreshThreshold" : Uint16, minValue=1.
"GT_CLS_HTTP_CONTENT_FILTERING_DBCheckKeepAlive" : bool.
"GT_CLS_HTTP_CONTENT_FILTERING_DBClassificationPolicy2boolean" : bool[5000].
"GT_CLS_HTTP_CONTENT_FILTERING_DBDepthPath" : Uint8, minValue=0.
"GT_CLS_HTTP_CONTENT_FILTERING_DBKeepAliveResponseTime" : Uint32.
"GT_CLS_HTTP_CONTENT_FILTERING_DBKeepAliveTimeInterval" : Uint32.
"GT_CLS_HTTP_CONTENT_FILTERING_DBKeepAliveTimeThreshold" : Uint32.
"GT_CLS_HTTP_CONTENT_FILTERING_DBOperationMode" : Uint8, minValue=0, maxValue=3.
"GT_CLS_HTTP_CONTENT_FILTERING_DBRepeatWaitingMethod" : Uint8, minValue=1, maxValue=5.
"GT_CLS_HTTP_CONTENT_FILTERING_DBWaitingMethod" : Uint8, minValue=0, maxValue=2.
```

```
"GT_DBG_clsType" : Uint8.
"GT_DBG_packetDumpNumBytes" : Uint8.
SCE#>
```

EXAMPLE 4

The following example illustrates how to display a listing of all tunables that currently have a non-default value.

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 changed-tunables
Application at slot 0 has these changed tunables:
GT_GLB_currentMonth=6
GT_SubsNotificationDismissMethod[0..31]=2,0*31
```

Related Commands

Command	Description
tunable	

show applications slot viewable

Displays the value of the specified viewable. Can also be used to display a listing of all existing viewables and the format in which the value for each one is displayed.

show applications slot *slot-number* viewable cpu *cpu#* name *viewable-name*

show applications slot *slot-number* all-viewables names

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
viewable-name	Name of the viewable.
cpu#	The number of the CPU (1-3).

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Use the **all-viewables names** keyword phrase to display the names of all existing viewables and the format in which the value for each one is displayed (see Example 1).

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to display current values for all existing viewables. (Partial output only)

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 all-viewables names
Application at slot 0 has 51 viewables:
"GV_COUNTER_sessionIfLinkIsBelowZero" : Uint8.
"GV_REP_nonReportedDownVolumeInTUR" : int32.
"GV_REP_nonReportedSessionsInTUR" : int32.
"GV_REP_nonReportedUpVolumeInTUR" : int32.
"GV_REP_resetActiveSubscribers" : Uint8.
"GV_REP_tooManyReportsPerPacketCounter" : Uint32.
"G_lnk_downstreamDroppedBytes" : Uint32[2][64].
"G_lnk_downstreamDroppedPackets" : Uint32[2][64].
"G_lnk_upstreamDroppedBytes" : Uint32[2][64].
"G_lnk_upstreamDroppedPackets" : Uint32[2][64].
"G_LURCountersErrors" : Uint16[4][65].
"G_MibLnkCounters" : Uint32[2][64][6].
"G_MibPkgActiveSubs" : Uint32[64].
"G_MibPkgCounters" : Uint32[64][64][6].
"G_pkg_downstreamDroppedBytes" : Uint32[64][64].
"G_pkg_downstreamDroppedPackets" : Uint32[64][64].
"G_pkg_upstreamDroppedBytes" : Uint32[64][64].
```

```
"G_pkg_upstreamDroppedPackets" : Uint32[64][64].
"MMS_maxLengthOfLoop" : Uint32.
"PL_AGED_DB_HIT_MORE_THAN_90_MIN" : Uint32.
"PL_AGED_DB_HIT_UP_TO_15_MIN" : Uint32.
"PL_AGED_DB_HIT_UP_TO_30_MIN" : Uint32.
"PL_AGED_DB_HIT_UP_TO_45_MIN" : Uint32.
"PL_AGED_DB_HIT_UP_TO_60_MIN" : Uint32.
"PL_AGED_DB_HIT_UP_TO_75_MIN" : Uint32.
--More--
SCE#>
```

EXAMPLE 2

The following example illustrates how to find the value for a specific viewable:

```
SCE>enable 15
Password:<cisco>
SCE#>show applications slot 0 viewable cpu 1 name V_numOfLinks
2
SCE#>
```

Related Commands

Command	Description

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the blink status of slot 0.

```
SCE>enable 5
Password:<cisco>
SCE>show blink slot 0
Slot 0 blink status: off
SCE>
```

Related Commands

Command	Description
blink	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the current system calendar.

```
SCE>enable 5
Password:<cisco>
SCE>show calendar
12:50:03 GMT MON November 13 2005
SCE>
```

Related Commands

Command	Description
calendar set	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the current system clock.

```
SCE>enable 5
Password:<cisco>
SCE>show clock
12:50:03 GMT MON November 13 2005
SCE>
```

Related Commands

Command	Description
clock set	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example displays the failure recovery operation mode:

```
SCE>enable 5
Password:<cisco>
SCE>show failure-recovery operation-mode
System Operation mode on failure recovery is: operational
SCE>
```

Related Commands

Command	Description
failure-recovery operation-mode	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows that SCE2000 is the current hostname.

```
SCE>enable 5
Password:<cisco>
SCE>show hostname
SCE2000
SCE>
```

Related Commands

Command	Description
hostname	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the domain and hosts configured.

```
SCE>enable 5
Password:<cisco>
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

Command	Description
hostname	
ip domain-name	
ip name-server	

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

User 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 GigabitEthernet line interface.

The **queue** keyword displays the bandwidth and burst size of a queue in a GigabitEthernet line interface.

Authorization: viewer

Examples

The following example shows the GigabitEthernet details.

```
SCE>enable 5
Password:<cisco>
SCE>show interface gigabitethernet 0/1
SCE>
```

Related Commands

Command	Description
interface gigabitethernet	

show interface global-controller

Displays the rate and assurance level of the specified global controller on the specified interface.

show interface gigabitethernet *slot/port* global-controller *GC#*

Syntax Description

slot/port	The number of the identified slot and port: 0/1, 0/2, 0/3 or 0/4
CG#	Number of the global controller

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface gigabitethernet 0/1 global-controller 0
Name: default Configured BW: 100000 Current BW: 0 [Kbps]
SCE#>
```

Related Commands

Command	Description
global-controller	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows how to use this command.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0
The application assigned to slot 0 is /tffs0/app/eng30102.sli
Silent is off
Configured shutdown is off
Shutdown due to sm-connection-failure is off
Resulting current shutdown state is off
WAP handling is disabled
SCE>
```

Related Commands

Command	Description
interface linecard	

show interface linecard accelerate-packet-drops

Displays the currently configured hardware packet drop mode.

show interface linecard *slot-number* accelerate-packet-drops

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

Authorization: viewer

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 accelerate-packet-drops
Accelerated packet drops mode is enabled
SCE>
```

Related Commands

Command	Description
accelerate-packet-drops	

show interface linecard accurate-accounting

Displays the current status of the accurate accounting mode (enabled or disabled).

show interface linecard *slot-number* accurate-accounting

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: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 accurate-accounting
Accurate accounting is enabled
-----------------------------
SCE#>
```

Related Commands

Command	Description
accurate-accounting	

show interface linecard aggregative-global-controller

Displays information regarding the aggregative global controller for the specified side.

show interface linecard ***slot-number*** **aggregative-global-controller side {subscriber | network}**

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 the side (**network** or **subscriber**) for which to display the aggregative global controller information.

The following information is displaye for the aggregative global controller for the specified side:

- configured bandwidth
- activated mode
- current bandwidth / congestion level

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 aggregative-global-controller side network
Network side AGCs:
AGC# | Limit | Rate | Link0 Enforced | Link1 Enforced
0 200000 0  100000 100000
1 200000 0  100000 100000
2 200000 0  100000 100000
3 200000 0  100000 100000
4 200000 0  100000 100000
5 200000 0  100000 100000
6 200000 0  100000 100000
7 200000 0  100000 100000
8 200000 0  100000 100000
9 200000 0  100000 100000
10 200000 0  100000 100000
11 200000 0  100000 100000
12 200000 0  100000 100000
13 200000 0  100000 100000
14 200000 0  100000 100000
15 200000 0  100000 100000
16 200000 0  100000 100000
17 200000 0  100000 100000
18 200000 0  100000 100000
SCE#>
```

Related Commands

Command	Description
aggregative-global-controller	

show interface linecard analysis layer

Displays the layer currently configured for protocol analysis.

show interface linecard *slot-number* analysis layer

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: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 analysis layer
application
SCE#>
```

Related Commands

Command	Description
analysis layer	

show interface linecard application

Displays the name of the application loaded on 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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the currently loaded application.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 application
/tffs0/app/eng30102.sli
SCE>
```

Related Commands

Command	Description

show interface linecard asymmetric-L2-support

Displays the current asymmetric layer 2 support configuration.

show interface linecard *slot-number* asymmetric-L2-support

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates how to use this command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 asymmetric-L2-support
Asymmetric layer 2 support is disabled
SCE>
```

Related Commands

Command	Description
asymmetric-L2-support	

show interface linecard asymmetric-routing-topology

Displays information relating to asymmetric routing topology.

show interface linecard *slot-number* asymmetric-routing-topology

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Displays the following:

- Current asymmetric routing topology status
- The ratio of TCP unidirectional flows to total TCP flows per traffic processor (*TCP unidirectional flows ratio*).

  The unidirectional flows ratio is displayed only for TCP flows, and reflects the way the flows were opened. It is calculated over the period of time since the SCE platform was last reloaded, or since the counters were last reset.

  To reset the asymmetric routing mode counters, see **clear interface linecard asymmetric-routing-topology counters.**

Note The SCE platform identifies unidirectional flows by default and regardless of the asymmetric routing mode.

Authorization: viewer

Examples

The following example illustrates how to use this command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 asymmetric-routing-topology
Asymmetric Routing Topology mode is disabled
TCP Unidirectional flows ratio statistics:
=========================================
Traffic Processor 1 : 2%
Traffic Processor 2 : 7%
Traffic Processor 3 : 0%
The statistics are updated once every two minutes
SCE>
```

Related Commands

Command	Description
asymmetric-routing-topology enabled	
clear interface linecard asymmetric-routing-topology counters	

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

User 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.

The following information is displayed:

- Protocol Side — Whether the attack detector applies to attacks originating at the subscriber or network side.
- Direction — Whether the attack detector applies to single sided or dual sided attacks.
- Action to take if an attack is detected.
- Thresholds:
  - open-flows-rate — Default threshold for rate of open flows (new open flows per second).
  - suspected-flows-rate — Default threshold for rate of suspected DDoS flows (new suspected flows per second).
  - suspected-flows-ratio — Default threshold for ratio of suspected flow rate to open flow rate.
- Subscriber notification — enabled or disabled.
- Alarm — sending an SNMP trap enabled or disabled.

Authorization: viewer

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>enable 5
Password:<cisco>
SCE>show interface linecard 0 attack-detector 3
Detector #3:
Comment: 'Sample'
Access-list: 1
Effective only for TCP port(s) 21,23,80
Effective for all UDP ports
Protocol|Side|Direction ||Action| Thresholds  |Sub- |Alarm
| |  || |Open flows|Ddos-Suspected flows|notif|
| |  || |rate |rate |ratio | |
--------|----|-----------||------|----------|------------|-------|-----|-----
TCP |net.|source-only|| |  |  | | |
TCP |net.|dest-only || |  |  | | |
TCP |sub.|source-only|| |  |  | | |
TCP |sub.|dest-only || |  |  | | |
TCP |net.|source+dest|| |  |  | | |
TCP |sub.|source+dest|| |  |  | | |
TCP+port|net.|source-only||Block |  |  | | |Yes
TCP+port|net.|dest-only || |  |  | | |
TCP+port|sub.|source-only||Block |  |  | | |Yes
TCP+port|sub.|dest-only || |  |  | | |
TCP+port|net.|source+dest|| |  |  | | |
TCP+port|sub.|source+dest|| |  |  | | |
UDP |net.|source-only|| |  |  | | |
UDP |net.|dest-only || |  |  | | |
UDP |sub.|source-only|| |  |  | | |
UDP |sub.|dest-only || |  |  | | |
UDP |net.|source+dest|| |  |  | | |
UDP |sub.|source+dest|| |  |  | | |
UDP+port|net.|source-only|| |  |  | | |
UDP+port|net.|dest-only || |  |  | | |
UDP+port|sub.|source-only|| |  |  | | |
UDP+port|sub.|dest-only || |  |  | | |
UDP+port|net.|source+dest|| |  |  | | |
UDP+port|sub.|source+dest|| |  |  | | |
ICMP |net.|source-only|| |  |  | | |
ICMP |net.|dest-only || |  |  | | |
ICMP |sub.|source-only|| |  |  | |Yes |
ICMP |sub.|dest-only || |  |  | | |
other |net.|source-only|| |  |  | | |
other |net.|dest-only || |  |  | | |
other |sub.|source-only|| |  |  | | |
other |sub.|dest-only || |  |  | | |
Empty fields indicate that no value is set and configuration from
the default attack detector is used.
SCE>
```

EXAMPLE 2:

The following example displays the configuration of the default attack detector.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 attack-detector default
Protocol|Side|Direction ||Action| Thresholds  |Sub- |Alarm
| |  || |Open flows|Ddos-Suspected Flows|notif|
| |  || |rate |rate |ratio | |
--------|----|-----------||------|----------|------------|-------|-----|-----
TCP |net.|source-only||Report| 1000|  500|50 |No |No
TCP |net.|dest.-only ||Report| 1000|  500|50 |No |No
TCP |sub.|source-only||Report| 1000|  500|50 |No |No
TCP |sub.|dest.-only ||Report| 1000|  500|50 |No |No
TCP |net.|source+dest||Report| 100|  50|50 |No |No
TCP |sub.|source+dest||Report| 100|  50|50 |No |No
TCP+port|net.|source-only||Report| 1000|  500|50 |No |No
TCP+port|net.|dest.-only ||Report| 1000|  500|50 |No |No
TCP+port|sub.|source-only||Report| 1000|  500|50 |No |No
TCP+port|sub.|dest.-only ||Report| 1000|  500|50 |No |No
TCP+port|net.|source+dest||Report| 100|  50|50 |No |No
TCP+port|sub.|source+dest||Report| 100|  50|50 |No |No
UDP |net.|source-only||Report| 1000|  500|50 |No |No
UDP |net.|dest.-only ||Report| 1000|  500|50 |No |No
UDP |sub.|source-only||Report| 1000|  500|50 |No |No
UDP |sub.|dest.-only ||Report| 1000|  500|50 |No |No
UDP |net.|source+dest||Report| 100|  50|50 |No |No
UDP |sub.|source+dest||Report| 100|  50|50 |No |No
UDP+port|net.|source-only||Report| 1000|  500|50 |No |No
UDP+port|net.|dest.-only ||Report| 1000|  500|50 |No |No
UDP+port|sub.|source-only||Report| 1000|  500|50 |No |No
UDP+port|sub.|dest.-only ||Report| 1000|  500|50 |No |No
UDP+port|net.|source+dest||Report| 100|  50|50 |No |No
UDP+port|sub.|source+dest||Report| 100|  50|50 |No |No
ICMP |net.|source-only||Report| 500|  250|50 |No |No
ICMP |net.|dest.-only ||Report| 500|  250|50 |No |No
ICMP |sub.|source-only||Report| 500|  250|50 |No |No
ICMP |sub.|dest.-only ||Report| 500|  250|50 |No |No
other |net.|source-only||Report| 500|  250|50 |No |No
other |net.|dest.-only ||Report| 500|  250|50 |No |No
other |sub.|source-only||Report| 500|  250|50 |No |No
other |sub.|dest.-only ||Report| 500|  250|50 |No |No
SCE>
```

Related Commands

Command	Description
attack-detector	
attack-detector default	
attack-detector <number>	

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

User Exec

Usage Guidelines

Following is a list of options that may be displayed:

- **query IP configured** : displays the configured threshold values and action as follows:
  - **query single-sided IP** *ip-address* **configured** : displays the configured threshold values and action for attack detection for a specified IP address (single-sided detection)
  - **query dual-sided source-IP** *ip-address1* **dest** *ip-address2* **configured** : displays the configured threshold values and action for attack detection between two specified IP addresses (dual-sided detection)
  - **dest-port** *port#:* displays the configured threshold values and action for the specified port. You can include this argument with both single-sided and dual-sided queries.
- **query IP current** : displays the current counters for a specified attack detector for all protocols and attack directions as follows:
  - **query single-sided IP** *ip-address* **current** : displays the current counters for attack detection for a specified IP address (single-sided detection)
  - **query dual-sided source-IP** *ip-address1* **dest** *ip-address2* **current** : displays the current counters for attack detection between two specified IP addresses (dual-sided detection)
  - **dest-port** *port* #: displays the configured threshold values and action for the specified port. You can include this argument with both single-sided and dual-sided queries.
- **current-attacks** : displays all currently handled attacks
- **counters** : displays all attack detection counterd
- **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
- **subscriber-notification redirect:** displays the configuration of subscriber-notification redirection, such as the configured destination and dismissal URLs, and allowed hosts.

Authorization: viewer

Examples

The following examples illustrate the use of this command.

EXAMPLE 1:

The following example displays the configuration of attack detection between two specified IP addresses (dual-sided) for destination port 101.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 attack-filter
query dual-sided source-IP 10.10.10.10 dest 10.10.10.145 dest-port 101 configured
SCE>
```

EXAMPLE 2:

The following example displays all existing forced attack filters.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 attack-filter
force-filter No force-filter commands are set for slot 0
SCE>
```

EXAMPLE 3:

The following example displays the subscriber notification ports.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 attack-filter
subscriber-notification ports
Configured Subscriber notification ports: 100
SCE>
```

Related Commands

Command	Description
attack-filter	
attack-filter force-filter | dont-filter	

show interface linecard cascade connection-status

Displays information regarding the connection between two cascaded SCE 2000 platforms, using the cascade interfaces.

show interface linecard *slot-number* cascade connection-status

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

In order to assist the user when installing a cascaded system and to prevent wrong cabling, this command provides information on the cascade connectivity.

Example 1

The following example shows the output of this command in the case of two cascaded Cisco SCE platforms where the cascade interfaces have not been connected correctly.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade connection-status
SCE is improperly connected to peer
Please verify that each cascade port is connected to the correct port of the peer SCE.
Note that in the current topology, the SCE must be connected to its peer as follows:
Port 0/3 must be connected to port 0/4 at peer
Port 0/4 must be connected to port 0/3 at peer
SCE>
```

Example 2

The following example shows the output of this command in the case of two cascaded Cisco SCE platforms where the cascade interfaces have been connected correctly.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade connection-status
SCE is connected to peer
SCE>
```

Related Commands

Command	Description
connection-mode (sce 2000 only)	

show interface linecard cascade peer-sce-information

Displays information about the peer SCE platform. The data is available even when the two platforms are no longer in cascade connection mode.

show interface linecard *slot-number* cascade peer-sce-information

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

Example 1

The following example shows typical output of this command when the two SCE platforms are connected correctly.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade peer-sce-information
Peer SCE's IP address is 10.10.10.10
SCE>
```

Example 2

The following example shows typical output of this command when the two SCE platforms are not connected correctly.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade peer-sce-information
SCE is improperly connected to peer.
For further information, please consult cli show "cascade connection-status" command
Last known peer SCE's IP address was 10.10.10.10
```

Related Commands

Command	Description
connection-mode (SCE 2000 platform)	
connection-mode (SCE 1000 platform)	

show interface linecard cascade redundancy-status

Displays the current redundancy-status of the SCE platform.

show interface linecard *slot-number* cascade redundancy-status

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows typical output of this command.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 cascade redundancy-status
Redundancy status is active
SCE>
```

Related Commands

Command	Description
connection-mode (SCE 2000 platform)	
connection-mode (SCE 1000 platform)	

show interface linecard connection-mode

Shows the current configuration of the SCE platform link connection.

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

Example 1

The following example shows typical output of this command for a single SCE 2000 platform.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 connection-mode
slot 0 connection mode
Connection mode is inline
slot failure mode is bypass
Redundancy status is active
SCE>
```

Example 2

The following example shows typical output of this command for a cascaded SCE 2000 platform.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 connection-mode
slot 0 connection mode
Connection mode is inline-cascade
slot 0 sce-id is 1
slot 0 is secondary
slot 0 is connected to peer
slot failure mode is bypass
Redundancy status is standalone
SCE>
```

Related Commands

Command	Description
connection-mode (SCE 2000 platform)	
connection-mode (SCE 1000 platform)	

show interface linecard control-exception-traffic

Displays the exception configuration, both as configured by the user and the actual configuration in the DP. (The actual configuration may differ from the user configuration when the system connection mode is '*receive-only* '.)

show interface linecard *slot-number* control-exception-traffic

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: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 control-exception-traffic
Exception Configuration:
------------------------
NON_IP : BYPASS
IP_BROD : BYPASS
IP_ERR : BYPASS
TTL_ERR : BYPASS
GEN_PARSER_E: BYPASS
PPP_PROTOCOL: BYPASS
ARP  : BYPASS
L2TP_CONTROL: BYPASS
L2TP_OFFSET : BYPASS
Note that the actual DP configuration may differ from the shown configuration
Actual configuration depends on the Connection Mode.
SCE#>
```

Related Commands

Command	Description
control-exception-traffic	

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

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Specify any of the optional keywords to display only the desired counters.

The **VAS-traffic-bandwidth** option is supported by the SCE 2000 platform only.

Authorization: viewer

Examples

The following example shows the hardware counters for the Linecard Interface.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 counters
DP packets in: 340
DP packets out: 340
DP IP packets in: 340
DP Non-IP packets: 0
DP IP packets checksum err: 0
DP IP packets length err: 0
DP IP broadcast packets: 0
DP IP fragmented packets: 0
DP IP packets with TTL=0 err: 0
DP Non TCP/UDP packets: 0
DP TCP/UDP packets checksum err: 0
DP ARP packets: 0
DP PPP compressed packets: 0
DP packets dropped: 0
DP tuples to FF: 340
DP tuples from CLS: 340
DP L7 Filter congested packets: 0
DP VLAN packets: 0
DP MPLS packets: 0
DP parse errors: 0
DP IPinIP skipped packets: 0
DP no payload packets: 53
DP self-IP packets: 0
DP tunneled packets: 0
DP L2TP control packets: 0
DP L2TP packets with offset: 0
```

```
traffic-counters information:
-----------------------------
Counter 'myCounter' value: 0 L3 bytes. Rules using it: None.
1 counters listed out of 36 available
...
SCE>
```

Related Commands

Command	Description
clear interface linecard	

show interface linecard counters dropped-bytes

Displays the number of dropped bytes according to mode and group.

show interface linecard *slot-number* counters dropped-bytes

The **VAS-traffic-dropped-bytes** option is supported on the SCE 2000 4xGBE platform only.

show interface linecard *slot-number* counters VAS-traffic-dropped-bytes

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

The **VAS-traffic-dropped-bytes** option is supported by the SCE 2000 4xGBE platform only.

Dropped bytes (bytes dropped due to exceeding the provisioned bandwidth) can be counted by either of the following mechanisms:

- by global controller (default)
- by queue

Note that the dropped bytes counters and provisioned bandwidth can also be accessed via SNMP, by viewing the following MIB objects:

- global controller:
  - globalControllersBandwidth
  - globalControllersDroppedBytes
- queue:
  - txQueuesBandwidth
  - txQueuesDroppedBytes

Authorization: root

Examples

The following examples show how to use this command.

EXAMPLE 1

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 counters dropped-bytes
interface 1 - dropped bytes
-----------------------------
Supporting 16 global-controllers. Only non-zero values appear.
interface 2 - dropped bytes
```

```
------------------------------
Supporting 16 global-controllers. Only non-zero values appear.
SCE#>
```

EXAMPLE 2

This example illustrates the **VAS-traffic-dropped-bytes** option. Note that VAS traffic forwarding must be enabled (see **VAS-traffic-forwarding**). (Partial output only)

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 counters VAS-traffic-dropped-bytes
Traffic bytes received from a VAS server and dropped [L3 bytes]:
Port 1 Port 2 Port 3 Port 4
---------- ---------- ---------- ----------
VAS server id 0:  0  0  0  0
VAS server id 1:  0  0  0  0
VAS server id 2:  0  0  0  0
VAS server id 3:  0  0  0  0
VAS server id 4:  0  0  0  0
VAS server id 5:  0  0  0  0
Traffic bytes dropped instead of being sent to a VAS server [L3 bytes]:
Port 1 Port 2 Port 3 Port 4
---------- ---------- ---------- ----------
VAS server id 0:  0  0  0  0
VAS server id 1:  0  0  0  0
VAS server id 2:  0  0  0  0
VAS server id 3:  0  0  0  0
VAS server id 4:  0  0  0  0
--More-
```

Related Commands

Command	Description
vas-traffic-forwarding	

show interface linecard counters flow-filter

Displays the linecard interface flow filter counters.

show interface linecard *slot-number* counters flow-filter

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: root

Examples

The following examples shows shows the flow filter counters.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0counters flow-filter
Flow Filter Rules Counters
--------------------------
FF counter #0: 0
FF counter #1: 0
FF counter #2: 0
FF counter #3: 0
FF counter #4: 0
FF counter #5: 0
FF counter #6: 0
FF counter #7: 0
FF counter #8: 0
FF counter #9: 0
FF counter #10: 0
FF counter #11: 0
FF counter #12: 0
FF counter #13: 0
FF counter #14: 0
FF counter #15: 0
FF counter #16: 0
FF counter #17: 0
FF counter #18: 0
FF counter #19: 0
FF counter #20: 0
FF counter #21: 0
FF counter #22: 0
FF counter #23: 0
FF counter #24: 0
FF counter #25: 0
FF counter #26: 0
FF counter #27: 0
FF counter #28: 0
FF counter #29: 0
```

```
FF counter #30: 0
FF counter #31: 0
FF counter #32: 0
FF counter #33: 0
FF counter #34: 0
FF counter #35: 0
FF counter #36: 5910
FF counter #37: 0
FF counter #38: 0
FF counter #39: 5910
FF counter #40: 4429
FF counter #41: 0
FF counter #42: 4429
FF counter #43: 3718
FF counter #44: 0
FF counter #45: 0
FF counter #46: 0
FF counter #47: 0
FF counter #48: 0
FF counter #49: 0
FF counter #50: 0
FF counter #51: 0
FF counter #52: 0
FF counter #53: 195
FF counter #54: 195
FF counter #55: 142
```

Command	Description
show interface linecard counters	
clear interface linecard counters	

show interface linecard duplicate-packets-mode

Displays the currently configured duplicate packets mode.

show interface linecard *slot-number* duplicate-packets-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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of this command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 duplicate-packets-mode
Packet duplication of flows due to Delay Sensitive <bundles>is enabled
Packet duplication of flows due to No-Online-Control <set-flow>is enabled
Packet duplication of flows due to No-Online-Control <set-flow>ratio percent is 70
Packet duplication in case of shortage is enabled
SCE>
```

Related Commands

Command	Description

show interface linecard flow-aging default-timeout

Displays the default timeouts for flow aging.

show interface linecard *slot-number* flow-aging default-timeout

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: root

Examples

The following examples show how to use this command.

EXAMPLE 1

This example shows the standard output of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 flow-aging default-timeout
TCP-Establishment default flow aging timeout = 10 seconds
TCP-Data default flow aging timeout = 120 seconds
UDP default flow aging timeout = 10 seconds
Non TCP/UDP default flow aging timeout = 10 seconds
SCE#>
```

EXAMPLE 2

This example shows the output of this command when asymmetric routing is enabled..

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 flow-aging default-timeout
TCP-Establishment default flow aging timeout = 10 seconds
TCP-Data default flow aging timeout = 120 seconds
UDP default flow aging timeout = 10 seconds
Non TCP/UDP default flow aging timeout = 10 seconds
Default flow aging timeouts in Asymmetric Routing topologies
============================================================
TCP-Establishment default flow aging timeout = 20 seconds
TCP-Data default flow aging timeout = 120 seconds
UDP default flow aging timeout = 20 seconds
Non TCP/UDP default flow aging timeout = 20 seconds
SCE#>
```

Related Commands

Command	Description
flow-aging default-timeout	

show interface linecard flow-capture

Displays the flow capture status.

show interface linecard *slot-number* flow-capture

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: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 flow-capture
Flow Capture Status:
--------------------
Flow Capture Status:  RECORDING
Recording Rule name:  FlowCaptureRule
Buffer Capacity (bytes): 50000
Capacity Usage:  100
Time limit (sec):  45
Number of recorded packets: 7800
SCE#>
```

Related Commands

Command	Description
debug flow-capture	
flow-capture controllers	
traffic-rule	

show interface linecard flow-filter

Displays data relating to flow filtering.

show interface linecard *slot-number* flow-filter default-mode|partitions

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

Use one of two keywords:

- **default-mode** - Displays the current flow-filter default mode
- **partitions** - Displays the current flow-filter partitions

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 flow-filter partitions
There are 1 flow-filter partitions defined:
Partition 'ignore_filter' uses rules 4 - 35, total 32 Rules.
SCE#>
```

Related Commands

Command	Description
flow-filter	

show interface linecard flow-open-mode

Displays the currently configured flow open mode.

show interface linecard *slot-number* flow-open-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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of this command.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 flow-open-mode
Enhanced flow open mode is disabled
Asymmetric layer 2 support is disabled
Note that other settings may override all/part of the Enhanced Flow Open mode, e.g. VAS,
TCP no bypass est, etc.(in which cases will behave as in the classical mode)
SCE>
```

Related Commands

Command	Description
flow-open-mode	

show interface linecard hosts info

Displays the current hosts configuration information (aging timeout and max hosts).

show interface linecard *slot-number* hosts info

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: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 hosts info
Hosts aging timeout = 600 seconds
Hosts number lower limit (per traffic processor) = 50000
SCE>
```

Related Commands

Command	Description
hosts aging-timeout	
hosts max-hosts	

show interface linecard ip-tunnel

Displays the current IP tunnel configuration.

show interface linecard *slot-number* 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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of the **show interface linecard ip-tunnel** command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 ip-tunnel
no IP tunnel
SCE>
```

Related Commands

Command	Description
ip tunnel	

show interface linecard ip-tunnel IPinIP

Displays the current IPinIP configuration.

show interface linecard ***slot-number*** **IP-tunnel IPinIP**

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows how to use this command.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 ip-tunnel IPinIP
IPinIP skip mode is enabled
IPinIP DSCP skip mode is disabled
SCE>
```

Related Commands

Command	Description
ip-tunnel IPinIP skip	
ip-tunnel IPinIP DSCP-marking-skip	

show interface linecard l2tp

Displays the currently configured L2TP support parameters.

show interface linecard *slot-number* l2tp

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of the **show interface linecard L2TP** command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 l2tp
L2TP identify-by port-number 1701
SCE>
```

Related Commands

Command	Description
l2tp identify-by	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the configured link mode for the Linecard Interface.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 link mode
Link mode on port1-port2
Current link mode is  :forwarding
Actual link mode on active is :forwarding
Actual link mode on failure is :monopath-bypass
SCE>
```

Related Commands

Command	Description
link mode	

show interface linecard link-to-port-mappings

Displays the link ID to port ID mappings.

show interface linecard *slot-number* link-to-port-mappings

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the link ID to port ID mapping for the Linecard Interface.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 link-to-port-mappings
Link Id | Upstream Port <Out>| Downstream Port <Out>
-------------------------------------------------------
0  | 0/2  | 0/1
SCE>
```

Related Commands

Command	Description

show interface linecard mac-mapping

Displays the linecard MAC mapping information.

show interface linecard *slot-number* mac-mapping

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the MAC mapping information.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 mac-mapping
MAC mapping status is: disabled
MAC mapping default mapping is: none set
MAC mapping dynamic insertion to table is enabled
SCE>
```

Related Commands

Command	Description
show interface linecard mac-resolver arp	
mac-resolver	

show interface linecard mac-resolver arp

Displays a listing of all IP addresses and corresponding MAC addresses currently registered in the MAC resolver database.

show interface linecard 0 mac-resolver arp

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows how to display the entries in the MAC-resolver ARP database.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 mac-resolver arp
There are no entries in the mac-resolver arp database
SCE>
```

Related Commands

Command	Description
mac-resolver arp	

show interface linecard max-sustained-bw

Displays estimated maximum bandwidth.

show interface linecard *slot-number* max-sustained-bw

show interface linecard *slot-number* max-sustained-bw-by-active-subscribers

show interface linecard *slot-number* max-sustained-bw-by-cpu-utilization

show interface linecard *slot-number* max-sustained-bw-by-memory-utilization

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

The following options area available for display:

- **max-sustained-bw** — estimated maximum bandwidth
- **max-sustained-bw-by-active-subscribers** — estimated maximum bandwidth used by active subscribers
- **max-sustained-bw-by-cpu-utilization** — estimated maximum bandwidth by cpu utilization
- **max-sustained-bw-by-memory-utilization** — estimated maximum bandwidth by memory utilization

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 max-sustained-bw
The traffic bw is low then threshold definition for max bw estimation
The threshold is define to 1Mbps
SCE#>
```

Related Commands

Command	Description
show interface linecard max-sustained-subscribers	

show interface linecard max-sustained-subscribers

Displays estimated maximum number of sustained subscribers.

show interface linecard *slot-number* max-sustained-subscribers

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: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 max-sustained-subscribers
The traffic bw is low then threshold definition for max bw estimation
The threshold is define to 1Mbps
SCE#>
```

Related Commands

Command	Description
show interface linecard max-sustained-bw	

show interface linecard mpls

Displays the current MPLS tunnelling configuration.

show interface linecard *slot-number* mpls

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of this command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 mpls
MPLS Traffic-Engineering skip
SCE>
```

Related Commands

Command	Description

show interface linecard mpls vpn

Displays information about MPLS configuration and current VPN mappings.

show interface linecard *slot-number* mpls vpn
[bypassed-vpns][non-vpn-mappings][pe-database [pe-id *pe-ip*]]

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
bypassed	VPNs Displays all currently bypassed VPNs, grouped by downstream label
non-VPN-mappings	Displays the mappings of upstream labels that belong to non-VPN flows
PE-database	Displays the configured PE routers and their interfaces. If a PE-ID is specified, only that PE is displayed.
pe-ip	IP address of the specified PE router.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

The following information can be displayed:

- OS counters (current number of subscribers and various types of mappings)
- bypassed VPNs
- non-VPN-mappings
- PE router configuration

If no keyword is used, the OS counters are displayed (current number of subscribers and various types of mappings).

Use the **PE-database** keyword to display information about all currently configured PE routers. Include the **PE-ID** argument to specify a particular PE router to display.

Authorization: viewer

Examples

The following example illustrates the use of the **show interface linecard MPLS** command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 mpls
MPLS/VPN auto-learn mode is enabled.
MPLS based VPNs with subscribers mappings: 2 used out of 2015 max
Total HW MPLS/VPN mappings utilization: 4 used out of 57344 max
MPLS/VPN mappings are divided as follows:
downstream VPN subscriber mappings: 4
upstream VPN subscriber mappings: 0
non-vpn upstream mappings: 0
downstream bypassed VPN mappings: 0
upstream bypassed VPN mappings: 0
SCE>
```

Related Commands

Command	Description
mpls	
clear interface linecard mpls vpn	
mpls vpn pe-id	

show interface linecard mpls vpn (ROOT level options)

Displays MPLS VPN information available only at the root authorization level.

show interface linecard *slot-number* mpls vpn validity-checks

show interface linecard *slot-number* mpls vpn pe-database alldata

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

The following options are available for display at the root authorization level:

- **MPLS VPN validity-checks** — Current configuration of the MPLS VPN validity check mechanisms
- **MPLS VPN PE-database AllData** — Hidden information regarding the PE routers database for debug purposes.

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 mpls vpn validity-checks
Current MPLS mode is: MPLS Traffic-Engineering skip
--Note that the MPLS/VPN validity checks are only active when the system is in
MPLS/VPN auto-learn mode--
Mpls Validity checks parameters:
Upstream Labels Aging:  enabled Aging time: 10 minutes
Unidirectional TCP detection: enabled
Invalidity threshold:  20
Bypassed VPNs aging time: 10 minutes
SCE#>
```

Related Commands

Command	Description
show interface linecard mpls vpn	
mpls vpn validity-checks	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the link mapping for the Linecard Interface.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 physically-connected-links
slot 0 is connected to link-0 and link-1
SCE>
```

Related Commands

Command	Description
connection-mode (SCE 2000 platform)	

show interface linecard sanity-checks

Displays information relating to the sanity check configuration.

show interface linecard *slot-number* sanity-checks status

show interface linecard *slot-number* sanity-checks attack-filter [memory | times]

show interface linecard *slot-number* sanity-checks control-watchdog-monitor

show interface linecard *slot-number* sanity-checks disk-rw-test

show interface linecard *slot-number* sanity-checks event-counters

show interface linecard *slot-number* sanity-checks intensive-cpu-consuming-flows

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

The following options are available:

- status — Displays the current status (enabled or disabled) of all sanity checks.
- attack-filter — Displays information relating to the status and recent history of the attack filter, or specific configuration of one of the following options:
  - memory threshold — Use the **memory** keyword with the **attack-filter** option to display configured value for the attack filter memory threshold.
  - time constants — Use the **times** keyword with the **attack-filter** option to display the configured values for the following attack filter time constants:

    – filter-cycle-time

    – max-attack-time
- control-watchdog-monitor — Displays the current status (enabled or disabled) and configuration of the control-watchdog-monitor sanity check.
- disk-rw-test — Displays the current status (enabled or disabled) and configuration of the disk-rw-test sanity check.
- event-counters — Displays the current status (enabled or disabled) and configuration of all event counter sanity checks.
- intensive-cpu-consuming-flows — Displays the current status (enabled or disabled) and configuration of the intensive-cpu-consuming-flows sanity check.

Authorization: root

Examples

The following examples show how to use this command.

EXAMPLE 1

The following example shows how to display the attack filter status and recent history.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 sanity-checks attack-filter
Attack filter: enabled.
Counters last cleared 247206 seconds ago.
Accumulated shortage time: 0.000 seconds
Current state: Peace time, waiting for attack.
Accumulated filtering times and current status for interface 0:
Total aggregate filtering time: 0 seconds.
Last filtering: at least 247206 seconds ago.
Attack ICMP   : 0 seconds, Inactive
Attack UDP   : 0 seconds, Inactive
Attack UDP Fragments : 0 seconds, Inactive
Attack TCP SYN  : 0 seconds, Inactive
Attack TCP SYN + ACK : 0 seconds, Inactive
Attack TCP SYN + RST : 0 seconds, Inactive
Attack TCP No-SYN + RST : 0 seconds, Inactive
Attack TCP Fragment  : 0 seconds, Inactive
Accumulated filtering times and current status for interface 1:
Total aggregate filtering time: 0 seconds.
Last filtering: at least 247206 seconds ago.
Attack ICMP   : 0 seconds, Inactive
Attack UDP   : 0 seconds, Inactive
Attack UDP Fragments : 0 seconds, Inactive
Attack TCP SYN  : 0 seconds, Inactive
Attack TCP SYN + ACK : 0 seconds, Inactive
Attack TCP SYN + RST : 0 seconds, Inactive
Attack TCP No-SYN + RST : 0 seconds, Inactive
Attack TCP Fragment  : 0 seconds, Inactive
SCE#>
```

EXAMPLE 2

The following example shows how to display the currently configured values for the attack filter time constants.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 sanity-checks attack-filter times
Filtering cycle: 3600 seconds.
Max attack time: 86400 seconds.
SCE#>
```

EXAMPLE 3

The following example shows how to display the status of all sanity checks.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 sanity-checks status
Sanity Checks Status:
Test-Packets: enabled.
Counters-Test: enabled.
Classifier-Aging: enabled.
Attack filter: enabled.
Event Counter Sanity Check 'Traffic-Processor-Logger-Errs' : enabled.
Event Counter Sanity Check 'Master-Processor-Logger-Errs'  : enabled.
Event Counter Sanity Check 'Flow-ID-Allocations-Failed'           : enabled.
```

```
Event Counter Sanity Check 'HW-Interrupts'     : enabled.
intensive-cpu-consuming-flows: enabled.
SCE#>
```

EXAMPLE 4

The following example shows how to display the status and currently configured values for the event counter sanity checks.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 sanity-checks event-counters
-------------------------------------------------------------------
Event Counter Sanity Check 'Traffic-Processor-Logger-Errs' : enabled Threshold: 10
Normalizer Validation Value: 100000
-------------------------------------------------------------------
Event Counter Sanity Check 'Master-Processor-Logger-Errs' : enabled Threshold: 6000000
Normalizer Validation Value: 0
-------------------------------------------------------------------
Event Counter Sanity Check 'Flow-ID-Allocations-Failed' : enabled Threshold: 2500
Normalizer Validation Value: 1000
-------------------------------------------------------------------
Event Counter Sanity Check 'HW-Interrupts' : enabled  Threshold: 2500 Normalizer
Validation Value: 1000
-------------------------------------------------------------------
SCE#>
```

EXAMPLE 5

The following example shows how to display the status and currently configured values for the intensive-cpu-consuming-flows sanity check.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 sanity-checks intensive-cpu-consuming-flows
intensive-cpu-consuming-flows: enabled.
min-packets-threshold: 10.
max-packets-threshold: 10000.
aggregated-packet-rate: 10.
action: bypass.
trigger: shortage-only.
SCE#>
```

Related Commands

Command	Description
sanity-checks	

show interface linecard sce-url-database

Displays the contents of the protected URL database.

Can also be used to look for a specific URL and display the related flavor ID.

show interface linecard *slot-number* sce-url-database

show interface linecard *slot-number* sce-url-database url *url*

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
url	The specific URL to lookup in the sce-url-database.

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

- In order to display the contents of the protected URL database, it must have all protection removed and no assigned owner. If there is an assigned owner, the database is protected and cannot be displayed.
- In order to display the flavor ID of a specific URL, the user executing the command must have lookup permission for the protected URL database.

Authorization: admin

Examples

The following example shows how to use this command

```
SCE>enable 10
Password:<cisco>
SCE#show interface linecard 0 sce-url-database
SCE#
```

Related Commands

Command	Description
sce-url-database protection	
show interface linecard sce-url-database	

show interface linecard sce-url-database protection

Displays the following current protected URL database protection settings:

- owner username
- current protection settings
- whether a key is configured

show interface linecard *slot-number* sce-url-database protection

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows how to use this command

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 sce-url-database protection
Protection Domain BLACK_LIST_DOMAIN Status:
Domain owner:black
Read is allowed to no user
Write is allowed to user black only
Lookup is allowed to no user
Encryption key is not set
SCE>
```

Related Commands

Command	Description
sce-url-database protection	
show interface linecard sce-url-database	

show interface linecard service-bandwidth-prioritization-mode

Displays the currently configured service bandwidth prioritization mode.

show interface linecard *slot-number* service-bandwidth-prioritization-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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of this command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 service-bandwidth-prioritization-mode
Service bandwidth prioritization mode is: Subscriber Internal
SCE>
```

Related Commands

Command	Description
service-bandwidth-prioritization-mode	

show interface linecard shutdown

Displays the current shutdown state.

show interface linecard *slot-number* shutdown

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the linecard Interface shutdown mode.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 shutdown
off
SCE>
```

Related Commands

Command	Description
shutdown	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the Linecard Interface silent mode.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 silent
off
SCE>
```

Related Commands

Command	Description
silent	

show interface linecard statistics-logging

Displays linecard statistics logging information.

show interface linecard *slot-number* statistics-logging [frequency]

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

Use the **frequency** keyword to display the configured frequency of the statistics slogging.

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 statistics-logging "
Statistics logging on slot 0 is enabled
SCE#>
```

Related Commands

Command	Description
statistics-logging	

show interface linecard subscriber

Displays subscribers meeting specified criteria.

show interface linecard *slot-number* subscriber [amount] [*prefix* prefix] [suffix *suffix*] [property *propertyname* equals|bigger-than|less-than *property-val*] [all-names]

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

User Exec

Usage Guidelines

Use this command to display names of subscribers or the number of 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** keyword to display the number of subscribers meeting the criteria rather than listing actual subscriber names.

Use the **all-names** keyword to display the names of all subscribers currently in the SCE platform subscriber database.

Authorization: viewer

Examples

The following examples illustrate the use of this command.

EXAMPLE 1

Following is an example that lists the number of subscribers with the prefix ‘gold’ in the subscriber name

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber amount prefix gold
There are 40 subscribers with name prefix 'gold'.
SCE>
```

EXAMPLE 2

Following is an example that lists all subscribers currently in the SCE platform subscribers database.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber all-names
There are 8 subscribers in the database.
john_doe
mary_smith
david_jones
betty_peters
bill_jackson
jane_doe
bob_white
andy_black
SCE>
```

Related Commands

Command	Description
subscriber name property	

show interface linecard subscriber aging

Displays the subscriber aging configuration 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

User Exec

Usage Guidelines

Use the **anonymous** keyword to display the subscriber aging configuration for anonymous subscribers.

Use the **introduced** keyword to display the subscriber aging configuration for introduced subscribers.

Authorization: viewer

Examples

The following is an example of how to display the aging of introduced subscribers.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber aging introduced
Introduced subscriber aging is enabled.
Introduced subscriber aging time is 30 minutes.
SCE>
```

Related Commands

Command	Description
subscriber aging	

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

User Exec

Usage Guidelines

If no **group-name** is specified, all anonymous subscribers in all groups are displayed.

Authorization: viewer

Examples

The following is an example of how to display the number of subscribers in the anonymous subscriber group anon1.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber anonymous amount name anon1
SCE>
```

Related Commands

Command	Description
clear interface linecard subscriber	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following is an example of how to display the anonymous subscriber groups.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber anonymous-group all
name   IP range  Template #
----   --------  ----------
Group1  10.10.10.10/99  0
1 anonymous groups are configured
SCE>
```

Related Commands

Command	Description

show interface linecard subscriber db counters

Displays the subscriber database counters.

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

User Exec

Usage Guidelines

Authorization: viewer

Counter Definitions

The following sections present definitions of the counters displayed in the output of this command.

Current values:

Subscribers: Number of currently existing subscribers (excluding subscribers waiting to be removed).

Introduced subscribers: Number of introduced subscribers.

Anonymous subscribers: Number of anonymous subscribers.

Subscribers with mappings: Number of subscribers with mappings.

Single non-VPN IP mappings: Number of mappings to single IP addresses that are not within a VPN.

non-VPN IP Range mappings: Number of mappings to ranges of IP addresses that are not within a VPN.

IP Range over VPN mappings: Number of mappings to ranges of IP addresses that are within a VPN.

Single IP over VPN mappings: Number of mappings to single IP addresses that are within a VPN.

MPLS/VPN mappings (appears only if MPLS/VPN-based subscribers are enabled): Total number of MPLS/VPN mappings used out of maximum available.

Note This value reflects the total number of MPLS/VPN mappings currently used, not only the mappings used by MPLS/VPN-based subscribers. Bypassed VPNs and non-VPN labels also consume MPLS/VPN mappings.

MPLS based VPNs with subscriber mappings (appears only if MPLS/VPN-based subscribers are enabled): Number of VPNs that currently have logged-in subscribers.

VLAN based subscribers (appears only if VLAN-based subscribers are enabled): Number of VLAN based VPNs with subscribers.

Subscribers with open sessions: Number of subscribers with open flows (sessions).

Subscribers with TIR mappings: Number of subscribers with mapping to a TP-IP range.

Sessions mapped to the default subscriber: Number of open flows (sessions) related to the default party.

Peak values:

Peak number of subscribers with mappings:

Peak number occurred at:

Peak number cleared at:

Event counters:

Subscriber introduced: Number of login calls resulting in adding a subscriber.

Subscriber pulled: Number of pullResponse calls.

Subscriber aged: Number of aged subscribers.

Pull-request notifications sent: Number of pull request notifications sent.

State notifications sent: Number of state change notifications sent to peers.

Logout notifications sent: Number of logout events.

Subscriber mapping TIR contradictions: Number of contradicting configured TIRs that are invalid.

Examples

The following examples illustrate the output for this command.

EXAMPLE 1

The following example shows the output for a system with MPLS/VPN-based subscribers enabled:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber db counters
Current values:
===============
Subscribers: 3 used out of 9999 max.
Introduced/Pulled subscribers: 3.
Anonymous subscribers: 0.
Subscribers with mappings: 3 used out of 9999 max.
Single non-VPN IP mappings: 1.
non-VPN IP Range mappings: 1.
IP Range over VPN mappings: 1.
Single IP over VPN mappings: 3.
MPLS/VPN based subscribers are enabled.
MPLS/VPN mappings: 4 used out of 16384 max.
MPLS based VPNs with subscriber mappings: 3 used out of 2015 max
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: 3
Peak number occurred at: 17:55:20 UTC THU June 15 2007
Peak number cleared at: 13:28:49 UTC THU June 15 2007
Event counters:
===============
Subscriber introduced: 2.
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>
```

EXAMPLE 2

The following example shows partial output for a system with VLAN-based subscribers enabled:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber db counters
Current values:
===============
Subscribers: 3 used out of 9999 max.
Introduced/Pulled subscribers: 3.
Anonymous subscribers: 0.
Subscribers with mappings: 3 used out of 9999 max.
Single non-VPN IP mappings: 1.
non-VPN IP Range mappings: 1.
IP Range over VPN mappings: 1.
Single IP over VPN mappings: 3.
VLAN based VPNs with subscribers: 2 used out of 2047
Subscribers with open sessions: 0.
Subscribers with TIR mappings: 0.
Sessions mapped to the default subscriber: 0.
```

Related Commands

Command	Description
clear interface linecard subscriber db counters	

show interface linecard subscriber mapping

Displays subscribers whose mapping meets the specified criteria.

show interface linecard *slot-number* subscriber mapping [IP *ipaddress/range*] [[amount] included-in IP *iprange* [VPN *vpn-name* | any-vpn]] [MPLS-VPN PE-ID *PE-id* BGP-label *BGP-label*] [VLAN-id *vlan-id*] [none]

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
ip-range	Specified range of IP addresses.
vpn-name	Name of VPN in which to search for the IP address. Displays a subscriber with a private IP mapping.
any-vpn	You can use this keyword instead of specifying a VPN name to match all the mappings within the specified IP ranges, regardless of their VPN, including non-VPN mappings
vlan-id	Specified VLAN tag.
PE-id	Loopback IP address of the relevant PE router (must also specify the **BGP-label**)
BGP-label	BGP label of the MPLS/VPN to search for (must also specify the **MPLS-VPN PE-ID**)

Defaults

BGP label of the MPLS/VPN to search for (must also specify the MPLS-VPN PE-ID)

Command Modes

User Exec

Usage Guidelines

Use this command to display subscribers whose mapping meets one of the following specified criteria:

- Matches a specified IP address or range of IP addresses (exact match of the specified range)
- Intersects a specified IP range (not necessarily an exact match of the specified range, but with IP addresses that are within the specified range).

  Use the **amount** keyword to display the number of subscribers meeting the criteria rather than listing actual subscriber names.
- Matches a specified VLAN tag (This option is provided for backwards compatibility and has certain restrictions. See **Note** below)
- Matches a specified MPLS/VPN mapping (This option is provided for backwards compatibility and has certain restrictions. See **Note** below)
- Has no mapping

When specifying an MPLS/VPN mapping, you must specify both the **MPLS-VPN PE-ID** and the **BGP-label.**

The **any-vpn** keyword is a wildcard that matches all the mappings within the IP ranges, regardless of their VPN, including non-VPN mappings.

Note the specific results of the following options:

- VLAN—if the VLAN tag is configured as a single subscriber (mapped to 0.0.0.0/0 on the VPN that is mapped to the specified VLAN tag) this option displays that subscriber.
- MPLS-VPN PE-ID BGP-label—if the MPLS mapping is configured as a single subscriber (mapped to 0.0.0.0/0 on the VPN that is mapped to the specified MPLS) this option displays that subscriber.
- included-in IP (no VPN specified)—matches non-VPN mappings only
- included-in IP VPN—matches private-IP mappings
- IP and VPN- the mapping must match the exact VPN as well as the IP range

Note The VLAN and MPLS-VPN PE-ID BGP-label options are provided for backward compatibility. These options require that the entire VLAN or MPLS/VPN be defined as a single subscriber with an IP address of 0.0.0.0/0@vpn, which corresponds to the MPLS/VPN and VLAN subscriber definition of pre-3.1.5 versions.

Authorization: viewer

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example lists the number of subscribers with no mapping.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber mapping amount none
Subscribers with no mappings:
N/A
Total 1 subscribers listed.
SCE>
```

EXAMPLE 2

The following example lists the subscribers that have IP mappings in the specified range in the specified VPN.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber mapping included-in IP 0.0.0.0/0 VPN Vpn1
Subscribers with IP mappings included in IP range '0.0.0.0/0@Vpn1':
Subscriber 'debugSub10', mapping '10.1.4.146/32@Vpn1'.
Subscriber 'debugSub10', mapping '18.0.0.0/16@Vpn1'.
Subscriber 'debugSub10', mapping '10.1.4.145/32@Vpn1'.
Total 1 subscribers found, with 3 matching mappings.
SCE>
```

EXAMPLE 3

The following example displays the number of VPN subscribers within the specified IP range.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber mapping amount included-in IP 0.0.0.0/0 VPN Vpn1
There are 1 subscribers with 3 IP mappings included in IP range '0.0.0.0/0@Vpn1'
SCE>
```

Related Commands

Command	Description

show interface linecard subscriber name

Displays information about a specified subscriber.

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

User Exec

Usage Guidelines

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.

Authorization: viewer

Examples

The following is an example of how to list the mappings for the specified subscriber.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber name gold123 mappings
Subscriber 'gold123' mappings:
IP 10.0.0.0 - Expiration (sec): Unlimited
SCE>
```

Related Commands

Command	Description
subscriber name property	

show interface linecard subscriber properties

Displays all existing subscriber properties.

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following is an example of how to display the subscriber properties.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber properties
Subscriber properties:
"monitor" : int16, minValue=0, maxValue=1.
"new_classification_policy" : Uint16.
"packageId : Uint16, minValue=0, maxValue=4999.
"QpLimit" : int32[18].
"QpSet" : Uint8[18].
Subscriber read-only properties:
"concurrentAttacksNumber" : Uint8.
"PU_QP_QuotaSetCounter" : Uint8[18].
"PU_QP_QuotaUsageCounter" : int32[18].
"PU_REP_nonReportedSessionsInTUR" : int32.
"P_aggPeriodType" :Uint8.
"P_blockReportCounter : int32
"P_endOfAggPeriodTimestamp : Uint32.
"P_firstTimeParty" : bool.
"P_localEndOfAggPeriodTimestamp : Uint32.
"P_mibSubCounters16" : Uint16[36][2].
"P_mibSubCounters32" : Uint32[36][2].
"P_newParty" : bool.
"P_numOfRedirections : Uint8.
"P_partyCurrentPackage : Uint16
"P_partyGoOnlineTime : Uint32
"P_partyMonth : Uint16
SCE>
```

Related Commands

Command	Description

show interface linecard subscriber sm-connection-failure

Displays the current state of the SM-SCE platform connection, as well as the configured action to take in case of failure of that connection.

show interface linecard *slot-number* subscriber sm-connection-failure [timeout]

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use the **timeout** keyword to display the configured SM-SCE platform link failure timeout value.

Authorization: viewer

Examples

The following examples illustrate the use of this command.

EXAMPLE 1

The following is an example of how to display the state of the SM-SCE platform connection.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber subscriber sm-connection-failure
Current SM link state: down.
Please note that this refers to the logical connection,
which means the synchronization with the SM i.e.
There might be cases where the connection at the SM will be up
and down at the SE since synchronization hasn't been completed yet.
Configured action to take when SM link is down: No action
SCE>
```

EXAMPLE 2

The following is an example of how to display the configured timeout value for the SM-SCE platform connection.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber subscriber sm-connection-failure timeout
SM SCE link failure timeout is: 90
SCE>
```

Related Commands

Command	Description
subscriber sm-connection-failure	

show interface linecard subscriber templates

Displays a specified subscriber template.

show interface linecard ***slot-number*** **subscriber templates [all|index** ***template-number*** **]**

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
template-number	The index number of the template to be displayed.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use the **all** keyword to display all existing subscriber templates.

Authorization: viewer

Examples

The following is an example of how to display a specified subscriber template.

```
SCE>enable 5
SCE>show interface linecard 0 subscriber templates index 3
Subscriber template 3 properties
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
QpSet[0..17]=0*17,1
SCE>
Password:<cisco>
```

Related Commands

Command	Description

show interface linecard subscriber tp-mappings statistics

Displays the traffic processor mappings statistics.

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following is an example of how to display the traffic processor mapping statistics.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber tp-mappings statistics
SCE>
```

Related Commands

Command	Description
subscriber tp-mappings	

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

User Exec

Usage Guidelines

Use the **all** keyword to display all existing TIR configurations.

Authorization: viewer

Examples

Following is an example of how to display all existing TIR configurations.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber tp-ip-range all
SCE>
```

Related Commands

Command	Description
subscriber tp-ip-range	

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

User Exec

Usage Guidelines

Use the **amount** keyword to display the number of existing mappings only, rather than the mappings themselves.

Authorization: viewer

Examples

The following examples illustrate how to use this command:

EXAMPLE 1:

Following is an example of how to display all existing mappings for TIR CMTS1.

```
SCE>enable 5
Password:<cisco>
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>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber amount mapping included-in tp-ip-range CMTS1
SCE>
```

Related Commands

Command	Description
subscriber tp-ip-range	

show interface linecard subscriber max-subscribers

Displays the maximum number of subscribers. Also indicates whether the capacity options have been disabled.

show interface linecard *slot-number* subscriber max-subscribers

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following is an example of how to display the maximum number of subscribers when the capacity options have not been disabled. (In which case the capacity options determine the maximum number of subscribers.)

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 subscriber max-subscribers
Configured actual maximum number of subscribers: 80000.
Note, however, that Subscriber Capacity Options are enabled, and they determine the actual
maximum number of subscribers.
SCE>
```

Related Commands

Command	Description
subscriber **max-subscribers**	
subscriber capacity-options	

show interface linecard tcp

Displays the current TCP handling state; whether bypassing TCP flow establishment is enabled or disabled.

show interface linecard *slot-number* tcp

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: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 tcp
Bypassing the TCP flow establishment is disabled
Note: The actual current state also depends on the attack filter and attack detector
states.
SCE#>
```

Related Commands

Command	Description
tcp bypass-establishment	

show interface linecard tos-marking

Displays the current TOS marking state.

show interface linecard *slot-number* tos-marking

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use this command to display the current TOS marking state, including:

- translation table
- marking mode per interface (enable/disable)

Authorization: viewer

Examples

The following example shows a sample of the output from this command.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 tos-marking
ToS Translation Table
=====================
| tos-id | tos-value (DSCP) |
|--------|------------------|
| 1 | 00 (0x00) |
| 2 | 00 (0x00) |
| 3 | 00 (0x00) |
| 4 | 00 (0x00) |
| 5 | 00 (0x00) |
| 6 | 00 (0x00) |
| 7 | 00 (0x00) |
ToS Marking state by egress interface
=====================================
| Interface | State |
|------------|----------|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
SCE>
```

Related Commands

Command	Description
tos-marking enabled	

tos-marking clear-table	
tos-marking set-table-entry	

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

User Exec

Usage Guidelines

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

Authorization: viewer

Examples

The following example displays information for all existing traffic counters.

```
SCE>enable 5
Password:<cisco>
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.
SCE>
```

Related Commands

Command	Description
traffic-counter	
clear interface linecard traffic-counter	

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.s

Command Modes

User Exec

Usage Guidelines

Use the **all** keyword to display all traffic counter rules.

Use the **tunnel-id-mode** keyword to display all rules defined in *tunnel-id-mode.*

Authorization: viewer

Examples

The following example displays traffic rule information.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 traffic-rule name Rule1
0 rules listed out of 127 available.
SCE>
```

Related Commands

Command	Description
traffic-rule	

show interface linecard vas-traffic-forwarding

Displays tnformation regarding VAS configuration and operational status summary.

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

User Exec

Usage Guidelines

Use this command to display the following for VAS traffic-forwarding information:

- 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

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.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 vas-traffic-forwarding
VAS traffic forwarding is enabled
VAS traffic link configured: Link-1 actual: Link-1
SCE>
```

EXAMPLE 2

This example shows how to display operational and configuration information for a specific VAS Server Group.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 vas-traffic-forwarding VAS server-group 0
VAS server group 0:
State: Failure configured servers: 0 active servers: 0
minimum active servers required for Active state: 1 failure action: Pass
SCE>
```

EXAMPLE 3

This example shows how to display operational and configuration information for a specific VAS server.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 vas-traffic-forwarding VAS server-id 0
VAS 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
SCE>
```

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.**)

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 vas-traffic-forwarding VAS server-id 0 counters health-check
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 :
SCE>
```

Related Commands

Command	Description
vas-traffic-forwarding	
vas-traffic-forwarding vas server-id health-check	
vas-traffic-forwarding vas server-group	
vas-traffic-forwarding vas server-group failure	
vas-traffic-forwarding vas server-id	
vas-traffic-forwarding server-id vlan	
vas-traffic-forwarding vas traffic-link	
show interface linecard subscriber name	
show interface linecard counters	
clear interface linecard vas-traffic-forwarding vas counters health-check	

show interface linecard virtual-links

Displays the currently configured virtual links

You can also use this command to see which virtual links have GCs whose values have been changed from the original SCA BB configuration.

show interface linecard *slot-number virtual*-links all

show interface linecard *slot-number virtual*-links changed

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec.

Usage Guidelines

Use the **all** keyword to see all the currently configured virtual links, with their ID number and direction.

Use the **changed** keyword to see which virtual links have GCs for which the PIR is now different from the values configured for the template GCs via the console.

Examples

The following examples illustrate the use of this command.

Example 1

This example shows how to display all existing virtual links.

```
SCE>enable 5
password<cisco>
SCE>show interface LineCard 0 virtual-links all
Virtual Link enabled
Virtual link index 1 direction upstream
Virtual link index 2 direction upstream
Virtual link index 3 direction upstream
Virtual link index 4 direction upstream
Virtual link index 12 direction upstream
Virtual link index 13 direction upstream
Virtual link index 14 direction upstream
Virtual link index 15 direction upstream
```

Example 2

This example displays the virtual links that have GCs with values that are different from the original configuration.

```
SCE>enable 5
password<cisco>
SCE>show interface LineCard 0 virtual-links changed
Virtual Link enabled
Virtual link index 3 direction upstream
```

```
Global Controller index 0 timebased values = 300,300,300,300
Global Controller index 1 timebased values = 500,500,500,500
Virtual link index 12 direction upstream
Global Controller index 0 timebased values = 700,700,700,700
Virtual link index 14 direction upstream
Global Controller index 0 timebased values = 5500,5500,5500,5500
Global Controller index 1 timebased values = 1500,1500,1500,1500
```

Related Commands

Command	Description
virtual-links index direction [upstream | downstream]	

show interface linecard vlan

Displays the VLAN tunnel configuration.

show interface linecard *slot-number* vlan

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the VLAN configuration.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 vlan
VLAN symmetric skip
SCE>
```

Related Commands

Command	Description
vlan	

show interface linecard vlan translation

Displays the 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

User Exec

Usage Guidelines

Authorization: Viewer

Examples

The following example shows the vlan translation configuration.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 vlan translation
vlan translation constant: increment 20
SCE>
```

Related Commands

Command	Description
vlan translation	

show interface linecard vpn

Displays information regarding currently logged-in VPNs.

show interface linecard *slot-number* VPN {name *vpn-name* | all-names [automatic]}

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
vpn-name	The name of the VPN in which to search for the IP mapping.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use the **name** option to specify a specific currently logged-in VPN for which to display the details.

Use the **all-names** keyword to display he names of all VPNs that are currently logged into the system.

Use the **automatic** keyword with the **all-names** option to display the names of all VPNs that were created automatically by the SCE platform.

Authorization: viewer

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example displays names of all currently logged in VPNs.

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 VPN all-names
There are 2 VPNs in the data-base:
VPN1
VPN2
SCE>
```

EXAMPLE 2

The following example illustrates the output of this command for an MPLS-based VPN:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 VPN name Vpn1
VPN name: Vpn1
Downstream MPLS Mappings:
PE-ID = 1.0.0.1 Mpls Label = 20
PE-ID = 1.0.0.1 Mpls Label = 30
=======>Total Downstream Mappings: 2
Upstream MPLS Mappings:
=======>Total Upstream Mappings: 0
Number of subscriber mappings: 0
SCE>
```

EXAMPLE 3

The following example illustrates the output of this command for an empty VPN:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 VPN name Vpn2
VPN name: Vpn2
VPN has no mappings
Number of subscriber mappings: 0
SCE>
```

EXAMPLE 4

The following example illustrates the output of this command for a VLAN-based VPN:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 VPN name Vpn3
VPN name: Vpn3
VLAN: 2
Number of subscriber mappings: 0
SCE>
```

EXAMPLE 5

The following example illustrates the output of this command for an automatically created VLAN VPN:

```
SCE>enable 5
Password:<cisco>

SCE>show interface linecard 0 VPN name Vpn2 VPN name: Vpn2
VLAN: 2
Number of subscriber mappings: 1
Automatically created VPN
SCE>
```

Related Commands

Command	Description

show interface linecard wap

Displays the current WAP handling state.

show interface linecard *slot-number* wap

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates how to use this command:

```
SCE>enable 5
Password:<cisco>
SCE>show interface linecard 0 wap
WAP handling is disabled
SCE>
```

Related Commands

Command	Description
wap	

show interface linecard watchdog

Displays the current Line Card watchdog mode.

show interface linecard *slot-number* watchdog

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: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface linecard 0 watchdog
Line Card watchdog mode: enabled
SCE#>
```

Related Commands

Command	Description
show watchdog	

show interface mng

Displays information regarding the specified management interface.

show interface mng {0/1 | 0/2} [auto-fail-over|duplex|ip address|speed]

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use this command to display the following information for the specified management interface:

- speed
- duplex
- IP address
- auto-fail-over (SCE 2000 platform only)

If no keyword is specified, all information is displayed.

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: viewer

Examples

This example shows how to display all information for Management port 1.

```
SCE>enable 5
Password:<cisco>
SCE>show interface mng 0/1
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>
```

Related Commands

Command	Description
interface mng	

show interface ruc

Displays the counters for the specified RUC (traffic processor).

show interface ruc ***slot-number/ruc-number***

Syntax Description

slot-number	The number of the identified slot. Enter a value of 0.
ruc-number	The number of the RUC (1-3).

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show interface ruc 0/1
Ruc 0/0 statistics are:
Total number of packets handled: 0
Total number of packets entered the graph: 0
Total number of threads traversed: 0
Total number of nodes traversed: 0
Total number of flows traversed: 0
Total number of flows that were split: 0
Total number of flows that experienced spraying: 0
First in flows of new flows: 0
First in flows of existing flows: 0
First in flows of aggregate flows: 0
First in flows of TCP flows: 0
First in flows of UDP flows: 0
First in flows of Non TCP/UDP flows: 0
First in flows starting from upstream: 0
First in flows starting from downstream: 0
First in Flow with Error for an existing flow: 0
First in Flow with Error for a non-existing flow: 0
Packets with errors: 0
TestPackets with errors: 0
EOCs for flows: 0
Out of Sequences for packets that should enter the graph: 0
Packets with payload of a non-established flow connection: 0
Attempting to traverse when there is no root node: 0
Stopped traversing threads due to many threads: 0
Stopped traversing due to no node in thread: 0
Stopped traversing node of a thread due to many nodes: 0
Exited packet/aging related traversing of nodes due to Traverser watchdog timeout: 0
Pulled out of packet/aging related traversing due to traverser watchdog timeout: 0
Exited party/global related traversing of nodes due to Traverser watchdog timeout: 0
Pulled out of party/global related traversing due to Traverser watchdog timeout: 0
```

```
Any other traversing error states not listed above: 0
Traverser exceptions which caused killing of the current FC: 0
Total number of test-packets received: 0
Total number of ip msg packets : 0
non IP packets : 0
IP checksum error packets : 0
IP length error packets : 0
IP broadcast packets : 0
IP TTL error packets : 0
TCP UDP checksum error packets : 0
Number of failures to allocate flow memory : 0
Number of flows bypassed due to CPU congestion : 0
SCE#>
```

Related Commands

Command	Description

show inventory

Displays UDI information for the SCE platform.

show inventory

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use this command to display the following UDI information for the SCE platform:

- Device name
- Description
- Product identifier
- Version identifier
- Serial number

Authorization: viewer

Examples

The following example displays the UDI information for the SCE platform.

```
SCE>enable 5
Password:<cisco>
SCE>show inventory
NAME: "Chassis", DESCR: "Cisco SCE 2020 Service Control Engine, Multi Mode, 4-port GE"
PID: SCE2020-4XGBE-MM , VID: V01, SN: CAT093604K3
SCE>
```

Related Commands

Command	Description

show ip (ROOT level options)

Displays information about IP-related options available only at the root authorization level.

show ip ftp-server [passive-port-range | port]

show ip http-tech-if

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

The following options are available for display:

- **ftp-server passive-port-range** — range of port numbers used for passive FTP
- **ftp-server port** — FTP server port number
- **http-tech-if** — HTTP adaptor attributes

Authorization: root

Examples

The following examples illustrate the use of this command.

EXAMPLE 1

```
SCE>enable 15
Password:<cisco>
SCE#>show ip ftp-server passive-port-range
Passive FTP port range is 21001-21100
SCE#>
```

EXAMPLE 2

```
SCE>enable 15
Password:<cisco>
SCE#>show ip http-tech-if
HTTP server is enabled
HTTP server port is 8082
SCE#>
```

Related Commands

Command	Description
ip ftp-server	
ip http-tech-if	

show ip access-class

Shows the access list defined for global IP access to the SCE platform. 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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the IP access class mapping.

```
SCE>enable 5
Password:<cisco>
SCE>show ip access-class
IP layer is using access-list # 1.
SCE>
```

Related Commands

Command	Description
ip access-class	

show ip advertising

Shows the status of IP advertising, the configured destination and the configured interval.

show ip advertising [destination|interval]

Syntax Description

destination	Displays IP advertising destination.
interval	Displays the interval between ping commands

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use the form **show ip advertising destination** to display the IP advertising destination.

Use the form **show ip advertising interval** to display the interval between ping commands.

Authorization: viewer

Examples

The following example shows the IP advertising status and configuration.

```
SCE>enable 5
Password:<cisco>
SCE>show ip advertising
IP advertising is disabled
IP advertising destination is 10.10.10.10
IP advertising interval is 853 seconds
SCE>
```

Related Commands

Command	Description
ip advertising	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example displays the default gateway.

```
SCE>enable 5
Password:<cisco>
SCE>show ip default-gateway
Default gateway: 10.1.1.1
SCE>
```

Related Commands

Command	Description
ip default-gateway	

show ip filter

Displays information regarding the management interface IP filtering.

show ip filter

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use this command to display 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)

Authorization: viewer

Examples

The following command shows how to display information for management interface IP filtering

```
SCE>enable 5
Password:<cisco>
SCE>show ip filter
is fragment filtered : 0
Input Bandwidth  : 0 Kb/sec
Input packets rate : 2 Pkt/sec
Input bandwidth policer : CIR: 20000.00 Kb/sec BTime: 200 msec LP: 100 %
Input packet rate policer : CIR: 5000.00 Pkt/sec BTime: 200 msec LP: 100 %
Permit monitor  :state : no_attack BW: 0
High : CIR: 20000.00 Kb/sec BTime: 10000 msec LP: 100 %
Low : CIR: 20000.00 Kb/sec BTime: 10000 msec LP: 100 %
Denied monitor  :state : no_attack BW: 0
High : CIR: 20000.00 Kb/sec BTime: 10000 msec LP: 100 %
Low : CIR: 20000.00 Kb/sec BTime: 10000 msec LP: 100 %
in_bytes  : 85115466
in_pkt  : 371598
in_pkt_accept : 371598
in_pkt_denied : 0
drop_fragment_cnt : 0
action_delay_due_bw : 0
action_delay_due_pkt : 0
PERMIT events
meStartAttack : 0
meStopAttack : 0
DENIED events
meStartAttack : 0
SCE>
```

Related Commands

Command	Description
ip filter fragment	
ip filter moniter	

show ip radius-client

Displays the RADIUS client general configuration.

show ip radius-client

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 illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#show ip radius-client
SCE>
```

Related Commands

Command	Description
ip radius-client retry limit	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following examples illustrate the use of this command.

EXAMPLE 1:

The following example shows the default gateway.

```
SCE>enable 5
Password:<cisco>

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>enable 5
Password:<cisco>
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

Command	Description
ip route	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the configuration of the RPC adapter.

```
SCE>enable 5
Password:<cisco>
SCE>show ip rpc-adapter
RPC Server is OFFLINE
RPC Server port is 14374
SCE>
```

Related Commands

Command	Description
ip rpc-adapter	
ip rpc-adapter port	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows how to retrieve the current SSH status.

```
SCE>enable 5
Password:<cisco>
SCE>show ip ssh
SSH server is enabled.
SSHv1 support is enabled
SSH server does not use any access-list.
There are no active SSH sessions.
SCE>
```

Related Commands

Command	Description
ip ssh	

show jvm

Displays information regarding the built in Java machine (jvm) configuration options.

show jvm input-string [cold-start|warm-start|all]

show jvm class-path

Syntax Description

Specify the input string to display:

- cold-start
- warm-start
- all

Defaults

By default, the warm-start jvm input string is displayed.

Command Modes

Privileged exec

Usage Guidelines

The following options are available for display:

- jvm input string — specify either cold start input string, warm start input string or all. If no keyword is included, the warm-start jvm input string is displayed.
- jvm class-path — displays the path for searching for java classes

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show jvm input-string
JVM warm-start input string = -Dcom.pcube.WarmStart StartSE
SCE#>
```

Related Commands

Command	Description
jvm input-string	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the access list configured for telnet lines.

```
SCE>enable 5
Password:<cisco>
SCE>show line vty access-class in
Telnet server is using access-list # 1.
SCE>
```

Related Commands

Command	Description
line vty	

show log

Displays the contents of the user log file.

show log

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of this command.

```
SCE>enable 5
Password:<cisco>
SCE>show log
2006-01-25 00:14:46 | INFO | CPU #000 | User message files were successfully cleared, new
files were opened
2006-01-25 00:23:07 | INFO | CPU #000 | A new password was set for level 10
2006-01-25 00:49:41 | INFO | CPU #000 | System hostname changed to :ecco"
2006-01-25 01:02:41 | INFO | CPU #000 | Time zone set to GMT
2006-01-25 01:06:33 | INFO | CPU #000 | A new password was set for level 15
2006-01-25 01:08:07 | INFO | CPU #000 | A new password was set for level 5
2006-01-25 01:23:07 | INFO | CPU #000 | IP address of slot 0, port 0 set to 10.10.10
2006-01-25 01:56:44 | INFO | CPU #000 | Configuration file '/tffs0/system/config.txt' was
saved - file size 1200
2006-01-25 05:34:45 | INFO | CPU #000 | A telnet session from 20.20.20.20 was established
SCE>
```

Related Commands

Command	Description
clear logger	
logger get user-log file-name	
more user-log	

show logger

Displays information regarding the logger.

show logger status

show logger counters

show logger nv-counters

show logger flow-tracking

show logger application-stats

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Displays specified information regarding the logger:

- Status
- Counters
- Flow tracking status
- Global logger non-volatile counters
- Application statistics

Use the appropriate keyword to display the desired logger information.

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show logger counters
Logger counters:
Total messages read: 188686
Total messages masked: 0
Total messages failed: 0
Total messages written: 188686
Total info messages: 188684
Total warning messages: 2
Total error messages: 0
Total fatal messages: 0
Last time these counters were cleared: 12:03:22 GMT WED June 7 2006
SCE#>
```

Related Commands

Command	Description
clear logger counters	
show logger device	

show logger device

Displays the configuration of the specified SCE platform logger file. Also displays the current user log counters.

show logger device {line-attack-file-log | user-file-log[counters|max-file-size|status|nv-counters]}

Syntax Description

See "Usage Guidelines".

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Specify the desired logger device:

- **Line-Attack-File-Log** : displays the following information:
  - Status
  - Maximum file size
- **User-File-Log:** displays the following information:
  - Status
  - Maximum file size

If you specify **User-File-Log,** you can specify one of the following options:

- counters: Displays the User-File-Log counters
- max-file-size: Displays the currently configures maximum file size for the User-File-Log
- nv-counters: Displays the User-File-Log non-volatile counters
- status: Displays the current status of the User-File-Log

Authorization: viewer

Examples

The following examples illustrate the use of this command.

EXAMPLE 1

The following example shows the SCE platform Line-Attack-File-Log status and configuration.

```
SCE>enable 5
Password:<cisco>
SCE>show logger device Line-Attack-File-Log
Line-Attack-File-Log status: Enabled
Line-Attack-File-Log file size: 1000000
SCE>
```

EXAMPLE 2

The following example shows the SCE platform User-File-Log counters.

```
SCE>enable 5
Password:<cisco>
SCE>show logger device line-attack-file-log counters
device User-File-Log counters
Total info messages: 62
Total warning messages: 4
Total error messages: 0
Total fatal messages: 0
Last time these counters were cleared: 02:23:27 GMT TUES January 17 2006
SCE>
```

Related Commands

Command	Description
logger device	
clear logger	

show logger device (ROOT level options)

Displays information for the specified logger device.

show logger device {debug-file-log | statistics-file-log | statistics-archive-file-log}

show logger device {debug-file-log | statistics-file-log | statistics-archive-file-log} status

show logger device debug-file-log module

show logger device debug-file-log min-severity

show logger device {debug-file-log | statistics-file-log | statistics-archive-file-log} max-file-size

show logger device {debug-file-log | statistics-file-log | statistics-archive-file-log} counters

show logger device statistics-archive-file-log log message-timeout

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

The available logger devices are:

- Debug-File-Log
- Statistics-File-Log
- Statistics-Archive-File-Log
- Line-Attack-File-Log (Available at Viewer authorization level. See **show logger device**)
- User-File-Log (Available at Viewer authorization level. See **show logger device**)

The following types of information can be displayed for the logger devices:

- status
- module: logged module
- min-severity: severity level
- max-file-size: maximum file size
- counters
- log message-timeout: minimum time between logging of the same message

If no option is specified, all relevant information, with the exception of the counters, will be displayed.

The information available for the various logger devices varies somewhat. Refer to the following table for a summary of what information can be displayed for each logger device.

Table 2-5 Logger Device Information

Logger Device	Information
Debug-File-Log	status, module, min-severity, max-file-size, counters
Statistics-File-Log	status, max-file-size, counters
Statistics-Archive-File-Log	status, max-file-size, counters, log message-timeout

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show logger device debug-file-log
Device Debug-File-Log status: Enabled
Device Debug-File-Log file size: 1000000
Device Debug-File-Log logged module: 0xffff
Device Debug-File-Log severity: Info
SCE#>
```

Related Commands

Command	Description
clear logger device	
clear logger device counters	
show logger	
logger (ROOT level options)	

show logger flow-tracking

Shows the information gathering state per the last logger track flows command, even if flow tracking has already terminated. Also shows the configuration of the last flow-tracking command.

show logger flow-tracking

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show logger flow-tracking
SCE#>
```

Related Commands

Command	Description
logger track flows	

show management-agent

Displays information regarding the management agent.

show management-agent

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use this command to display the following information for the management agent:

- status (enabled or disabled)
- access control list number assigned

Authorization: viewer

Examples

The following example shows how to display the information for the management-agent.

```
SCE>enable 5
Password:<cisco>
SCE>show management-agent
management agent is enabled.
management agent is active, version: SCE Agent 3.0.3 Build 15
management agent does not use any access-list.
SCE>
```

Related Commands

Command	Description
management-agent access-class	
service management-agent	

show management-agent sce-api quota

Displays information relating to the quota message buffer.

show management-agent sce-api quota

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use this command to display the following information:

- Quota rate control
- Maximum size of the quota message buffer
- Number of messages currently in the quota message buffer, waiting to be sent to the QM

Authorization: viewer

Examples

The following example shows how to display the information for the management-agent.

```
SCE>enable 5
Password:<cisco>
SCE>show management-agent sce-api quota
Quota rate control : 125
Quota max buffer size : 1000
Quota msg in buffer : 0
SCE>
```

Related Commands

Command	Description
management-agent sce-api quota-buffer-size	

show party

Displays information regarding the party database. Use this command to obtain information about the parameters of the currently loaded application, such as a listing of all tunable names or all viewable names.

show party aging

show party all

show party all-names

show party all-parties-with-open-flows

show party db-statistics

show party default-name

show party meters

show party num-of-pid-to-remove

show party num-parties

show party num-parties-with-open-flows

show party pull-retries-till-trap

show party state

show party tunables

show party unmapped-group {all | group-name ***group-name*** **| ip-range** ***ip-range*** **}**

show party variables

show party viewables

Syntax Description

group-name	The name of the group.
ip-range	Range of IP addresses.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

The following options are available for display:

- **aging** — party aging configuration
- **all** — the entire contents of the Party database (for tunables, displays only those that have changed)

- **all-names** — list of party names in the Party database
- **all-parties-with-open-flows** — list of all active parties
- **db-statistics** — information about the status of the party database, such as capacity and number of entries
- **default-name** — name of the default party
- **meters** — list of meter names defined by the current loaded application
- **num-of-pid-to-remove** — number of PIDs in the system waiting to be removed
- **num-parties** — number of parties in the system
- **num-parties-with-open-flows** — number of active parties
- **pull-retries-till-trap** — number of pull requests permitted before a trap is issued
- **state** — list of variable names that define the party state
- **tunables** — list of tunable names defined by the current loaded application
- **unmapped-group** — party unmapped groups according to the optional parameters, as follows:
  - group-name — displays the specified unmapped group
  - ip-range — displays all unmapped groups found within the specified range of IP addresses
  - all — displays all unmapped groups
- **variables** — list of variable names defined by the current loaded application
- **viewables** — list of viewable names defined by the current loaded application

Authorization: root

Examples

The following example shows how to use this command.

EXAMPLE 1

The following example shows how to display all party information.

```
SCE>enable 15
Password:<cisco>
SCE#>show party all
There are 2 parties in the data-base:
Party "DefaultParty" is static
Party "DefaultParty" has 0 mappings:
Party "DefaultParty" IP-range-mappings:
No records found.
Party "DefaultParty" VLAN-mappings:
No records found.
Party "DefaultParty" has 5 tunables:
Party "DefaultParty" has no meters
Party "partyall" is static
Party "partyall" has 1 mappings:
Party "partyall" IP-range-mappings:
10.0.0.0:0xffffffff - Expiration (sec): Unlimited
Party "partyall" VLAN-mappings:
No records found.
Party "partyall" has 5 tunables:
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
```

```
QpSet[0..17]=0*17,1
Party "partyall" has no meters
SCE#>
```

EXAMPLE 2

The following example shows how to display the party database statistics.

```
SCE>enable 15
Password:<cisco>
SCE#>sshow party db-statistics
Parties: 2 used out of 10000 max.
Parties with mappings: 10000 max.
Parties waiting to be removed: 0.
Unmapped range groups: 0 used out of 1000 max.
Mapping Entries: 1 used out of 31957 max.
IP-address Entries: 1 used out of 20000 max.
Available IP-Addresses: 19999 (under hardware rules constrains).
IP-range Entries: 0 used out of 7972 max.
Available IP-Ranges: 7972 (under hardware rules constrains).
VLAN Entries: 0 used out of 3985 max.
Available VLAN-Ids: 3985 (under hardware rules constrains).
Party contexts: 2 used out of 11000 max context in the control database.
Parties waiting to be removed : 0.
Parties waiting to be removed due to logout retry: 0.
Mapped parties: 1
Peak number of mapped parties: 1
Peak number occurred at: 13:54:58 GMT THU June 15 2006
Peak number cleared at: 13:54:47 GMT THU June 15 2006
Parties using CPU #1: 2 out of 10001 max.
SCE#>
```

Related Commands

Command	Description
party aging	
party default-name	

show party mapping

Displays the party that is mapped to a specified IP address of VLAN tag. Can also be used to display the total number of mappings of the specified type in the database.

show party mapping IP-address ***ip-address***

show party mapping IP-address number

show party mapping IP-range ***ip-address:mask***

show party mapping IP-range number

show party mapping vlan-id ***vlan-id***

show party mapping vlan-id number

Syntax Description

ip-address	Specific IP address.
ip-address:mask	Range of IP addresses specified in the format x.x.x.x:y.
vlan-id	Specific VLAN tag number.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

The following options are available for display:

- **IP-address** — the party mapped to the specified IP address
- **IP-range** — the party mapped to the specified range of IP addresses
- **vlan-id** — the party mapped to the specified VLAN ID

Use the **number** keyword with any of the above options to display the total number of mappings of that type in the database (omit the specific iP address or VLAN ID).

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example shows how to display the party that is mapped to a specific IP address range.

```
SCE>enable 15
Password:<cisco>
SCE#>show party mapping IP-range 10.0.0.0:0xffffffff
IP range 10.0.0.0:0xffffffff is mapped to party "partyall".
SCE#>
```

EXAMPLE 2

The following example shows how to display the total number of VLAN mappings in the database.

```
SCE>enable 15
Password:<cisco>
SCE#>show party mapping vlan-id number
There are 0 VLAN mappings in the data-base.
SCE#>
```

Related Commands

Command	Description
party mapping	

show party name

Displays information regarding the specified party.

show party name party-name

show party name party-name all-meters

show party name party-name all-tunables

show party name party-name all-variables

show party name party-name all-viewables

show party name party-name changed-tunables

show party name party-name cpu-mapping

show party name party-name meter party-meter-name

show party name party-name meter party-meter-name dropped-cir-bytes

show party name party-name open-flows

show party name party-name tunable party-tunable-name

show party name party-name variable party-variable-name

show party name party-name vas-servers

Syntax Description

party-name	The name of the party.
party-meter-name	The name of the specific party meter.
party-tunable-name	The name of the specific party tunable.
party-variable-name	The name of the specific party variable.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

The following options are available for display:

- **all-meters** — all meter CIR and PIR values
- **all-tunables** — all party tunables
- **all-variables** — all party variables
- **all-viewables** — all party viewables
- **changed-tunables** — all party tunables that have changed

- **cpu-mapping** — the location (slot and cpu number) where the content of the specified party is located
- **meter** — specified party meter CIR and PIR
- **meter dropped-cir-bytes** — the number of dropped CIR bytes of the specified party meter
- **open-flows** — Number of currently open flows on this party (bundles are counted as one flow)
- **tunable** — specified party tunable
- **variable** — specified party variable
- **vas-servers** — Vas server used by this subscriber

If no option is specified, all party variables, meters and IP mappings for the specified party are displayed.

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show party name partyall
Party "partyall" is static
Party "partyall" has 1 mappings:
Party "partyall" IP-range-mappings:
10.0.0.0:0xffffffff - Expiration (sec): Unlimited
Party "partyall" VLAN-mappings:
No records found.
Party "partyall" has 21 variables:
concurrentAttacksNumber=0
monitor=0
new_classification_policy=0
packageId=0
PV_QP_QuotaSetCounter[0..17]=0*18
PV_QP_QuotaUsageCounter[0..17]=0*18
PV_REP_nonReportedSessionsInTUR=0
P_aggPeriodType=5
P_blockReportCounter=0
P_endOfAggPeriodTimestamp=0
P_firstTimeParty=TRUE
P_localEndOfAggPeriodTimestamp=0
P_MibSubCounters16[0..31][0..1]=0*64
P_MibSubCounters32[0..31][0..1]=0*64
P_newParty=TRUE
p_numOfRedirections=0
P_partyCurrentPackage=0
P_partyGoOnlineTime=0
P_partyMonth=0
QpLimit[0..17]=0*17,8
QpSet[0..17]=0*17,1
Party "partyall" has no meters
SCE#>
```

Related Commands

Command	Description
party name tunables	
party name cpu-mapping	

show party name mappings

Displays the indicated mapping for the specified party.

show party name ***party-name*** **mappings ip-addresses**

show party name ***party-name*** **mappings ip-ranges**

show party name ***party-name*** **mappings vlans**

show party name ***party-name*** **mappings all**

Syntax Description

party-name	The name of the party.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

The following options are available for display:

- **ip-addresses** — all IP addresses mapped to the specified party
- **ip-ranges** — all IP address ranges mapped to the specified party
- **vlans** — all VLAN tags mapped to the specified party
- **all** — all mapped mapped to the specified party

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show party name partyall mappings all
Party "partyall" has 1 mappings:
Party "partyall" IP-range-mappings:
10.0.0.0:0xffffffff - Expiration (sec): Unlimited
Party "partyall" VLAN-mappings:
No records found.
SCE#>
```

Related Commands

Command	Description
party mapping	

show party template

Displays template configurations.

show party template index *index* [all-meters | all-tunables | changed-tunables | meter *meter-name* | tunable *tunable-name*]

show party template all-non-default

show party template all

show party template index *index* [all-meters | all-tunables | changed-tunables | meter *meter-name* | tunable *tunable-name*]

show party template all-non-default

show party template all

Syntax Description

index	Index number of the template.
meter-name	Name of the specific meter.
tunable-name	Name of the specific tunable.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

The following options are available for display:

- **all-meters** — current values assigned to all meters for the specified template
- **all-tunables** — current values assigned to all tunables for the specified template
- **changed-tunables** — all non-default tunable values for the specified template
- **meter** — name of the specified meter for the specified template
- **tunable** — name of the specified tunable for the specified template
- **all-non-default** — display the names of all templates that have a non-default configuration
- **show party template all** — display the configuration of all existing templates

Authorization: root

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example shows how to display the value of a specific tunable (monitor) for a specified template (#1).

```
SCE>enable 15
Password:<cisco>
SCE#>show party template index 1 tunable monitor
monitor 0
SCE#>
```

EXAMPLE 2

The following example shows how to display the configurations of all existing templates.

```
SCE>enable 15
Password:<cisco>
SCE#>show party template all
There are 200 templates in the data-base:
Template 0
Template 0 has 5 tunables:
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
QpSet[0..17]=0*17,1
Template 0 has no meters
Template 1
Template 1 has 5 tunables:
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
QpSet[0..17]=0*17,1
Template 1 has no meters
Template 2
Template 2 has 5 tunables:
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
QpSet[0..17]=0*17,1
Template 2 has no meters
Template 3
Template 3 has 5 tunables:
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
QpSet[0..17]=0*17,1
Template 3 has no meters
Template 4
Template 4 has 5 tunables:
monitor=0
new_classification_policy=0
packageId=0
QpLimit[0..17]=0*17,8
```

```
QpSet[0..17]=0*17,1
Template 4 has no meters
SCE#>
```

Related Commands

Command	Description
party template	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows how to display application file information.

```
SCE>enable 5
Password:<cisco>
SCE>show pqi file myfile.pqi info
application: sm
description: SCE 1000 sm
target SCE : SCE 1000
module names: sm20001.pm0
SCE>
```

Related Commands

Command	Description
pqi install file	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows how to find out what pqi file is installed.

```
SCE>enable 5
Password:<cisco>
SCE>show pqi last-installed
package name: SACS BB
package version 3.0.1. build 02
package date: Tue Jun 10 17:27:55 GMT+00:00 2006
operation: Upgrade
SCE>
```

Related Commands

Command	Description
pqi rollback file	
pqi uninstall file	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the configuration of the RDR formatter.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter
Status: enabled
Connection is: down
Forwarding mode: redundancy
Connection table:
-------------------------------------------------------
Collector | Port | Status | Priority per Category: |
IP Address / | |  |-------------------------|
Host-Name | |  | 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: queued: 0, sent:4460807, thrown: 0, format-mismatch:0
UM: queued: 0, sent: 0, thrown: 0
Logger: queued: 0, sent: 39, thrown: 0
Last time these counters were cleared: 20:23:05 IST WED March 14 2007
SCE>
```

Related Commands

Command	Description
rdr-formatter destination	
service rdr-formatter	

show rdr-formatter buffer-size

Displays the size of the buffer for each RDR formatter category.

show rdr-formatter buffer-size all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show rdr-formatter buffer-size all
Category #1: 3000000 bytes.
Category #2: 1800000 bytes.
Category #3: 600000 bytes.
Category #4: 600000 bytes.
Total 6000000 bytes used out of 6000128 available (100%).
SCE#>
```

Command	Description
rdr-formatter buffer-size	
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter destination	
show rdr-formatter enabled	
show rdr-formatter forwarding-mode	
show rdr-formatter rdr-mapping	
show rdr-formatter statistics	

show rdr-formatter connection-status

Displays information regarding the RDR formatter connections.

show rdr-formatter connection-status

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Displays the following information regarding the RDR formatter connections:

- main connection
- status: status and forwarding mode connection table with the following information for each destination:
  - port
  - status
  - priority

Authorization: viewer

Examples

The following example shows the RDR formatter connection status.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter connection-status
Connection is: up
Forwarding mode: redundancy
Connection table:
-------------------------------------------------------
Collector | Port | Status | Priority per Category: |
IP Address / | |  |-------------------------|
Host-Name | |  | 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

Command	Description
show rdr-formatter	
show rdr-formatter counters	

show rdr-formatter destination	
show rdr-formatter enabled	
show rdr-formatter forwarding-mode	
show rdr-formatter history-size	
show rdr-formatter protocol NetflowV9 dscp	
show rdr-formatter rdr-mapping	
show rdr-formatter statistics	

show rdr-formatter counters

Displays 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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the RDR-formatter counters.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter counters
RDR: queued: 0, sent:4460807, thrown: 0, format-mismatch:0
UM: queued: 0, sent: 0, thrown: 0
Logger: queued: 0, sent: 39, thrown: 0
Last time these counters were cleared: 20:23:05 IST WED March 14 2007
SCE>
```

Related Commands

Command	Description
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter destination	
show rdr-formatter enabled	
show rdr-formatter forwarding-mode	
show rdr-formatter history-size	
show rdr-formatter protocol NetflowV9 dscp	

show rdr-formatter rdr-mapping	
show rdr-formatter statistics	

show rdr-formatter destination

Displays the RDR formatter destinations, including protocol and transport type.

show rdr-formatter destination

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the configured RDRv1 formatter destinations.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter destination
Destination: 10.56.201.50
Port: 33000
Protocol: RDRv1
Destination: 10.56.204.7
Port: 33000
Protocol: NetflowV9
Destination: 10.56.204.10
Port: 33000
Protocol: RDRv1
SCE>
```

Related Commands

Command	Description
rdr-formatter destination	
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter enabled	
show rdr-formatter forwarding-mode	
show rdr-formatter history-size	

show rdr-formatter protocol NetflowV9 dscp	
show rdr-formatter rdr-mapping	
show rdr-formatter statistics	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows that the RDR formatter is enabled.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter enabled
Status: enabled
SCE>
```

Related Commands

Command	Description
service rdr-formatter	
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter destination	
show rdr-formatter forwarding-mode	
show rdr-formatter history-size	
show rdr-formatter rdr-mapping	
show rdr-formatter statistics	

show rdr-formatter forwarding-mode

Shows the configured RDR-formatter forwarding-mode (redundancy/multicast/simple load balancing).

show rdr-formatter forwarding-mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the RDR formatter forwarding-mode.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter forwarding-mode
Forwarding mode: redundancy
SCE>
```

Related Commands

Command	Description
rdr-formatter forwarding-mode	
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter destination	
show rdr-formatter enabled	
show rdr-formatter history-size	
show rdr-formatter rdr-mapping	
show rdr-formatter statistics	

show rdr-formatter history-size

Shows the configured size of the RDR formatter history buffer.

show rdr-formatter history-size

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the size of the RDR formatter history buffer.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter history-size
History buffer size: 16000 bytes
SCE>
```

Related Commands

Command	Description
rdr-formatter history-size	
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter destination	
show rdr-formatter enabled	
show rdr-formatter forwarding-mode	
show rdr-formatter rdr-mapping	
show rdr-formatter statistics	

show rdr-formatter protocol NetflowV9 dscp

Displays the NetflowV9 assigned DSCP value.

show rdr-formatter protocol NetflowV9 dscp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example illustrates the use of this command.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter protocol NetflowV9 dscp
Configured DSCP for Netflow traffic: 0
SCE>
```

Related Commands

Command	Description
rdr-formatter protocol NetflowV9 dscp	
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter destination	
show rdr-formatter statistics	

show rdr-formatter protocol NetflowV9 mapping

Displays the current Netflow mappings.

show rdr-formatter protocol NetflowV9 mapping

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show rdr-formatter protocol NetflowV9 mappinng
<tag id,template id>
<4042321920,256>
---------------------
Number of fields: 14
IsOption:  yes
NetflowIndex:  0
NetflowType:  16
NetflowId:  32770
NetflowLength:  1
------------
IsOption:  yes
NetflowIndex:  1
NetflowType:  16
NetflowId:  32769
NetflowLength:  4
------------
IsOption:  no
NetflowIndex:  2
NetflowType:  16
NetflowId:  32774
NetflowLength:  64
------------
IsOption:  no
NetflowIndex:  3
SCE#>
```

Related Commands

Command	Description
show rdr-formatter	

show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter destination	
show rdr-formatter statistics	
show rdr-formatter protocol NetflowV9 dscp	

show rdr-formatter rdr-mapping

Shows to which RDR formatter category a specified RDR tag is mapped.

show rdr-formatter rdr-mapping all|*tag-ID*

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Use the all keyword to display all current RDR-category mappings.

Authorization: viewer

Examples

The following example illustrates the use of this command, showing partial output:

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter rdr-mapping all
Tag  Categories
---  ----------
0xb2d05e01 1
0xb2d05e02 1
0xb2d05e04 1
0xb2d05e05 1
0xf0f0f000 1
0xf0f0f002 1
0xf0f0f004 1
0xf0f0f005 1
0xf0f0f010 1
0xf0f0f016 1
0xf0f0f017 1
0xf0f0f018 1
---More---
SCE>
```

Related Commands

Command	Description
rdr-formatter rdr-mapping	
show rdr-formatter	
show rdr-formatter counters	
show rdr-formatter destination	

show rdr-formatter enabled	
show rdr-formatter forwarding-mode	
show rdr-formatter history-size	
show rdr-formatter statistics	

show rdr-formatter statistics

Displays 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

User Exec

Usage Guidelines

Use this command to display the following RDR formatter statistics:

- Rates and counters per connection
- Protocol and transport attributes for each connection
- For Netflow destinations only:
  - Number of templates sent
  - Number of records sent

Authorization: viewer

Examples

The following example shows the current RDR statistics.

```
SCE>enable 5
Password:<cisco>
SCE>show rdr-formatter statistics
RDR-formatter statistics:
=========================
Category 1:
sent:  1794517
in-queue:  0
thrown:  0
format-mismatch: 0
unsupported-tags: 1701243
rate:  2 RDRs per second
max-rate:  64 RDRs per second
Category 2:
sent:  12040436
in-queue:  0
thrown:  0
format-mismatch: 0
unsupported-tags: 0
rate:  12 RDRs per second
max-rate:  453 RDRs per second
Category 3:
sent:  0
in-queue:  0
thrown:  0
```

```
format-mismatch: 0
unsupported-tags: 0
rate:  0 RDRs per second
max-rate:  0 RDRs per second
Category 4:
sent:  0
in-queue:  0
thrown:  0
format-mismatch: 0
unsupported-tags: 0
rate:  0 RDRs per second
max-rate:  0 RDRs per second
Destination: 10.56.201.50 Port: 33000 Status: up
Sent: 13835366
Rate: 211 Max: 679
Last connection establishment: 17 hours, 5 minutes, 14 seconds
Destination: 10.56.204.7 Port: 33000 Status: up
Sent: 12134054
Rate: 183 Max: 595
Sent Templates:  13732
Sent Data Records: 12134054
Refresh Timeout (Sec): 5
Last connection establishment: 17 hours, 5 minutes, 15 seconds
SCE>
```

Related Commands

Command	Description
show rdr-formatter	
show rdr-formatter connection-status	
show rdr-formatter counters	
show rdr-formatter destination	
show rdr-formatter enabled	
show rdr-formatter forwarding-mode	
show rdr-formatter history-size	
show rdr-formatter protocol NetflowV9 dscp	
show rdr-formatter rdr-mapping	

show rdr-server

Displays the RDR server configuration.

show rdr-server [counters]

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Use the **counters** keyword to display the RDR server counters.

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show rdr-server
RDR server is ONLINE
RDR server port is 33001
SCE#>
```

Related Commands

Command	Description
rdr-server	

show running-config

Shows the current configuration.

show 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

Use the all data switch to see sample usage for many CLI configuration commands.

Authorization: admin

Examples

The following example shows the partial output of the **show running-config** command.

```
SCE>enable 10
Password:<cisco>
SCE#>show running-config all-data
#This is a general configuration file (running-config).
#Created on 16:48:11 UTC WED May 13 2006
cli-type 1
#version 1
service logger
no service password-encryption
enable password level 10 0 “cisco”
enable password level 15 0 “cisco”
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

Command	Description
more	

show running-config (ROOT level options)

Displays the specified current configuration.

show running-config-application [all-data]

show running-config-all

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

This command displays either the current application configuration or the complete current configuration, depending on the option specified:

- **show running-config-application** — Displays the current application configuration (non-default values only).
- **show running-config-application all data** — Displays the current application configuration as well as all default values.
- **show running-config-all** — Displays the complete current configuration (general configuration plus application configuration).

Authorization: root

Examples

The following sample output displays a portion of the contents of the running configuration application file.

```
SCE>enable 15
Password:<cisco>
SCE#>show running-config-application
#This is an application configuration file (running-config-application).
#Created on 09:54:48 GMT WED April 26 2006
#cli-type 1
#version 1
interface Linecard 0
application /tffs0/app/eng30102.sli capacity-option "EngageDefaultSE100"
tunable "GT_GLB_currentMonth" v "4"
tunable "GT_SubsNotificationDismissMethod[0]" v "2"
lookup "GT_NotificationLUT[0]" remove-all
lookup "GT_NotificationLUT[1]" remove-all
lookup "GT_NotificationLUT[2]" remove-all
lookup "GT_NotificationLUT[3]" remove-all
--More--
SCE#>
```

Related Commands

Command	Description
more (ROOT level options)	
show running-config	

show scmp

Displays the SCMP (ISG) general configuration and status.

show scmp [all | name *name*] [counters]

Syntax Description

name	Display configuration or counters for the specified destination (SCMP peer device).

Defaults

This command has no default settings.

Command Modes

Privileged Exec

Usage Guidelines

You can display configuration for a specified destination by using the name argument. Use the **all** keyword to display configuration for all destinations.

Use the **counters** keyword to display the statistics per destination. For this option, you must either specify the desired destination, using the **name** argument, or use the **all** keyword to display statistics for all destinations.

Authorization: admin

Examples

The following example illustrates how to display the SCMP counters for a specified destination.

```
SCE>enable 10
Password:<cisco>
SCE#show scmp name scmp_peer1 counters
SCMP Connection 'scmp_peer1' counters:
Total messages sent:  72
Total messages received: 72
Establish requests sent: 1
Establish replies received: 1
Accounting requests sent: 20
Accounting replies received: 20
Subscriber queries sent: 0
Subscriber query response recv: 0
Request retry exceeded:  0
Requests replied with errors: 0
Subscriber requests received: 50
Subscriber responses sent: 50
Failed Requests:  0
Keep-alive sent:  1
Keep-alive received:  1
SCE>
```

Related Commands

Command	Description

clear scmp name counters
scmp

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the SNMP server configuration and statistics.

```
SCE>enable 5
Password:<cisco>
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

Command	Description
show snmp community	
show snmp contact	
show snmp enabled	
show snmp host	
show snmp location	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the SNMP manager communities.

```
SCE>enable 5
Password:<cisco>
SCE>show snmp community
Community: public, Access Authorization: RO,
Access List Index: 1
SCE>
```

Related Commands

Command	Description
snmp-server community	
show snmp	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the system contact.

```
SCE>enable 5
Password:<cisco>
SCE>show snmp contact
Contact: Brenda@mycompany.com
SCE>
```

Related Commands

Command	Description
snmp-server contact	
show snmp	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the SNMP server enabled status.

```
SCE>enable 5
Password:<cisco>
SCE>show snmp enabled
SNMP server status: Enabled
SCE>
```

Related Commands

Command	Description
snmp-server	
show snmp	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the destination hosts for SNMP traps.

```
SCE>enable 5
Password:<cisco>
SCE>show snmp host
Trap host: 10.1.1.205, community: public, version: SNMPv2c
SCE>
```

Related Commands

Command	Description
snmp-server host	
show snmp	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the system location.

```
SCE>enable 5
Password:<cisco>
SCE>show snmp location
Location: London_Office
SCE>
```

Related Commands

Command	Description
snmp-server location	
show snmp	

show snmp mib

Displays MIB variables.

show snmp mib ***mib variables***

Syntax Description

mib	Name of MIB to display. **MIB-II** **pcube-SE-MIB**
variables	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: *application, chassis, disk, global-controller, link, logger, module, port, rdr-formatter, subscriber, system, traffic-counters, tx-queue, vas-traffic-forwarding*

Defaults

This command has no default settings.

Command Modes

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the MIB-2 system group.

```
SCE>enable 5
Password:<cisco>
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

Command	Description

show snmp mib (ROOT level options)

Displays the pcube-se-mib traffic processor group objects.

show snmp mib pcube-se-mib traffic-processor

Syntax Description

This command has no arguments or eywords.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Authorization: root

Examples

The following example illustrates the use of this command (partial output).

```
SCE>enable 15
Password:<cisco>
SCE#>show snmp mib pcube-se-mib traffic-processor
tpModuleIndex.1 = 1
tpIndex.1 = 1
tpTotalNumHandledPackets.1 = 0
tpTotalNumHandledFlows.1 = 0
tpNumActiveFlows.1 = 0
tpNumActiveFlowsPeak.1 = 0
tpNumActiveFlowsPeakTime.1 = 6 days, 10 hours, 14 minutes, 14 seconds
tpNumTcpActiveFlows.1 = 0
tpNumTcpActiveFlowsPeak.1 = 0
tpNumTcpActiveFlowsPeakTime.1 = 6 days, 10 hours, 14 minutes, 14 seconds
tpNumUdpActiveFlows.1 = 0
tpNumUdpActiveFlowsPeak.1 = 0
tpNumUdpActiveFlowsPeakTime.1 = 6 days, 10 hours, 14 minutes, 14 seconds
tpNumNonTcpUdpActiveFlows.1 = 0
tpNumNonTcpUdpActiveFlowsPeak.1 = 0
tpNumNonTcpUdpActiveFlowsPeakTime.1 = 6 days, 10 hours, 14 minutes, 14 seconds
tpFlowsCapacityUtilization.1 = 0
--More--
SCE#>
```

Related Commands

Command	Description
show snmp mib	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the SNMP server traps status.

```
SCE>enable 5
Password:<cisco>
SCE>show 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

Command	Description
snmp-server enable traps	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows statistics from the SNTP clients.

```
SCE>enable 5
Password:<cisco>
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

Command	Description
sntp server	
sntp broadcast client	
sntp update-interval	

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

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 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 (use the **copy running-config startup-config** command to save the configuration).

Authorization: admin

Examples

The following example shows a sample output.

```
SCE>enable 10
Password:<cisco>
SCE#show 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 *<cisco>*
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

Command	Description
more	

show startup-config (ROOT level options)

Displays the specified startup configuration.

show startup-config-application

show startup-config-all

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Usage Guidelines

This command displays either the startup application configuration or the complete startup configuration, depending on the option specified:

- show startup-config-application — Displays the startup application configuration.
- show startup-config-all — Displays the complete startup configuration.

Authorization: root

Examples

The following sample output displays a portion of the startup application configuration.

```
SCE>enable 15
Password:<cisco>
SCE#>show startup-config-application
#This is an application configuration file (running-config-application).
#Created on 09:54:48 GMT WED April 26 2006
#cli-type 1
#version 1
interface linecard 0
application /tffs0/app/eng30102.sli capacity-option "EngageDefaultSE100"
tunable "GT_GLB_currentMonth" v "4"
tunable "GT_SubsNotificationDismissMethod[0]" v "2"
lookup "GT_NotificationLUT[0]" remove-all
lookup "GT_NotificationLUT[1]" remove-all
lookup "GT_NotificationLUT[2]" remove-all
--More--
SCE#>
```

Related Commands

Command	Description
more (ROOT level options)	
show startup-config	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the system operation status:

```
SCE>enable 5
Password:<cisco>
SCE>show system operation-status
System Operation status is Operational
SCE>
```

Related Commands

Command	Description

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the system uptime for the SCE platform.

```
SCE>enable 5
Password:<cisco>
SCE>show system-uptime
SCE uptime is 4 days, 13 hours, 21 minutes, 37 seconds
SCE>
```

Related Commands

Command	Description

show tacacs

Displays statistics for the TACACS+ servers.

show tacacs [all]

Syntax Description

This command has no arguments.

Defaults

This command has no default settings.

Command Modes

User Exec

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.

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

This example shows how to display statistics for all TACACS+ servers.

```
SCE>enable 5
Password:<cisco>
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>enable 10
Password:<cisco>
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

Command	Description
tacacs-server host	
tacacs-server key	
tacacs-server timeout	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows that there is one active Telnet session.

```
SCE>enable 5
Password:<cisco>
SCE>show telnet sessions
There is 1 active telnet session:
Index | Source
================
0 | 10.1.1.201
SCE>
```

Related Commands

Command	Description
telnet	
show telnet status	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows that the telnet daemon is currently enabled.

```
SCE>enable 5
Password:<cisco>
SCE>show telnet status
Telnet daemon is enabled.
SCE>
```

Related Commands

Command	Description
service telnetd	
show telnet sessions	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the time zone configured by the user.

```
SCE>enable 5
Password:<cisco>
SCE>show timezone
Time zone: ISR minutes offset from UTC: 120
SCE>
```

Related Commands

Command	Description
clock timezone	

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>enable 10
Password:<cisco>
SCE# show users
User: name = Joe
privilege level = 10
password = joespwd
is password encrypted = no
SCE#
```

Related Commands

Command	Description
username	
username privilege	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the current version information of the SCE platform.

```
SCE>enable 5
Password:<cisco>
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 :
optic mode : MM
Product S/N : CAT093604K3
Product ID : SCE2020-4XGBE-MM
Version ID : V01
Deviation :
Part number : 800-26601-01
Revision : B0
Software revision: G001
LineCard S/ : CAT09370L1Q
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, 2006 at 21:25:21
```

```
Compiler version: SANc v3.0.5 Build 32 gcc_codelets=true built on: Tue November 12 2006
09:51:57 AM.;SME plugin v1.1
Default capacity option used.
Logger status: Enabled
Platform: SCE 2000 - 4xGBE
Management agent interface version: SCE Agent 3.0.0 Build 18
Software package file: ftp://vk:vk@10.1.8.22/P:/EMB/LatestVersion/3.0.5/se1000.pkg
SCE2000 uptime is 21 minutes, 37 seconds
SCE>
```

Related Commands

Command	Description
show version all	
show version software	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows version and configuration information for all the system components.

```
SCE>enable 5
Password:<cisco>
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 : MM
Product S/N : CAT093604K3
Product ID : SCE2020-4XGBE-MM
Version ID : V01
Deviation :
Part number : 800-26601-01
Revision : B0
Software revision : G001
LineCard S/N : CAT09370L1Q
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, 2006 at 21:25:21
Compiler version: SANc v3.0.5 Build 32 gcc_codelets=true built on: Tue November 12 2006
```

```
09:51:57 AM.;SME plugin v1.1
Default capacity option used.
Logger status: Enabled
Platform: SCE2000 - 4xGBE
Management agent interface version: SCE Agent 3.0.5 Build 18
Software package file: ftp://vk:vk@10.1.8.22/P:/EMB/LatestVersion/3.0.5/se1000.pkg
SCE2000 uptime is 21 minutes, 37 secondsCurrent configuration:
======================
#This is a general configuration file (running-config).
#Created on 10:14:59 UTC TUE November 12 2006
.
interface LineCard 0
connection-mode active
no silent
.
.
Software package file: Not available
Unified management package file: /tffs0/images/um13012.pkg
SCE>
```

Related Commands

Command	Description
show version	
show version software	

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

User Exec

Usage Guidelines

Authorization: viewer

Examples

The following example shows the current software version.

```
SCE>enable 5
Password:<cisco>
SCE>show version software
Software version is: Version 3.0.5 Build 240
SCE>
```

Related Commands

Command	Description
show version	
show version all	

show watchdog

Displays watchdog software and hardware reset status (enabled/disabled).

show watchdog

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged exec

Usage Guidelines

Authorization: root

Examples

The following example illustrates the use of this command.

```
SCE>enable 15
Password:<cisco>
SCE#>show watchdog
Watchdog Software Reset is enabled.
Watchdog Hardware Reset is enabled.
SCE#>
```

Related Commands

Command	Description
show interface linecard watchdog	
watchdog hardware-reset	
watchdog software-reset	

shutdown

Enables shut mode Use the **no** form of the command to disable shut mode.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

By default, shut mode is disabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

The SCOS can be in one of two modes:

- "no shut" mode — the normal working mode; an an application is loaded and is processing the traffic.
- "shut" mode — a temporary method of making the SCOS behave like a wire despite the fact that an application is loaded. When "shut" mode is activated, all flows are closed immediately and no service is given.

  The result is the same as unloading the application, but execution is considerably faster.

Authorization: root

Examples

The following example shows how to enable shut mode.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>shutdown
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard shutdown	

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#silent
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard silent	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#no snmp-server
SCE(config)#
```

Related Commands

Command	Description
snmp-server community	
show snmp	

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

community-string	The SNMPv1 and SNMPv2c security string that identifies a community of managers that can access the SNMP server.
read-option	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.
acl-number	Number of the access list that lists the managers who may access the SCE platform via SNMP.

Defaults

no SNMP access

Command Modes

Global Configuration

Usage Guidelines

Use the **all** keyword with the **no** form of the command to remove all configured communities.

Authorization: admin

Examples

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#snmp-server community public ro 1
SCE(config)#
```

Related Commands

Command	Description
access-list	
show access-lists	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#snmp-server contact Brenda@MyCompany.com
SCE(config)#
```

Related Commands

Command	Description
show snmp contact	

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 arecurrently redundant.

Authorization: admin

Examples

The following example configures the SNMP server to send traps.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#snmp-server enable traps
SCE(config)#
```

Related Commands

Command	Description
show snmp traps	

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

address	The IP address of the SNMP server host.
traps	Optional switch, does not influence command functionality.
version	SNMP version running in the system. Can be set to 1 or 2c.
community-string	The SNMPv1 and SNMPv2c security string that identifies a community of managers that are able to access the SNMP server.

Defaults

No hosts

Command Modes

Global Configuration

Usage Guidelines

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.

Use the **all** keyword with the **no** form of the command to remove all configured hosts.

Authorization: admin

Examples

The following example adds a host destination for SNMP traps.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#snmp-server host 10.1.1.205 version 2c public
SCE(config)#
```

Related Commands

Command	Description
show snmp host	

snmp-server interface

Defines a specific SNMP server interface. Use the**no** form of this command to remove the interface definition

snmp-server interface ***interface#*** **(alias** ***alias*** **| link-up-down-trap)**

no snmp-server interface ***interface#***

Syntax Description

interface#	Number of the SNMP server interface.
alias	Logical name assigned to the interface.

Defaults

no interface

Command Modes

Global Configuration

Usage Guidelines

Use the **alias** option to assign a logical name to the specified interface.

Use the **link-up-down-trap** option to enable the link up\down trap for the specified interface.

Authorization: admin

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example defines an alias for the specified interface.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#snmp-server interface 4 alias snmp-server1
SCE(config)#
```

EXAMPLE 2

The following example enables the link up\down trap for the specified interface.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#snmp-server interface 4 link-up-down-trap
SCE(config)#
```

Related Commands

Command	Description

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#snmp-server location London_Office
SCE(config)#
```

Related Commands

Command	Description
show snmp location	

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

By default, the SNTP multicast client is disabled.

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example enables the SNTP multicast client.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#sntp broadcast client
SCE(config)#
```

Related Commands

Command	Description
show sntp	
sntp server	
sntp update-interval	

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

address	The IP address of the SNTP server.
hostname	The hostname of the SNTP server.

Defaults

SNTP uni-cast server is disabled

Command Modes

Global Configuration

Usage Guidelines

Use the **all** keyword with the **no** form of this command to disable all SNTP uni-cast servers.

Authorization: admin

Examples

The following example enables an SNTP server at a specified IP address.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#sntp server 128.182.58.100
SCE(config)#
```

Related Commands

Command	Description
show sntp	
sntp broadcast client	
sntp update-interval	

sntp update-interval

Defines the interval (in seconds) between SNTP uni-cast update queries.

sntp update-interval ***interval***

Syntax Description

interval	interval

Defaults

interval = 900 seconds

Command Modes

Global Configuration

Usage Guidelines

Authorization: admin

Examples

The following example sets the SNTP update interval for 100 seconds.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#sntp update-interval 100
SCE(config)#
```

Related Commands

Command	Description
show sntp	
sntp server	
sntp broadcast client	

speed

Configures the speed of the FastEthernet management 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

speed = auto

Command Modes

Mng Interface Configuration

Usage Guidelines

Use this command to configure the speed of the Fast Ethernet management interface.

- command mode = Mng Interface Configuration
- interface designation = 0/1 or 0/2

If the duplex mode (see **duplex**) of the relevant interface is configured to auto, changing this configuration has no effect.

Authorization: admin

Examples

The following example configures the speed of management port #1 to auto.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface mng 0/1
SCE(config if)#speed auto
SCE(config if)#
```

Related Commands

Command	Description
duplex	
interface mng	
show interface mng	

statistics-logging

Enables statistics logging and configures the time interval between logging entries. Use the **no** form of the command to disable statistics logging.

statistics-logging enable

statistics-logging frequency *time*

no statistics-logging enable

Syntax Description

time	Time interval between logging entries in seconds.

Defaults

By default, statistics logging is enabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>statistics-logging enable
SCE(config if)#>statistics-logging frequency 60 SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard statistics-logging	

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

This command has no default settings.

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 who 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.

Note Introduced subscriber aging is not supported when using VPN-based subscribers.

Authorization: admin

Examples

The following example enables subscriber aging for anonymous subscribers with a timeout period of 10 minutes.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber aging anonymous timeout 10
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard subscriber aging	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# subscriber anonymous-group export csv-file s_g_0507.csv
SCE(config if)#
```

Related Commands

Command	Description
subscriber anonymous-group import csv-file	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# subscriber anonymous-group import csv-file subscribers_groups.csv
SCE(config if)#
```

Related Commands

Command	Description
subscriber anonymous-group export csv-file	

subscriber anonymous-group name ip-range

Assigns the anonymous group to the specified range of IP addresses and optional template or to an SCMP device. Use the **no** form of the command to delete the anonymous group or remove it from the specified SCMP destination.

subscriber anonymous-group name ***group-name*** **ip-range** ***range*** **[template** ***template*** **]**

subscriber anonymous-group name ***group-name*** **ip-range** ***range*** **scmp name** ***scmp-name***

no subscriber anonymous-group (name ***group-name*** **[scmp] | all)**

Syntax Description

group-name	Name of the anonymous group
range	IP range of the anonymous group
template	Group template for the anonymous group (optional)
scmp-name	Name of the SCMP peer device(optional)

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Usage Guidelines

An anonymous susbscriber group is a specified IP range, where each IP address in the given range is treated as a separate subscriber. You can assign a subscriber template to the group so that all subscribers in the group have properties as defined by that template.

This command defines the IP range of the specified anonymous group and optionally defines a subscriber template to be assigned to all subscribers within that IP range.

Use the **scmp** option to assign the anonymous group to the specified SCMP destination. In this case, the specified anonymous group is the IP range managed by the SCMP peer device and subscribers for this anonymous group are generated when subscriber traffic from the SCMP peer device is detected. If a subscriber template has been assigned to the group, the anonymous subscribers generated have properties as defined by that template. If no subscriber template has been assigned, the default template is used.

You must define the specified SCMP peer device before assigning the anonymous group (see **scmp name**).

The **no** form of the command has three options:

- Delete the specified anonymous susbscriber group definition: **no subscriber anonymous-group name** ***group-name***
- Remove the specified anonymous susbscriber group from the specified SCMP destination: **no subscriber anonymous-group name** ***group-name*** **scmp**
- Delete all anonymous susbscriber group definitions: **no subscriber anonymous-group all**

Authorization: admin

Examples

The following examples illustrate how to use this command.

EXAMPLE 1

The following example illustrates how to assign an anonymous group to an IP range and also assign a template.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber anonymous-group name anon_group IP-range 10.10.10.0/8 template 2
SCE(config if)#
```

EXAMPLE 2

The following example illustrates how to assign an anonymous group to an SCMP device.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#scmp name peer_device1 radius radius1 secret abcdef
SCE(config)#interface linecard 0
SCE(config if)#subscriber anonymous-group name anon_group IP-range 10.10.10.0/8 scmp name
peer_device1
SCE(config if)#
```

EXAMPLE 3

The following example illustrates how to remove an anonymous group from an SCMP device.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no subscriber anonymous-group name anon_group scmp
SCE(config if)#
```

EXAMPLE 4

The following example illustrates how to remove all currently defined anonymous groups.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no subscriber anonymous-group all
SCE(config if)#
```

Related Commands

Command	Description

subscriber capacity-options

Overrides the capacity option when loading the SCA BB application.

subscriber capacity-options (enable | disable)

Syntax Description

This command has no arguments or keywords

Defaults

By default, the capacity option is enabled.

Command Modes

Linecard Interface Configuration

Usage Guidelines

You must first define the maximum number of subscribers using the **subscriber max-subscribers** command**.**

You must override the capacity option before installing the pqi file.

If you have disabled the capacity option and then the next time you load a new application you want to use the capacity option, you must re-enable the capacity option before loading the application file.

Authorization: admin

Examples

The following example illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber max-subscribers 500K
SCE(config if)#subscriber capacity-options disable
SCE(config if)#pqi install file mov2008.pqi
```

Related Commands

Command	Description
subscriber max-subscribers	
show interface linecard 0 subscriber max-subscribers	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# subscriber export csv-file gold_subscribers_04072003.csv
SCE(config if)#
```

Related Commands

Command	Description
subscriber import csv-file	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# subscriber import csv-file gold_subscribers.csv
SCE(config if)#
```

Related Commands

Command	Description
subscriber export csv-file	

subscriber max-subscribers

Specifies the maximum number of subscribers.

subscriber max-subscribers (100K | 250K | 500 K | 1M)

Syntax Description

This command has no arguments or keywords.

Defaults

Default = 250K

Command Modes

Linecard Interface Configuration

Usage Guidelines

For this maximum to take effect, you must also do the following:

1. Disable the capacity option (see **subscriber capacity-options)**
2. Load a new application (see **pqi install**)

Authorization: admin

Examples

The following example illustrates how to use this command.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber max-subscribers 500K
SCE(config if)#subscriber capacity-options disable
SCE(config if)#pqi install file mov2008.pqi
```

Related Commands

Command	Description
subscriber capacity-options	
show interface linecard 0 subscriber max-subscribers	

subscriber name property

Assigns a value to the specified property of the specified subscriber.

subscriber name ***subs-name*** **property** ***propertyname*** **value** ***property-val***

Syntax Description

subs-name	Name of the subscriber.
propertyname	The subscriber property for which the value is to be assigned
property-val	The value to be assigned

Defaults

This command has no default settings.

Command Modes

Linecard Interface Configuration

Usage Guidelines

This command can be used to enable or disable the generation of the real-time subscriber usage RDRs (see example below).

To enable RDR generation, set *propertyname* = monitor and *property-val* = 1

To disable RDR generation, set *propertyname* = monitor and *property-val* = 0

To enable subscriber monitoring for a group of subscribers, create a text file containing the sequence of CLI commands, including the commands to access the appropriate CLI mode. The file would look something like this:

configure

interface linecard 0

subscriber name Jerry property monitor value 1

subscriber name George property monitor value 1

subscriber name Elaine property monitor value 1

subscriber name Kramer property monitor value 1

subscriber name Newman property monitor value 1

Use the **script run** command to run the script.

Authorization: admin

Examples

The following example disables the generation of the real-time subscriber usage RDRs for subscriber jane_smith.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber name jane_smith property monitor value 0
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard subscriber name	

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 timeout *timeout*

default subscriber sm-connection-failure

Syntax Description

timeout	The timeout interval in seconds.
force-failure	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.
none	No action needs to be taken in the event of any loss of connection between the SCE platform and the SM
remove-mappings	Remove all current subscriber mappings n the event of any loss of connection between the SCE platform and the SM
shut	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 examples illustrate how to use this command.

EXAMPLE 1

The following example configures forced failure of the SCE platform in case of failure of the SM.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE (config if)#subscriber sm-connection-failure action force-failure
SCE (config if)#
```

EXAMPLE 2

The following example sets the timeout interval to two minutes (120 seconds).

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE (config if)#subscriber sm-connection-failure timeout 120
SCE (config if)#
```

Related Commands

Command	Description
show interface linecard subscriber sm-connection-failure	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# subscriber template export csv-file gold0507.csv
SCE(config if)#
```

Related Commands

Command	Description
subscriber template import csv-file	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# subscriber template import csv-file gold0507.csv
SCE(config if)#
```

Related Commands

Command	Description
subscriber template export csv-file	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber tp-mappings max-tp-ip-ranges 500
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard subscriber mapping included-in tp-ip-range	
show interface linecard subscriber tp-mappings statistics	

subscriber tp-ip-range **name ip-range** **target-tp**	
subscriber tp-ip-range **{import | export}** **csv-file**	

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** ***ip-range*** **target-tp** ***target-tp*** **[remove-subscriber-mapping]**

no subscriber tp-ip-range [name ***name*** **| all] [remove-subscriber-mapping]**

Syntax Description

TP-IP-range nam	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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber tp-ip-range name CMTS1 ip-range 10.10.10.0/128 target-tp 5
remove-subscriber-mappings
SCE(config if
)#
```

Related Commands

Command	Description
show interface linecard subscriber tp-ip-range	
show interface linecard subscriber tp-mappings statistics	

subscriber **tp-mappings**
subscriber tp-ip-range **{import | export}** **csv-file**

subscriber tp-ip-range {import | export} csv-file

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*** **[remove-subscriber-mapping]**

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

Following is the format of the csv file:

```
range name, ip-address/mask-length, target-TP
```

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#subscriber TP-IP-range import csv-file TIR_definitions
remove-subscriber-mappings
```

Related Commands

Command	Description
show interface linecard subscriber TP-IP-range	
show interface linecard subscriber TP-mappings statistics	

subscriber **TP-mappings**
subscriber **TP-IP-range name** **IP-range target-TP**

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**)

Similarly, the user can configure a global default key that will be applied to all TACACS+ server hosts. (See **tacacs-server key**)

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#tacacs-server host server1 timeout 8
SCE(config)#
```

Related Commands

Command	Description
tacacs-server key	
tacacs-server timeout	
show tacacs	

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

key-string	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

This default key can be overridden for a specific TACACS+ server host by explicitly configuring a different key for that TACACS+ server host.

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.

Authorization: admin

Examples

The following example show how to configure the keystring.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#tacacs-server key ABCDE
SCE(config)#
```

Related Commands

Command	Description
tacacs-server host	
tacacs-server timeout	
show tacacs	

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE>(config)#tacacs-server timeout 10
SCE>(config)#
```

Related Commands

Command	Description
tacacs-server host	
tacacs-server key	
show tacacs	

tcp bypass-establishment

Enables bypassing TCP flow establishment. Use the **no** form of the command to disable bypassing TCP flow establishment.

tcp bypass-establishment

no tcp bypass-establishment

Syntax Description

This command has no arguments or keywords.

Defaults

By default, bypassing TCP flow establishment is enabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Authorization: root

Examples

The following example shows how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>
SCE(config if)#>tcp bypass-establishment
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard tcp	

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>enable 10
Password:<cisco>
SCE#telnet 10.1.5.120
connecting to 10.1.5.120:23...
```

Related Commands

Command	Description
show telnet sessions	
service telnetd	

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

time	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>enable 10
Password:<cisco>
SCE#config
SCE(config)#line vty 0
SCE(config-line)#timeout 45
SCE(config-line)#
```

Related Commands

Command	Description
telnet	

tos-marking clear-table

Clears the TOS translation table, setting the DSCP value for all table entries to '0'.

tos-marking clear-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: root

Examples

The following example illustrates how to use this command.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#>interface linecard 0
SCE(config if)#>tos-marking clear-table
SCE(config if)#>
```

Related Commands

Command	Description
tos-marking set-table-entry	
show interface linecard tos-marking	

tos-marking enabled

Enables TOS marking for the egress interface. Use the**no** form of the command to disable TOS marking for the interface. Use the **default** form of the command to restore the default TOS marking mode (disabled). (Currently the **no** and**default** forms of the command are interchangeable.)

tos-marking enabled

no tos-marking enabled

default tos-marking enabled

Syntax Description

This command has no arguments or keywords.

Defaults

By default, TOS marking is disabled.

Command Modes

Interface GigabitEthernet Configuration

Usage Guidelines

ToS marking must be explicitly enabled or disabled for each interface separately by entering the Interface GigabitEthernet Configuration mode for the interface (0/1, 0/2, 0/3, or 0/4) and executing the relevant command.

Authorization: root

Examples

The following example enables TOS marking for the cascade ports:

```
SCE2000>enable 15
Password:<cisco>
SCE2000#>config
SCE2000(config)#>interface gigabitethernet 0/3
SCE2000(config if)#>tos-marking enabled
SCE2000(config if)>exit
SCE2000(config)#>interface gigabitethernet 0/4
SCE2000(config if)#>tos-marking enabled
SCE2000(config if)#>
```

Related Commands

Command	Description
show interface linecard tos-marking	
tos-marking set-table-entry	

tos-marking set-table-entry

Configures an entry in the TOS translation table.

tos-marking set-table-entry tos-id *tos-id* tos-value tos-value

Syntax Description

tos-id	TOS ID (integer between 1 and 7) Note that when specifying a TOS ID in defining either a flow filter rule or a traffic rule, '0' is a legal value, indicating 'do not remark'. However, it is not a legal value in the TOS translation table.
tos-value	DSCP value to be assigned to the TOS ID (integer between 0 and 63). The DCSP values are the actual values written to the ToS field in IP header of the packet. DSCP values do not have to be unique, the same value can be assigned to more than one TOS ID.

Defaults

By default, all table entries are set to '0'.

Command Modes

Linecard Interface Configuration

Usage Guidelines

Authorization: root

Examples

The following example sets a TOS marking table entry.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config)#>interface linecard 0
SCE(config if)#>tos-marking set-table-entry tos-id 1 tos-value 63
SCE(config if)#>
```

Related Commands

Command	Description
tos-marking enabled	
tos-marking clear-table	
show interface linecard tos-marking	

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#tracert 64.103.125.118
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(config if)#
```

Related Commands

Command	Description
show ip route	

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#traffic-counter name counter1 count-bytes
SCE(config if)#
```

EXAMPLE 2:

The following example demonstrates how to delete all traffic counters.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no traffic-counter all
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard traffic-counter	
clear interface linecard traffic-counter	

traffic-rule

Defines a new traffic rule. Use the **no** form of the command to delete an existing traffic rule.

traffic-rule name ***name*** **ip addresses** ***ip-addresses*** **protocol** ***protocol*** **[port** ***port-id*****] [tunnel-id** ***tunnel-id*** **] direction** ***direction*** **traffic-counter name** ***traffic-counter*** **action** ***action***

traffic-rule tunnel-id-mode

no traffic-rule {name ***name*** **|all|tunnel-id-mode}**

Syntax Description

name	name to be assigned to this traffic rule.
IP-addresses	subscriber-side and network-side <IP specification>(see Usage Guidelines)
protocol	Any one of the following protocols: **TCP/UDP/ICMP/IGRP/EIGRP/IS-IS/OSPF/Other**
port	If the protocol is TCP or UDP, define a port or range of ports for each side (subscriber/network). (see Usage Guidelines)
tunnel-id	Tunnel ID, <tunnel Id specification>(see Usage Guidelines)
direction	upstream/downstream/both
traffic-counter	name of traffic counter/none
action	action to be performed on flows that meet the rule criteria (see Usage Guidelines)

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.

port specification:

all|([all-but] [port#] [port-range])

- Specify the port or port range for both the subscriber-side and the network-side.
- Specify a range of ports using the form MinPort:MaxPort.
- Specify the ports only if the protocol is either TCP or UDP.

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 name:

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.

action:

One of the following:

- block — Block the specified traffic
- ignore — Bypass the specified traffic; traffic receives no service
- quick-forwarding — Quick forwarding (duplication) of delay-sensitive packets with service.
- quick-forwarding-ignore — Quick forwarding (duplication) of delay-sensitive packets with no service.

Authorization: admin

Examples

The following examples illustrate how to use this 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
- subscriber-side port = 100
- network-side ports = all-but 200
- Direction = downstream
- Traffic counter = counter2
- Action = Block
- The actions performed will be counting and blocking

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
```

```
SCE(config if)# traffic-rule name rule2 ip-addresses subscriber-side all network-side
all-but 10.10.10.0/24 protocol tcp ports subscriber-side 100 network-side all-but 200
direction downstream traffic-counter name counter2 action block
SCE(config if)
```

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# traffic-rule name rule3 ip-addresses all protocol is-is direction upstream
traffic-counter name none action ignore
SCE(config if)
```

Example 3:

The following example demonstrates how to delete all traffic rules.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# no traffic-rule all
SCE(config if)
```

Related Commands

Command	Description
show interface linecard traffic-rule	

traffic-rule (ROOT level options)

Defines a new traffic rule. This is an admin level command with additional options that are available only at the Root level.

traffic-rule name ***name*** **ip addresses** ***IP-addresses*** **protocol** ***protocol*** **[tunnel-id** ***tunnel-id*** **] direction** ***direction*** **traffic-counter name** ***traffic-counter*** **action** ***action*** **[upstream-tos-id** ***tos-id1*** **downstream-tos-id** ***tos-id2*** **]**

no traffic-rule capture rules

Syntax Description

	See **traffic-rule** for a complete description of the syntax.
action	See the **Usage Guidelines** below for additional options available only at the Root level.
tos-id1	The ID of the entry in the TOS translation table to be assigned to the upstream traffic (0-7). • '0' indicates 'do not remark'. • A value of 1-7 indicates that the DSCP value assigned to that ID in the translation table will be inserted in the TOS field.
tos-id2	The ID of the entry in the TOS translation table to be assigned to the downstream traffic (0-7). • '0' indicates 'do not remark'. • A value of 1-7 indicates that the DSCP value assigned to that ID in the translation table will be inserted in the TOS field.

Defaults

Default tos-id = 0 (do not remark)

Command Modes

Interface Linecard Configuration

Usage Guidelines

This is an admin level command with additional options that are available only at the Root level. These options allow you to do the following:

- Specify Classical Open Flow mode for the defined flow
- Define a flow capture rule.
- Delete the flow capture rule.
- Define TOS marking to be applied to traffic matching this rule

See **traffic-rule** for a complete description of this command.

The following action and TOS marking options are available only at the Root authorization level.

Action

The following are the additional action options available to Root authorization users. (block, ignore, quick-forwarding, and quick-forwarding-ignore are available at both the admin and the root level)

action

- classical-open-flow-mode — Use Classical Open Flow mode for this flow.
- flow-capture — Capture the flow configured by this rule. No service to this flow.

Note Only one flow capture rule can be defined in the system at a time. If the **flow-capture** option is assigned to a rule when a flow capture rule already exists, a warning message appears.

Use the **no traffic-rule capture rules** command to delete the current flow capture rule.

TOS Marking

At the Root authorization level only, you can configure a TOS marking to be applied by this traffic rule. If you configure TOS marking, you must configure a value for both upstream and downstream traffic, although those values do not need to be the same.

TOS marking must be enabled for the relevant interfaces (see **tos-marking enabled**) and the TOS translation table defined (see **tos-marking set-table-entry**).

TOS marking cannot be used if **tunnel-id mode** is enabled and tunnel ID parameters are defined.

One action (with the exception of 'block') may be defined for these flows, but is not required. Blocking is incompatible with TOS marking.

Authorization: root

Examples

The following examples illustrate how to use the Root level options for this command.

Example 1

The following example illustrates how to configure a traffic rule that will be used as a recording rule using the flow-capture option. All flows that apply to this rule will be recorded to the location given in rule configuration.

1. Name = FlowCaptureRule
2. IP addresses: subscriber side = all IP addresses, network side = all IP addresses
3. Direction = both
4. Protocol = 250
5. Traffic counter name = counter2
6. Action = flow-capture
7. The actions performed will be counting and flow capture.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>traffic-rule name FlowCaptureRule ip-addresses subscriber-side all
network-side all protocol 250 direction both traffic-counter name counter2 action
flow-capture
SCE(config if)#>
```

Example 2

The following example illustrates how to configure a traffic rule thatwill apply TOS marking and quick forward the marked traffic.

1. Name = TOSMarkingRulewithAction
2. IP addresses: subscriber side = all IP addresses, network side = all IP addresses
3. Direction = both
4. Protocol = 1100
5. Traffic counter name = counter2
6. Action = quick forwarding
7. TOS marking: upstream TOS ID = 1, downstream TOS ID = 0 (do not remark)

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>traffic-rule name TOSMarkingRulewithAction ip-addresses subscriber-side
all network-side all protocol 1100 direction both traffic-counter none action
quick-forwarding upstream-tos-id 1 downstream-tos-id 0
SCE(config if)#>
```

Example 3

The following example illustrates how to configure a traffic rule that will apply TOS marking, with no other actions configured.

1. Name = TOSMarkingRuleNoAction
2. IP addresses: subscriber side = all IP addresses, network side = all IP addresses
3. Direction = both
4. Protocol = 1100
5. TOS marking: upstream TOS ID = 1, downstream TOS ID = 0 (do not remark)

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>traffic-rule name TOSMarkingRuleNoAction ip-addresses subscriber-side all
network-side all protocol 1100 direction both traffic-counter none upstream-tos-id 1
downstream-tos-id 0
SCE(config if)#>
```

Related Commands

Command	Description
traffic-rule	
show interface linecard traffic-rule	

tunable

Sets the value of the specified application tunable. Use the**tunables** (plural) form of the command to the set the value for up to 19 tunables in one command.

tunable ***tunable-name*** **value** ***tunable-value***

tunables name ***tunable-name*** **value** ***tunable-value*** **name** ***tunable-name*** **value** ***tunable-value*****...**

Syntax Description

tunable-name	The name of the specific tunable.
tunable-value	Value to assign to the tunable.

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

When using the **tunables** form of the command (plural), make sure to use the **name** keyword before the name of each specific tunable in the list.

Authorization: root

Examples

The following example shows how to set multiple application tunables in one command.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>tunables name currentMonth value 6 name SubsNotificationDismissMethod
value 2,0*31 name packetDumpPort value 4
SCE>(config if)#>
```

Related Commands

Command	Description
show applications slot tunable	

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>enable 10
Password:cisco>
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

Command	Description

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

name	Name of the user to be added
password	A clear text password.
secret	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

The following examples illustrate how to use this command.

Example 1

This example shows how to add a new user to the local database with a clear text password.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#username johndoe password mypassword
SCE(config)#
```

Example 2

This example shows how to add a new user to the local database with no password.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#username johndoe nopassword
SCE(config)#
```

Example 3

This example shows how to add a new user to the local database with an MD5 encrypted password entered in clear text.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#username johndoe secret 0 mypassword
SCE(config)#
```

Related Commands

Command	Description
show users	
username privilege	

username privilege

Sets the privilege level for the specified user.

username ***name*** **privilege** ***level***

Syntax Description

name	name of the user whose privilege level is set
level	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>enable 10
Password:<cisco>
SCE#config
SCE(config)#username johndoe privilege 5
SCE(config)#
```

Related Commands

Command	Description
show users	
username	

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 disable VAS traffic forwarding. You must first shutdown the linecard before disabling VAS forwarding, since there may still be some open flows that have already been forwarded to the VAS servers. If the VAS feature is stopped while there are still such flows open, their packets coming back from the VAS servers may be routed to their original destination with the VLAN tag of the VAS server on it.

Note that, although this command is an admin level command, you must enter the ROOT authorization level (15) to shutdown the linecard.

```
SCE>enable 15
Password:<cisco>
SCE#>config
SCE(config if)#>interface linecard 0
SCE(config if)#>shutdown
SCE(config if)#>no vas-traffic-forwarding
SCE(config if)#>no shutdown
SCE(config if)#>
```

Related Commands

Command	Description
vas-traffic-forwarding vas server-id	
vas-traffic-forwarding vas traffic-link	
vas-traffic-forwarding vas server-id health-check	
vas-traffic-forwarding vas server-group	
vas-traffic-forwarding vas server-group failure	
show interface linecard vas-traffic-forwarding	

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*|*auto-select*}

no vas-traffic-forwarding traffic-link

Syntax Description

Enter the link number on which to transmit VAS traffic

- **Link-0**
- **Link-1**
- **auto-select** : the active VAS link is selected by the system

Defaults

Default traffic link = Link-1

Command Modes

Interface Linecard Configuration

Usage Guidelines

Use the **auto-select** keyword with VAS over 10G. For VAS over 10G, the VAS link should always be set to auto-select, so that the system can switch to the backup link when necessary.

Note The VAS traffic link should be in Forwarding mode.

Authorization: admin

Examples

This example shows how to configure link 0 for VAS traffic.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding traffic-link link-0
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding	
vas-traffic-forwarding vas server-id	
vas-traffic-forwarding vas server-group	

vas-traffic-forwarding **vas server-group** **failure**
show interface **linecard** **vas-traffic-forwarding**

vas-traffic-forwarding traffic-link auto-select

Configures the VAS traffic link for VAS over 10G.

vas-traffic-forwarding traffic-link auto-select [link-switch-delay *switch-time* | initial-selection {*link-0*|*link-1* }]

no vas-traffic-forwarding traffic-link auto-select [link-switch-delay|initial-selection]

default vas-traffic-forwarding traffic-link auto-select [link-switch-delay|initial-selection]

Syntax Description

switch-time	The time in seconds to delay between two consecutive link switches on initial health check state.
initial-selection	Enter the link number to be set as the active VAS link (the link on which to transmit VAS traffic after a system reload and when working in auto-select mode). • **Link-0** • **Link-1**

Defaults

Default switch-time = 30 seconds

Default traffic link = Link-1

Command Modes

Interface Linecard Configuration

Usage Guidelines

For VAS over 10G, since the link used for forwarding VAS traffic may change automatically due to a failover situation, the following options must be configured:

- Set the VAS traffic link to auto-select, so that the system can select the link connected to the active 7600/VAS servers system.
- Specify the minimum time allowed between two consecutive link switches.
- Specify the link on which to transmit VAS traffic after a system reload and when in auto-select mode

To set the VAS traffic link to auto-select, use the basic command with no options (the same as using the **VAS-traffic-forwarding VAS traffic-link** command and specifying **auto-select**)

. To set the minimum time allowed between two consecutive link switches, use the **link-switch-delay** option. In 10G topology, the default delay between two consecutive link switches (30 seconds) is less than the time it takes for the health check to fail. This means that in cases where there is at least one failed VAS server group on both links, the SCE platform will flip continuously between the links. To avoid the constant flip between the links in such a case, it is recommended to configure a link-switch-delay time greater than 3 minutes.

To specify the link on which to transmit VAS traffic after a system reload and when in auto-select mode (the active VAS link), use the **initial-selection** option. Note that when executed, this command triggers an immediate link switch if the currently active VAS traffic link used is different from the one specified in the command.

Use the **default**form of the command to set either the **link-switch-delay** or the **initial-selection** to the default value. You can also use the **no** form of the command for the same purpose, since it removes the configured value, which results in the default value being restored.

Authorization: admin

Examples

The following examples show how to use this command.

Example 1

This example shows how to set the initial-selection to link-0.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding traffic-link auto-select initial-selection link-0
SCE(config if)#
```

Example 2

This example shows how to set the ilink-switch-delay to 60 seconds.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding traffic-link auto-select link-switch-delay 60
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding vas traffic-link	
show interface linecard vas-traffic-forwarding	

vas-traffic-forwarding vas debug

This command specifies the options to be used when debugging a VAS installation.

vas-traffic-forwarding vas debug force-redirect-flows-to-vas

vas-traffic-forwarding vas debug force-report-open-from-vas

vas-traffic-forwarding vas debug server-id *number* force-state {down | no-force | up}

Syntax Description

number	VAS server ID number

Defaults

This command has no default settings.

Command Modes

Interface Linecard Configuration

Usage Guidelines

This command presents the following options to be used when debugging a VAS installation:

- Force all new flows to be redirected to a logical VAS server
- Force 'opened from VAS' to be reported to the application
- Force a specific state on a specified VAS server

Authorization: root

Examples

The following example shows how to force a specified VAS server down.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>vas-traffic-forwarding VAS debug server-id 25 force-state down
SCE(config if)#>
```

Related Commands

Command	Description

vas-traffic-forwarding vas health-check

Configures the health check for compatibility with VAS over 10G (multiple GBE platform (MGSCP)) topology. It also defines the IP addresses to be used for the VAS health check in a VAS over 10G topology. Use the **ip-address** keyword to define source and destination IP addresses to be used by the health check packets. Use the**no** form of this command to disable health check compatibility for VAS over 10G. Use either the **no** or**default** form of this command with the **ip-address** keyword to remove the IP address configuration.

vas-traffic-forwarding health-check topology mgscp

vas-traffic-forwarding health-check ip-address source *source-ip* destination *dest-ip*

no vas-traffic-forwarding health-check topology mgscp

default vas-traffic-forwarding health-check topology mgscp

no vas-traffic-forwarding health-check ip-address

default vas-traffic-forwarding health-check ip-address

Syntax Description

source-ip	Health check source IP address. The source-ip must include a range indication (x.x.x.x/x).
dest-ip	Health check destination IP address. The dest-ip does not include a range indication.

Defaults

By default, the compatibility with VAS over 10G (multiple GBE platforms(MGSCP)) is disabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

Use the **topology MGSCP** keywords to enable or disable (use the **no** form of the command) health check compatibility for VAS over 10G.

Use the **ip-address** keyword to define **source** and **destination** IP addresses to be used by the health check packets.

- A range of source IP addresses (at least eight) is required.
- The configured IP addresses should not be in use in the network. They must be dummy IP addresses that are reserved for the VAS health check only. (Use the **pseudo-ip** command to configure these IP addresses.)
- The same IP address should be configured for all the SCE platforms under the same EtherChannel.

Authorization: admin

Examples

The following examples illustrate how to enable multiple GBE platform compatibility for the VAS health check, and how to define the IP addresses.

Example 1

This example shows how to enable multiple GBE platform compatibility for the VAS health check.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding health-check topology mgscp
SCE(config if)#
```

Example 2

This example shows how to define the source and destination IP addresses.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding health-check ip-address source 20.20.20.20/28
destination 10.10.10.10
SCE(config if)#
```

Example 3

This example shows how to remove the IP address configuration using the **no** keyword.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no vas-traffic-forwarding health-check ip-address
SCE(config if)#
```

Example 3

This example shows how to remove the IP address configuration using the **default** keyword.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#default vas-traffic-forwarding health-check ip-address
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding	
show interface linecard vas-traffic-forwarding	
pseudo-ip	

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-traffic-forwarding 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 = two port numbers for each server, starting with ports 63140 and 63141 used for server #0 through ports 63154 and 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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no vas-traffic-forwarding vas server-id 5 health-check
SCE(config if)#
```

Example 2

This example shows how to define the source and destination ports for VAS server 5 and enable the health check.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding vas server-id 5 health-check udp ports source 63150
destination 63151
SCE(config if)#vas-traffic-forwarding vas server-id 5 health-check
SCE(config if)#
```

Example 3

This example shows how to remove the UDP port configuration using the **no** keyword.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no vas-traffic-forwarding vas server-id 5 health-check udp ports
SCE(config if)#
```

Example 4

This example shows how to remove the UDP port configuration using the **default** keyword.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#default vas-traffic-forwarding vas server-id 5 health-check udp ports
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding	
vas-traffic-forwarding vas server-id	
vas-traffic-forwarding vas traffic-link	

vas-traffic-forwarding vas server-group
vas-traffic-forwarding vas server-group failure
show interface linecard vas-traffic-forwarding

vas-traffic-forwarding vas 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

number	The ID number of the VAS server
vlan-number	The VLAN tag to use for the specified VAS server

Defaults

Default vlan-number = No VLAN

Command Modes

Linecard Interface Configuration

Usage Guidelines

Note the following important points:

- 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).

Authorization: admin

Examples

The following example assigns the vlan id = 10 to server ID number = 4.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding vas server-id 4 vlan 10
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding	
vas-traffic-forwarding vas server-id	
vas-traffic-forwarding vas server-group	

vas-traffic-forwarding vas server-group failure	
vas-traffic-forwarding vas traffic-link	
show interface linecard vas-traffic-forwarding	

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

Usage Guidelines

The user may define up to eight VAS server groups. Each VAS server group has the following parameters:

- 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**).

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vas-traffic-forwarding vas server-group 1 vas server-id 5
SCE(config if)#
```

Example 2

This example shows how to remove VAS server 5 from VAS server group 1.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no vas-traffic-forwarding vas server-group 1 vas server-id 5
SCE(config if)#
```

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#no vas-traffic-forwarding vas server-group 1
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding	
vas-traffic-forwarding vas server-id	
vas-traffic-forwarding vas traffic-link	
vas-traffic-forwarding vas server-id health-check	
vas-traffic-forwarding vas server-group failure	
show interface linecard vas-traffic-forwarding	

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 in 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.**)

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#SCE(config-if)#vas-traffic-forwarding vas server-group 5 failure
minimum-active-servers 3
SCE(config if)#
```

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>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#SCE(config-if)#default vas-traffic-forwarding vas server-group 5 failure
minimum-active-servers
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding	
vas-traffic-forwarding vas server-id	
vas-traffic-forwarding vas traffic-link	
vas-traffic-forwarding vas server-id health-check	
vas-traffic-forwarding vas server-group	
show interface linecard vas-traffic-forwarding	

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

number	The ID number of the VAS server

Defaults

By default, a defined VAS server is enabled.

Command Modes

Linecard Interface Configuration

Usage Guidelines

The VAS server is not operational until the VLAN tag is defined (vas-traffic-forwarding server-id vlan).

Authorization: admin

Examples

The following examples illustrate how to create, enable, and disable a VAS server.

Example 1

The following example defines a VAS server, server ID number = 4, that is not yet operational.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# vas-traffic-forwarding vas server-id 4 enable
SCE(config if)#
```

Example 2

The following example disables the VAS server, but does not delete the server definition or the associated VLAN tag.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)# vas-traffic-forwarding vas server-id 4 disable
SCE(config if)#
```

Related Commands

Command	Description
vas-traffic-forwarding	
vas-traffic-forwarding server-id vlan	
vas-traffic-forwarding vas traffic-link	
vas-traffic-forwarding vas server-id health-check	
vas-traffic-forwarding vas server-group	
vas-traffic-forwarding vas server-group failure	
show interface linecard vas-traffic-forwarding	

virtual-links index direction

Adds a new virtual link. It also optionally changes the PIR values for a specified Global Controller configured in the SCA BB application.

Use the **no** form of the command to remove a specified virtual link.

virtual-links index *vl-index* **direction [upstream | downstream]**

virtual-links index *vl-index* **direction [upstream | downstream] gc** *relative-gc-index* **set-PIR value** *[']PIR-value[, PIR-value2, PIR-value3, PIR-value4']*

virtual-links index *vl-index* **direction [upstream | downstream] gc** *relative-gc-index* **reset-PIR**

no virtual-links index *vl-index* **direction [upstream | downstream]**

Syntax Description

vl-index	Index number assigned by the user to the virtual link.
relative-gc-index	The index number of the global controller (GC) whose PIR values you want to change. Make sure this index is the number of the desired GC template for the specified direction (upstream or downstream).
PIR-value	The PIR value to be assigned to the specified GC. You can either specify one PIR value that will be used for all time-frames, or specify four PIR values, one for each time-frame. If specifying four values, separate the values with commas and enclose the entire argument in quotes. For example: 'w,x,y,z'
direction	Specify the direction for this virtual link (**upstream** or **downstream**).

Defaults

This command has no default settings.

Command Modes

Interface linecard configuration.

Usage Guidelines

You can configure virtual links when the physical link that the SCE platform monitors is actually composed of multiple smaller links that you want to monitor and control separately. With virtual links, instead of creating hundreds or even thousands of separate packages with the specific bandwidth configuration for each small link, you can create a policy with a limited number of basic packages, each with a standard bandwidth configuration. Any specific bandwidth configuration is easily adjusted for each virtual link by reconfiguring the relevant Global Controller.

The virtual links solution consists of three separate stages in three different components of the Cisco Service Control solution:

- Create and apply a virtual links policy with the template Global Controllers.

  The policy is managed and applied via the GUI or API.
- Create the virtual links and optionally set any specific bandwidth configuration in the Global Controllers.

Virtual links are created and managed in the SCE via a set of CLI commands.

- Set the virtual link names in the CM.

  The virtual link names are set using a command line utility (CLU) in the CM. These names are used in the the Virtual Links Reports.

Direction

Virtual links are directional. In the CLI commands, a virtual link is always identified by both the index number assigned to the virtual link and the direction (upstream or downstream).

Always use the **direction** keyword and specify **upstream** or **downstream**.

Global Controller (GC) Templates

The virtual links policy created in the SCA BB console specifies Global Controllers that will be used as bandwidth templates for the virtual links. When a new virtual link is created using this command, it receives a set of the directional template VL Global Controllers with their PIR values as configured in the SCA BB console.

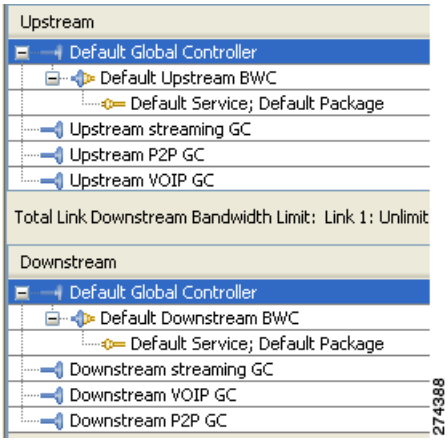
In some cases, you may want to modify the PIR values of a particular template GC for use with a particular virtual link:

- Use the **set-PIR** keyword with the desired PIR value to change the PIR value of a specified GC associated with a specified virtual link.
- Use the **reset-PIR** keyword with no PIR values to reset the PIR values of a specified GC to the original values, as configured via the console.

Global Controllers -Relative Index

To specify the GC, use the **gc** keyword and then indicate the relative GC index. This is the number of the relevant GC as found in the GC configuration for the specified direction. Note that GC numbering starts at 0 for the default BWC in each direction, so the third user-configured GC, for example, is number ‘3’. In the GC configuration pictured below, the relative index for the P2P GC for upstream is ‘2’ and for downstream is ‘3’.

Note Each GC also has an absolute index. Referring to the configuration below, you see that there are six configured GCs altogether, each of which is identified internally by a unique index. This absolute index does not concern us when identifying a particular GC in these commands.



PIR Values

Either one or four PIR values are configured for each template GC. By default, the SCA BB calendar function contains four time frames. You can configure a different PIR for each time frame or only one PIR that will be applied to all time frames.

Examples

The following examples illustrate the use of this command.

Example 1

This example shows how to create a new virtual link for the downstream direction.

```
SCE>enable
password<cisco>
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)#virtual-links index 10 direction downstream
```

Example 2

This example shows how to change the PIR values for a particular template GC (the third one, which is number 2) for the specified virtual link. Make sure to use the proper index number from the correct direction for the GC.

Note that the four PIR values are separated by commas and all enclosed in quotes.

```
SCE>enable
password<cisco>
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)#virtual-links index 10 direction downstream gc 2 set-PIR value
'10000,50000,50000,10000'
```

Example 3

This example shows how to remove a virtual link.

Make sure to specify the direction.

```
SCE>enable
password<cisco>
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)#no virtual-links index 10 direction downstream
```

Related CommandsE

Command	Description
show interface linecard virtual-links	

vlan

Configures the VLAN environment. A single VLAN tag is supported per packet (no QinQ support).

vlan symmetric skip

vlan a-symmetric skip

vlan symmetric classify

default vlan

Syntax Description

See "Usage Guidelines.

Defaults

Default mode = symmetric skip

Command Modes

Linecard Interface Configuration

Usage Guidelines

The various VLAN modes act as follows:

- **vlan symmetric skip** : ignore tunnel
- **vlan a-symmetric skip** : ignore tunnel, asymmetric
- **vlan symmetric classify** : VLAN tag as subscriber
- When the tunneling information is ignored, the subscriber identification is the subscriber IP of the IP packet carried inside the tunnel.

Use the **symmetric skip** form of the command to skip the VLAN header when VPN and flow classification do not use the VLAN tag. VLAN tags are symmetric.

Use the **a-symmetric skip** form of the command to skip the VLAN header when VPN and flow classification do not use the VLAN tag. VLAN tags are asymmetric. Note that this form of the command incurs a performance penalty.

Use the **symmetric classify** form of the command when VPN and flow classification use the VLAN tag. VLAN tags are symmetric. Using VLAN classification is mutually exclusive with any other tunnel-based classification.

Use the **default** keyword to set the VLAN configuration to the default value.

Symmetric and Asymmetric Environments

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 of the same flow 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.

Changing VPN Modes

VPNs can only exist in either **VLAN symmetric classify** or **MPLS VPN auto-learn,** but these two modes cannot be enabled simultaneously. When changing from one of these VPN-related modes to another, keep the following guidelines in mind:

- All VPN-based subscribers must be cleared in order to change the tunneling mode. If the connection with the SM is down, use the **no subscriber all with-vpn-mappings** CLI command.
- All VPN mappings must also be removed. This can only be done via the SM CLU (which means that the connection with the SM must be up).

Authorization: admin

Examples

The following example enables VLAN-based classification.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vlan symmetric classify
SCE(config if)#
```

Related Commands

Command	Description
vlan translation	
show interface linecard vlan	

vlan translation

Sets the VLAN translation constant for the network port side, and specifies whether to increment or decrement the received VLAN tag. The subscriber port side automatically performs the reverse operation. 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	Integer value by which the VLAN tag is to incremented or decremented at the network port side.

Defaults

value = 0

Command Modes

Linecard Interface Configuration

Usage Guidelines

The configured translation is applied to the network port side. The reverse operation is automatically performed at the subscriber side.

For example, if "increment 5" is defined, at the network port the VLAN is incremented by 5, and at the subscriber port the VLAN is decremented by 5.

In this case, the network side VLAN tags might be 105, 205, 305, and the subscriber side the VLAN tags would then be 100, 200, 300.

Make sure that the same VLAN translation constant is configured for all SCE platforms in the system.

Note the following limitations when VLAN translation is enabled:

- LIC Bypass not supported – In general, installations using the VLAN translation feature should rely on cutoff on failure and at upgrade (use redundant SCE platform).
- STP hazard – VLAN translation may interfere with Spanning Tree Protocol. This should be taken in consideration when deploying the solution.

Authorization: admin

Examples

The following example specifies a VLAN translation constant of 20 for the network port side.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#vlan translation increment value 20
SCE(config if)#
```

Related Commands

Command	Description
vlan	
show interface linecard vlan translation	

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.

```
SCE>enable 10
Password:<cisco>
SCE#config
SCE(config)#interface linecard 0
SCE(config if)#wap
SCE(config if)#
```

Related Commands

Command	Description
show interface linecard wap	

watchdog

Enables the linecard watchdog. Use the **no** form of the command to disable the linecard watchdog.

watchdog

no watchdog

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the linecard watchdog is enabled.

Command Modes

Interface Linecard Configuration

Usage Guidelines

The line card watchdog monitors the linecard traffic processor.

Authorization: root

Examples

The following example shows how to disable the linecard watchdog.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>interface linecard 0
SCE(config if)#>no watchdog
SCE(config if)#>
```

Related Commands

Command	Description
show interface linecard watchdog	
watchdog hardware-reset	
watchdog software-reset	

watchdog hardware-reset

Enables or disables the hardware watchdog reset.

watchdog hardware-reset enabled

watchdog hardware-reset disabled

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the hardware watchdog reset is enabled.

Command Modes

Global Configuration

Usage Guidelines

Specify the desired status for the hardware watchdog reset.

The hardware watchdog protects the system against situations in which the software watchdog reset may not be operational, such as:

- Total software crash
- Processor malfunction

Authorization: root

Examples

The following example illustrates how to disable the hardware watchdog reset.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>watchdog hardware-reset disabled
SCE(config)#>
```

Related Commands

Command	Description
show watchdog	
watchdog	
watchdog software-reset	

watchdog software-reset

Enables or disables the software watchdog reset.

watchdog software-reset enabled

watchdog software-reset disabled

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the software watchdog reset is enabled.

Command Modes

Global Configuration

Usage Guidelines

Specify the desired status for the software watchdog reset.

The software watchdog monitors the linecard and the management agent.

Authorization: root

Examples

The following example illustrates how to enable the software watchdog reset.

```
SCE>enable 15
Password:<cisco>
SCE#>configure
SCE(config)#>watchdog software-reset enabled
SCE(config)#>
```

Related Commands

Command	Description
show watchdog	
watchdog	
watchdog hardware-reset	