

Silver Peak

Command Line Interface Reference Guide

VXOA 8.0

September 2016

PN 200063-001 Rev O

Silver Peak Command Line Interface Reference Guide

PN 200063-001 Rev O

Date: September 2016

Copyright © 2016 Silver Peak Systems, Inc. All rights reserved. Information in this document is subject to change at any time. Use of this documentation is restricted as specified in the *End User License Agreement*. No part of this documentation can be reproduced, except as noted in the *End User License Agreement*, in whole or in part, without the written consent of Silver Peak Systems, Inc.

Trademark Notification

The following are trademarks of Silver Peak Systems, Inc.: Silver Peak Systems™, the Silver Peak logo, Network Memory™, Silver Peak NX-Series™, Silver Peak VX-Series™, Silver Peak VRX-Series™, Silver Peak Unity EdgeConnect™, and Silver Peak Orchestrator™. All trademark rights reserved. All other brand or product names are trademarks or registered trademarks of their respective companies or organizations.

Warranties and Disclaimers

THIS DOCUMENTATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. SILVER PEAK SYSTEMS, INC. ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THIS DOCUMENTATION OR OTHER DOCUMENTS WHICH ARE REFERENCED BY OR LINKED TO THIS DOCUMENTATION. REFERENCES TO CORPORATIONS, THEIR SERVICES AND PRODUCTS, ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. IN NO EVENT SHALL SILVER PEAK SYSTEMS, INC. BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENTATION. THIS DOCUMENTATION MAY INCLUDE TECHNICAL OR OTHER INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THE DOCUMENTATION. SILVER PEAK SYSTEMS, INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENTATION AT ANY TIME.

Silver Peak Systems, Inc.
2860 De La Cruz Blvd., Suite 100
Santa Clara, CA 95050

1.877.210.7325 (toll-free in USA)
+1.408.935.1850

http://www.silver-peak.com/support
support@silver-peak.com

Contents

Preface ix

Introduction ix
Audience ix
Structure of the Manual ix
Conventions Used in this Manual x
Typographical Conventions x
Syntax Notation x
Annotated Symbols x
Related Documents xi
Technical Support xi

Chapter 1 Using the Command-Line Interface 1

Understanding the CLI Structure 2
CLI Modes 2
User Privilege Levels 4
User Names 4
Passwords 5
Object Names 5
Understanding the Command Structure 5
Understanding the Command Syntax 5
Syntax Helper 6
Command History 6
Configuring DB-9 Console Access to the Appliance 7
Using the Command Line-Editing Keys 8

Chapter 2 Administration Commands 9

aaa authentication login default 10
aaa authorization map 11
arp 13
boot system 14
clear 15
cli 17
configuration 19
email 23
email send-test 25
excess-flow 26
file debug-dump 27
file job upload 29
file stats 30
file tcpdump 31
file upload cancel 32
help 33
image boot 34
image install 35
image upgrade 36
job 37
job execute 39
license 40
radius-server 41
reboot 43
reload 44
system disk 45

tacacs-server . . . 46
tca . . . 48
terminal . . . 51
username . . . 52
web . . . 54
write . . . 56

Chapter 3 Configuration Commands . . . 59

access-list . . . 60
active-flows . . . 64
application . . . 65
application-group . . . 67
banner login . . . 69
banner motd . . . 70
bridge . . . 71
cdp . . . 72
cifs signing delegation domain . . . 73
clock set . . . 74
clock timezone . . . 75
cluster . . . 77
configure terminal . . . 79
disable . . . 80
enable . . . 81
enable password . . . 82
exit . . . 83
flow-export . . . 84
flow-redirection . . . 86
hostname . . . 87
iflabel . . . 88
interface cdp . . . 89
interface dhcp . . . 90
interface harden . . . 91
interface inbound-max-bw . . . 92
interface ip address . . . 93
interface label . . . 94
interface lan-if . . . 95
interface mac address . . . 96
interface mtu . . . 97
interface outbound-max-bw . . . 98
interface pass-through . . . 99
interface shutdown . . . 100
interface speed-duplex . . . 101
interface tunnel admin . . . 102
interface tunnel alias . . . 103
interface tunnel bind-tunnel . . . 104
interface tunnel control-packet . . . 105
interface tunnel create . . . 107
interface tunnel gre-protocol . . . 109
interface tunnel ipsec . . . 110
interface tunnel max-bandwidth . . . 112
interface tunnel min-bandwidth . . . 113
interface tunnel mode . . . 115
interface tunnel mtu . . . 117
interface tunnel packet . . . 118
interface tunnel revert . . . 120
interface tunnel tag-name . . . 121
interface tunnel threshold . . . 122
interface tunnel udp-flow . . . 124
interface tunnel udp-port . . . 125
interface vrrp . . . 126

interface wan-if . . . 129
ip datapath route . . . 130
ip default-gateway . . . 132
ip domain-list . . . 133
ip host . . . 134
ip mgmt-ip . . . 135
ip name-server . . . 136
ip route . . . 137
nat-map . . . 139
nat-map match . . . 142
nat-map set . . . 144
nat-map activate . . . 146
nat-map comment . . . 147
no nat-map . . . 148
nat-map modify-priority . . . 150
ntp . . . 151
ntpdate . . . 153
opt-map . . . 154
opt-map match . . . 156
opt-map set . . . 161
opt-map activate . . . 164
opt-map comment . . . 165
no opt-map . . . 166
opt-map modify-priority . . . 167
preposition ftp . . . 168
qos-map . . . 169
qos-map match . . . 171
qos-map set . . . 176
qos-map activate . . . 178
qos-map comment . . . 179
no qos-map . . . 180
qos-map modify-priority . . . 181
route-map . . . 182
route-map match . . . 184
route-map set . . . 189
route-map activate . . . 192
route-map comment . . . 193
no route-map . . . 194
route-map modify-priority . . . 195
saas . . . 196
shaper inbound . . . 197
shaper outbound . . . 199
snmp-server . . . 201
snmp-server user v3 . . . 204
ssl auth-certificate . . . 206
ssl builtin-signing . . . 208
ssl cert-substitution . . . 209
ssl host-certificate . . . 210
ssl signing-certificate . . . 212
ssl subs-certificate . . . 214
subnet . . . 216
subnet ipv6 . . . 218
system 10gigabit . . . 220
system arp-table-size . . . 221
system auto-ipid . . . 222
system auto-subnet . . . 223
system auto-syn . . . 224
system auto-tunnel . . . 225
system auto-tunnel allow . . . 226
system bandwidth . . . 227
system bonding . . . 228

system bypass . . . 229
system contact . . . 231
system disk . . . 232
system dpc . . . 233
system hostname . . . 234
system igmp-snooping . . . 235
system int-hairpin . . . 236
system location . . . 237
system mode . . . 238
system nat-all-inbound . . . 240
system nat-all-outbound . . . 241
system network-memory . . . 242
system registration . . . 243
system router . . . 244
system routing . . . 246
system smb-signing . . . 247
system ssl-ipsec-override . . . 248
traffic-class . . . 249
wccp . . . 250

Chapter 4 Monitoring Commands . . . 253

monitor . . . 254
show aaa . . . 255
show access-list . . . 256
show alarms . . . 257
show application . . . 259
show application-builtin . . . 261
show application-group . . . 262
show arp . . . 264
show banner . . . 265
show bootvar . . . 266
show bridge . . . 267
show cdp . . . 269
show cifs signing delegation . . . 271
show cli . . . 272
show clock . . . 273
show cluster . . . 274
show configuration . . . 275
show email . . . 277
show excess-flow . . . 278
show files . . . 279
show flow-debug . . . 281
show flow-export . . . 282
show flow-redirection . . . 283
show hosts . . . 284
show iflabels . . . 285
show image . . . 286
show interfaces . . . 287
show interfaces cdp . . . 289
show interfaces pass-through . . . 291
show interfaces tunnel . . . 294
show interfaces vrrp . . . 297
show ip . . . 298
show jobs . . . 299
show licenses . . . 300
show log . . . 301
show log audit . . . 304
show log-files . . . 306
show log-list matching . . . 308
show logging . . . 309

show memory . . . 312
show nat statistics . . . 313
show nat-map . . . 314
show ntp . . . 316
show opt-map . . . 317
show overlay . . . 321
show pass-through . . . 323
show preposition . . . 325
show qos-map . . . 326
show radius . . . 329
show route-map . . . 330
show running-config . . . 333
show selftest . . . 334
show shaper . . . 336
show snmp . . . 338
show ssh . . . 340
show ssl . . . 341
show stats tunnel . . . 342
show subif . . . 344
show subnet . . . 345
show system . . . 347
show tacacs . . . 350
show tca . . . 351
show tech-support . . . 353
show terminal . . . 354
show tunnel . . . 355
show usernames . . . 358
show users . . . 359
show version . . . 360
show vlan . . . 362
show vrrp . . . 363
show wccp . . . 364
show web . . . 367
show whoami . . . 368

Chapter 5 Alarm Commands . . . 369

alarms . . . 370
logging . . . 371
logging facility . . . 373
logging files . . . 374
logging local . . . 376
logging trap . . . 378

Chapter 6 Troubleshooting Commands . . . 381

debug generate dump . . . 382
flow-debug . . . 383
hping2 . . . 385
mtr . . . 389
ping . . . 392
selftest . . . 395
slogin . . . 396
ssh client global . . . 400
ssh client user . . . 402
ssh server . . . 404
tcpdump . . . 406
tcptraceroute . . . 411
tech-support create job . . . 414
telnet . . . 415
traceroute . . . 417

Index of Commands 421

Preface

Introduction

This manual provides details of the command syntax for the VXOA software.

This manual does not provide feature descriptions, or explanations of the technologies. For information about the various features and technologies supported by Silver Peak physical and virtual appliances, see the *Silver Peak Appliance Manager Operator's Guide*.

Audience

This manual is intended for use by network administrators who are responsible for installing and setting up network equipment for Silver Peak NX Series appliances such as NX-10700, NX-5500, or NX-1700. The same commands apply to the VX and VRX Series of virtual appliances, which work with various hypervisors. This document assumes a basic working knowledge of Local Area Networks (LANs) and of Ethernet concepts.

Structure of the Manual

This manual documents all the commands of the operating system and their related commands based on their functionality. Within each chapter, commands appear in alphabetical order.

This section outlines the chapters and summarizes their content.

Chapter 1, "Using the Command-Line Interface," describes how to access the appliance and information about different command modes.

Chapter 2, "Administration Commands," describes all the commands that help you carry out the tasks of an administrator on the appliances.

Chapter 3, "Configuration Commands," describes the commands that help you configure the appliance with different features and functions.

Chapter 4, "Monitoring Commands," describes the commands that help you monitor the traffic on the appliance.

Chapter 5, "Alarm Commands," describes the commands that display the alarms and event logging information.

Chapter 6, "Troubleshooting Commands," describes the commands that help you troubleshoot the appliance and the network.

Conventions Used in this Manual

The following topics are discussed in this section:

- **Typographical Conventions** See page x.
- **Syntax Notation** See page x.
- **Annotated Symbols** See page x.

Typographical Conventions

The following typographical conventions are used in this manual:

- Words in *italics* emphasize a point or introduce a new term.
- `Courier` font is used for screen displays.
- The commands that you need to type exactly as shown in the screen display are in **`courier bold`**.
- *Italicized* words in the screen display indicate a variable in the command syntax that you need to replace with a value.

Syntax Notation

This manual uses these conventions to describe commands:

- Commands and keywords are in **bold** text.
- Arguments for which you supply values are in *italics*.
- Keyboard buttons are in **bold sans serif** text (**Enter**).
- Curly brackets ({}) contain required choices.
- Square brackets ([ ]) contain optional elements.
- Vertical bars (|) separate the alternative elements.
- Curly brackets and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.
- In examples, terminal sessions and system displays are in `courier` font.
- Nonprinting characters, such as passwords or tabs, and variables are in angled brackets (< >).



For more information and examples on syntax notation, see “Understanding the CLI Structure” on page 2.

Annotated Symbols

The following annotated symbols may be used in this manual:



Note The information that follows this symbol contains helpful suggestions or references to information not contained in the document.



CAUTION The information after this symbol contains tips to be careful while using the software or hardware, or it may lead to damaging the equipment or losing data.

Related Documents

- Release Notes provide information on new software features, system bugs, and software compatibility.
- All user documentation is available for download from http://www.silver-peak.com.

Technical Support

For product and technical support, contact Silver Peak Systems at any of the following:

- **1.877.210.7325 (toll-free in USA)**
- **+1.408.935.1850**
- **www.silver-peak.com**
- **support@silver-peak.com**

We're dedicated to continually improving the usability of our products and documentation. If you have suggestions or feedback for our documentation, please send an e-mail to **techpubs@silver-peak.com**.

For usability suggestions, questions, or issues, please send an e-mail to **usability@silver-peak.com**.

CHAPTER 1

Using the Command-Line Interface

This chapter discusses the following topics:

- **Understanding the CLI Structure** See page 2.
- **Configuring DB-9 Console Access to the Appliance** See page 7.
- **Using the Command Line-Editing Keys** See page 8.

Understanding the CLI Structure

This section describes the following topics:

- **CLI Modes** See page 2.
- **User Privilege Levels** See page 4.
- **Passwords** See page 5.
- **Understanding the Command Structure** See page 5.
- **Understanding the Command Syntax** See page 5.
- **Syntax Helper** See page 6.
- **Command History** See page 6.

CLI Modes

This section describes the following three command modes that the CLI uses for the Silver Peak NX Series appliances:

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode

Being in a particular command mode determines which commands you may execute. To display a list of the command that are available to you, enter that command mode and type **?**.

User EXEC Mode

When you first log in to a Silver Peak appliance, you are in the User EXEC mode. The User EXEC mode provides access to commands for non-configuration tasks, such as checking the appliance status. When you are in this mode, the following prompt displays:

```
<appliance> >
```

where *appliance* is the name of the appliance on which you logged in.

In the User EXEC mode, you have access to the following commands:

cli	Configure CLI shell options
enable	Enter enable mode
exit	Log out of the CLI
no	Negate or clear certain configuration options
ping	Send ICMP echo requests to a specified host
show	Display system configuration or statistics
slogin	Log into another system securely using ssh
telnet	Log into another system using telnet
terminal	Set terminal parameters
traceroute	Trace the route packets take to a destination
wccp	Configure WCCP

Privileged EXEC Mode

The Privileged EXEC mode provides access to all the commands you could execute in User EXEC mode, as well as several additional commands. Also, from this mode, you can enter Global Configuration mode. Most of the commands that the Privileged EXEC mode makes available are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces.

To enter the Privileged EXEC mode, type **enable** to log in as privileged user, which displays the following prompt:

```
<appliance> #
```

where *appliance* is the name of the appliance on which you logged in.

In the Privileged EXEC mode, you access to the following commands:

clear	Reset certain statistics or clear caches
cli	Configure CLI shell options
configure	Enter configuration mode
debug	Debugging commands
disable	Leave enable mode
email	Configure e-mail and event notification via e-mail
exit	Log out of the CLI
file	Manipulate files on disk
image	Manipulate system software images
job	Configure scheduled jobs
logging	Configure event logging
no	Negate or clear certain configuration options
ntpdate	Set system clock once from a remote server using NTP
ping	Send ICMP echo requests to a specified host
reboot	Reboot or shut down the system
show	Display system configuration or statistics
slogin	Log into another system securely using ssh
system	Configure system level information
tcpdump	Display packets on a network
telnet	Log into another system using telnet
terminal	Set terminal parameters
traceroute	Trace the route packets take to a destination
write	Save the running configuration to persistent storage

Global Configuration Mode

The Global Configuration mode allows you to make changes to the running configuration. If you later save the configuration, these commands are stored across appliance reboots. To enter the Global Configuration mode, you must first enter the Privileged EXEC mode and then type **configure terminal** at the prompt. When you press **Enter**, the following prompt displays:

```
<appliance> (config) #
```

where *appliance* is the name of the appliance on which you logged in.

The Global Configuration mode provides access to all CLI commands, including those available to the User EXEC and Privileged EXEC modes.

You must have an Administrator user privilege level to access the Global Configuration mode.

To leave Global Configuration mode, you can use the command:

```
<appliance> (config) # no configure
```

User Privilege Levels

The CLI has two user privilege levels, which determine the CLI modes you may enter and the commands you can execute. You can log in to one of the following user privilege levels:

- Administrator
- Monitor

To execute a CLI command at the prompt, you must be logged in at the required user privilege level for that command. For example, most configuration commands require you to have the Administrator privilege level.

Monitor

The Monitor user privilege level is the default privilege level for the CLI. This privilege level provides access to the both the User EXEC and Privileged EXEC modes. The Monitor user privilege level does not have access to most configuration commands.



Note You cannot delete user IDs in the CLI; you can only change the password for a user.

Administrator

The Administrator user privilege level has full access to all modes and commands in the CLI.

User Names

When you create a user name, ensure that the first character of the name is alphebetical (a-z or A-Z). The remaining characters must include one of the following:

- alphabetical (upper or lower case)
- numerical
- dash (-)
- underscore (_)
- dot (.)

No spaces are allowed.

Passwords

You can establish passwords for a user to enter the Privilege EXEC or Global Configuration modes. The CLI provides no restrictions on the password you create for a user. You may enter a clear-text password or use a utility to create an encrypted password for a user. There are also no restrictions on the use of, or requirement for, special characters in the password.

Object Names

When you create a name for an object, such as a tunnel, access control list, or a route map, you can use one of the following characters:

- alphabetical (upper or lower case)
- numerical
- dash (-)
- underscore (_)
- dot (.)

Understanding the Command Structure

The following information is provided for each command:

Description	A brief summary of what the command does
Syntax	The actual syntax of the command, including the arguments.
Arguments	The definition of any keywords and options used in the command.
Command Mode	The type of mode the command uses.
Default	The defaults, if any, for this command. The default can be the default action of the command if optional arguments are not provided, or it can be the default state of the switch (such as for an enable/disable command).
Example	Examples of the command usage, including output, if relevant.
See Also	Provides cross references to related commands.
Usage Guidelines	Contains any additional information.



Note The Silver Peak command line interface (CLI) supports only the US character set.

Understanding the Command Syntax

The following symbols are used in the CLI documentation to describe the command syntax. When you execute commands in the CLI, do not type these characters:

Angled brackets	< >	Enclose a variable or a value that you must specify in the command. For example, in the syntax: **configure vlan <***vlan name***> ip address <***ip_address***>**, you must supply a VLAN name for the variable <*vlan name*> and an IP address for the variable <*ip_address*> when you enter the command.
Vertical bars	|	Separate mutually exclusive items in a list, one of which must be entered. For example, in the syntax **file upload** <*filename*> | **cancel** you must specify either the file name variable or the word, **cancel**, when you enter the command.

Curly brackets	**{ }**	Enclose a required value or list of required arguments. One or more values or arguments can be specified in square brackets. For example, in the syntax **configure snmp community {read-only | read-write}** <*string*>**,** you must include either the *read-only* or *read-write* argument in the command.
Square brackets	**[ ]**	Enclose an optional value or a list of optional arguments. You can specify in curly brackets one or more values or arguments that are not required to execute the command. For example, in the syntax **reboot [<date> <time> | cancel]** you can choose to use the reboot command without any arguments. Alternately, you can specify either a particular date and time combination or the keyword **cancel** to cancel a previously scheduled reboot.

Syntax Helper

The CLI has a built-in Syntax Helper. If you are not sure of the complete syntax for a particular command, enter the first three letters of the command and press the **Tab** key. The Syntax Helper provides a list of options for the remainder of the command, and places the cursor at the end of the command you have entered so far, ready for the next option.

The Syntax Helper also provides assistance by informing you if you have entered an incorrect command.

Command History

The Silver Peak operating system keeps the last commands you entered in its memory. You can "walk" through these commands one at a time by using the **Up** and **Down** arrows on your keyboard.

Configuring DB-9 Console Access to the Appliance

For console port access, the appropriate settings are as follows:

Bits per second	9600
Data bits	8
Parity	none
Stop bits	1
Flow control	none

Using the Command Line-Editing Keys

These line-editing keys are available when you are using the CLI:

Key	Description
Backspace	This key deletes character to left of cursor and shifts remainder of line to left.
Delete or [**Ctrl**] + **D**	Deletes character under cursor and shifts remainder of line to left.
[**Ctrl**] + **K**	Deletes characters from under cursor to end of line.
Insert	Toggles between on and off. When on, inserts text and shifts previous text to right.
Left Arrow	Moves cursor to left.
Right Arrow	Moves cursor to right.
Home or [**Ctrl**] + **A**	Moves cursor to first character in line.
End or [**Ctrl**] + **E**	Moves cursor to last character in line.
[**Ctrl**] + **L**	Clears screen and movers cursor to beginning of line.
[**Ctrl**] + **P** or **Up Arrow**	Displays previous command in command history buffer and places cursor at end of command.
[**Ctrl**] + **N** or **Down Arrow**	Displays next command in command history buffer and places cursor at end of command.
[**Ctrl**] + **U**	Clears all characters typed from cursor to beginning of line.
[**Ctrl**] + **W**	Deletes previous word.

When you choose to display output in multiple pages, the CLI has additional “editor” keys available:

Key	Description
1 + [Shift] + g	Moves to the top of the screen display.
1 + g	Moves to the bottom of the screen display.
/**textstring**	Searches forward for the textstring you enter.
?textstring	Searches backward for the textstring you enter.
Spacebar	Moves forward a page.
[Enter]	Moves forward one line.
q	Quits out of what it was doing and returns you to the command prompt.

CHAPTER 2

Administration Commands

This chapter describes the commands that allow you to carry out the administrator's tasks for the Silver Peak appliances.

aaa authentication login default

Description

Use the **aaa authentication login default** command to configure the order in which authentication methods are tried. ***Authentication*** is the process of validating that the end user, or device, is who they claim to be. Generally, authentication precedes authorization.

Use the **no** form of this command to clear all authentication login settings.

Syntax

aaa authentication login default {*<method>* | *<method>* *<method>* | *<method>* *<method>* *<method>*}

no aaa authentication login

Arguments

<method>	Specifies the methods for authenticating the default login in the order that they will be used. The method options are: • **local** • **radius** • **tacacs+**

Defaults

No default behavior or values.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “aaa authorization map” on page 11
- “show aaa” on page 255

Usage Guidelines

You can use up to three methods (or databases) for authentication, place the methods in any order, and/or use any method more than once.

However, one of the methods that you include must be **local**.

Examples

To set the authentication login methods to be local and TACACS+, in that order:

```
(config) # aaa authentication login default local tacacs+
```

aaa authorization map

Description

Use the **aaa authorization map default-user** command to configure authorization mapping settings. ***Authorization*** is the action of determining what a user is allowed to do. Generally, authentication precedes authorization.

Syntax

aaa authorization map default-user <*user*>
no aaa authorization map default-user

aaa authorization map order <*policy*>
no aaa authorization map order

Arguments

default-user <user>	Specifies the user ID of a valid local user. Generally, this is **admin** or **monitor**.
map default-user <*user*>	Sets the local user default mapping. Use the **no** form of this command to clear the local user default mapping.
map order <*policy*>	Specifies in what order to handle remote-to-local user mapping. The available policies are: • **remote-only** Only honor user mapping from remote authentication server. • **remote-first** Honor user mapping from remote auth server, if provided; otherwise use local mapping. • **local-first** Ignore user mapping from remote auth server; use local mapping only. Use the **no** form of the command to clear the authorization user mapping order policy.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “aaa authentication login default” on page 10
- “show aaa” on page 255

Usage Guidelines

When you enter a user name, the system verifies in the database that the user ID is valid.

Examples

To set authorization mapping to check the remote database first:

```
(config) # aaa authorization map order remote-first
```

arp

Description

Use the **arp** command to add static entries to the Address Resolution Protocol (ARP) cache.

Use the **no** form of this command to remove a static entry from the ARP cache.

Syntax

arp <*ip address*> <*MAC address*>

no arp <*ip address*>

Arguments

<*ip address*>	Specifies an IP address.
<*MAC address*>	Defines the 48-bit MAC address that the IP address to which the IP address will be mapped.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show arp” on page 264
- “clear” on page 15

Usage Guidelines

None.

Examples

To create an entry in the ARP table for a machine with the IP address 10.10.1.1 and MAC address 00107654bd33:

```
(config) # arp 10.10.1.1 00107654bd33
```

boot system

Description

Use the **boot system** command to specify which partition to boot from next time.

Syntax

boot system {**1** | **2** | **next**}

Arguments

1	Sets the next boot partition to 1.
2	Sets the next boot partition to 2.
next	Sets the next boot partition to the partition that isn't running now.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- "show bootvar" on page 266
- "image boot" on page 34
- "reboot" on page 43
- "reload" on page 44

Usage Guidelines

None.

Examples

To set the appliance to start using partition 2, by default, beginning at the next system boot:

```
(config) # boot system 2
```

To boot from the other partition at the next system boot:

```
(config) # boot system next
```

clear

Description

Use the **clear** command to clear entries and/or counters.

Syntax

clear arp-cache

clear bridge counters

clear bridge mac-address-table

clear cdp counters

clear cdp table

clear cluster spcp

clear flow-redirection

Arguments

arp-cache	Clears dynamic entries from the ARP cache.
bridge counters	Clears the bridge counters.
bridge mac-address-table	Flushes the bridge MAC address table.
cdp counters	Clears the Cisco Discovery Protocol counters
cdp table	Clears the Cisco Discovery Protocol table
cluster spcp	Clears the cluster's Silver Peak Communication Protocol counters. These are used when doing flow redirection.
flow-redirection	Clears the flow redirection counters.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None

Usage Guidelines

None.

Examples

None.

cli

Description

Use the **cli** command to configure CLI shell options.

Syntax

cli clear-history

cli default allow-all-show {enable | disable}

cli default auto-logout <*number of minutes*>
no cli default auto-logout

cli session auto-logout <*number of minutes*>
no cli session auto-logout

cli session paging enable
no cli session paging enable

cli session terminal length <*number of lines*>

cli session terminal type {xterm | ansi | vt100}
no cli session terminal type

cli session terminal width <*number of characters*>

Arguments

clear-history	Clears the current user's command history.
default allow-all-show {enable | disable}	When enabled, allows the user to view all possible show commands. When disabled, the commands a user can see are based on privilege level.
default auto-logout <*number of minutes*>	Configures—for all ***future*** sessions—the amount of time for keyboard inactivity before automatically logging out a user. The default auto-logout setting is 15 minutes. Use the **no** form of this command to prevent users from being automatically logged out because of keyboard inactivity.
session auto-logout <*number of minutes*>	Configures—***for this session only***—how long the keyboard can be inactive before automatically logging out a user. Use the **no** form of this command to prevent users from being automatically logged out because of keyboard inactivity.
session paging enable	Configures—***for this session only***—the ability to view text one screen at a time. Paging is enabled, by default. Use the **no** form of this command to prevent parsing of text into individual, sequential screens.
session terminal length <*number of lines*>	Sets—***for this session only***—the number of lines of text for this terminal. The default terminal length is 24 rows.

session terminal type {xterm | ansi | vt100}	Sets—***for this session only***—the terminal type: • **xterm** – Sets terminal type to xterm. • **ansi** – Sets terminal type to ANSI. • **vt100** – Sets terminal type to VT100. The default type is **xterm**. Use the **no** form of the command to clear the terminal type.
session terminal width <*number of characters*>	Sets—***for this session only***—the maximum number of characters in a line.

Defaults

- The default auto-logout setting is 15 minutes.
- Paging is enabled, by default.
- The default terminal length is 24 rows.
- The default terminal type is *xterm*.
- The default number of characters per line is 80.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “show cli” on page 272.

Usage Guidelines

None.

Examples

To set 1.5 hours as the maximum time a session will last without keyboard activity, for this session only:

```
(config) # cli session auto-logout 75
```

To set the number of lines of text per page to 30 rows:

```
(config) # cli session terminal length 30
```

configuration

Description

Use the **configuration** command to manipulate configuration files.

Syntax

configuration copy <*filename*> <*filename*>

configuration delete <*filename*>

configuration download <*URL or scp://username:password@hostname/path/filename*> **[**<*filename*>**]**

configuration download cancel

configuration factory <*filename*>

configuration merge <*filename*>

configuration move <*filename***> <***filename***>**

configuration new <*filename*>

configuration reboot-next <*filename*>

configuration revert saved

configuration upload {**active** | <*filename*>} <*URL or scp://username:password@hostname/path/filename*>

configuration upload cancel

configuration write

configuration write to <*filename*>

Arguments

copy < *filename*> <*filename*>	Makes a copy of a configuration file. Specify, in order, the names of the existing source file and the new destination (configuration) file.
delete <*filename*>	Deletes the named configuration file. The filename you specify must be one of the configuration files listed on the appliance.
download {<*URL or scp://username:password@hostname/path/filename*>} [<*new filename*>]	Downloads a configuration file from a remote host. Optionally, you can rename the downloading file.
download cancel	Cancels a configuration file download.
factory <*filename*>	Creates a new configuration file.

merge <*filename*>	Merges settings from the specified configuration file to the currently active configuration file.
move <*filename*> **<***filename*>	Renames a configuration file. First enter the current file name, followed by the new file name.
new <*filename*>	Creates a new configuration file with all defaults plus active licenses.
reboot-next <*filename*>	Loads the named configuration file at the next reboot.
revert saved	Reverts to the last saved configuration.
upload <*filename*> <*URL or scp://username:password@hostname/path/filename*>	Uploads an existing, inactive configuration file to a remote host, as specified by a URL or an SCP path.
upload active <*URL or scp://username:password@hostname/path/filename*>	Uploads the currently active configuration file to a remote host, as specified by a URL or an SCP path.
upload cancel	Cancels the configuration file upload.
write	Saves the running configuration to the active configuration file (same as the *write memory*).
write to <*filename*>	Saves the running configuration to an inactive file and makes that copy the active file.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show configuration” on page 275.

Usage Guidelines

To display a list of available files, enter one of the following commands, depending on what argument you're using:

```
<silver-peak> (config) # configuration copy ?
<silver-peak> (config) # configuration delete ?
<silver-peak> (config) # configuration merge ?
<silver-peak> (config) # configuration move ?
<silver-peak> (config) # configuration reboot-next ?
<silver-peak> (config) # configuration upload ?
```

Examples

To make a copy of the configuration file, "Texas", and rename it "Texarkana" (three possible ways):

- `(config) # configuration copy Texas Texarkana`
- `(config) # config copy Texas Texarkana`
- `(config) # co copy Texas Texarkana`

To create a new, clean configuration file named, "wholesale":

```
(config) # config new wholesale
```

To merge the setting from the inactive configuration file, "lanes", with the currently active configuration file:

```
(config) # config merge lanes
```

To download the configuration file, "horsemen" from the URL, www.apocalypse.com/four/, and keep the original file name:

```
(config) # configuration download www.apocalyse.com/four/horsemen
```

To upload the configuration file, "initial.bak" to an account at the remote SCP host, "ocean", and rename the file to "coyotes.bak":

```
(config) # configuration upload initial.bak
scp://root:seminole@ocean/tmp/coyotes.bk
```

To upload the configuration file, "initial.bak" to an account at the remote SCP host, 10.0.55.28, and rename the file to "coyotes.bak" at the destination:

```
(config) # configuration upload initial.bak
scp://root:seminole@10.0.55.28/tmp/coyotes.bk
```

To rename the local configuration file, "laurel" to "andhardy":

```
(config) # configuration move laurel andhardy
```

To load the configuration file, “wolves”, at the next reboot:

```
(config) # configuration reboot-next wolves
```

To save the running configuration as a new file named, “newDeployment”, and make it the active configuration:

```
(config) # configuration write to newDeployment
```

email

Description

Use the **email** command to configure e-mail, and also event notification via e-mail.

Syntax

email autosupport enable
no email autosupport enable

email domain <*hostname or ip address*>
no email domain

email mailhub <*hostname or ip address*>
no email mailhub

email mailhub-port <*port number*>
no email mailhub-port

email notify event raise-alarm
no email notify event raise-alarm

email notify recipient <*email addr*> **class** {**failure** | **info**}
no email notify recipient <*email addr*> **class** {**failure** | **info**}

email notify recipient <*email addr*> **detail**
no email notify recipient <*email addr*> **detail**

Arguments

autosupport enable	Determines the handling of automatic support e-mail. Use the **no** form of this command to prevent the sending of automatic support notifications by e-mail.
domain <*hostname or ip address*>	Overrides the domain from which e-mail appears to come. Specify the hostname or IP address of the domain, for the “return address” you want users to see. Use the **no** form of this command to clear the e-mail domain override.
mailhub <*hostname or ip address*>	Specifies the mail relay to use to send e-mails. Use the **no** form of this command to clear the configured mailhub.
mailhub-port <*port number*>	Specifies the mail port to use for sending e-mails. Use the **no** form of this command to clear the configured mail port.
notify event raise-alarm	Sends an e-mail whenever a system alarm is raised. Use the **no** form of this command to stop sending e-mails when alarms are triggered.

notify recipient <*email addr*> **class** {**failure** | **info**}	Specifies which types of events are sent to a specific recipient: • **failure** – Sends failure events to the specified recipient • **info** – Sends informational events to the specified recipient Use the **no** form of this command to specify which events this recipient should ***not*** be sent.
notify recipient <*email addr*> **detail**	Sends detailed event e-mails to a specific recipient. Use the **no** form of this command to to send summarized (rather than detailed) event e-mails to a specific recipient.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “email send-test” on page 25
- “show email” on page 277

Usage Guidelines

None.

Examples

To set the outgoing e-mail relay to “canary-post”:

```
(config) # email mailhub canary-post
```

To notify all members of the mailgroup, engineering@silver-peak.com, whenever there’s a failure event:

```
(config) # email notify recipient engineering@silver-peak.com class failure
```

email send-test

Description

Use the **email send-test** command to send a test email to all configured event and failure recipients.

Syntax

email send-test

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “email” on page 23
- “show email” on page 277

Usage Guidelines

None.

Examples

None.

excess-flow

Description

Use the **excess-flow** command to manage flows that exceed the number of flows that an appliance supports.

Syntax

excess-flow bypass

excess-flow bypass dscp-marking {enable | disable}

excess-flow drop

Arguments

bypass	Bypasses excess flow traffic
dscp-marking enable	Enables excess flow DSCP markings.
dscp-marking disable	Disables excess flow DSCP markings.
drop	Drops excess flow traffic

Defaults

None.

Command Mode

Global Configuration Mode

See Also

- “show excess-flow” on page 278

Usage Guidelines

None.

Examples

None.

file debug-dump

Description

Use the **file debug-dump** command to manipulate debug dump files.

Syntax

file debug-dump delete <*filename*>

file debug-dump email <*filename*>

file debug-dump upload <*filename*> <*URL or scp://username:password@hostname/path/filename*>

Arguments

delete <*filename*>	Deletes an existing debug dump file. You can only delete one file at a time.
email <*filename*>	E-mails a debug dump file to preconfigured recipients. You can only e-mail one file at a time.
upload <*filename*>	Uploads a debug dump file to a remote host. You can only upload one file at a time.
<*URL or scp://username:password@ hostname/path/filename*>	Specifies the path to a remote host. Optionally, you can enter a new destination filename.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “email” on page 23
- “show files” on page 279.

Usage Guidelines

- To display a list of existing debug files, enter one of the following command, depending on what argument you’re using:

```
<silver-peak> (config) # file debug-dump delete ?
<silver-peak> (config) # file debug-dump email ?
<silver-peak> (config) # file debug-dump upload ?
```

- To pre-configure recipients to receive debug files by e-mail, use the **email mailhub** command.

Examples

To upload the debug dump file, “sysdump-localhost-20070206-025124.tgz” to an account at the remote SCP host, “ocean”, and rename the file to “sysdump-chicago-20070206-025124.tgz”:

```
(config) # file debug-dump upload sysdump-localhost-20070206-025124.tgz
scp://root:seminole@ocean/tmp/sysdump-chicago-20070206-025124
```

To upload the debug dump file, “gotitall” to the URL, www.catchall.com/tmp/, and keep the original file name:

```
(config) # file debug-dump upload gotitall www.catchall.com/tmp/
```

file job upload

Description

Use the **file job upload** command to upload a job output file to a remote host.

Syntax

file job upload *<job ID> <URL or scp://username:password@hostname/path/filename>*

file job upload cancel

Arguments

<job ID>	Specifies which job output file to upload to a remote host.
<URL or scp://username:password@hostname/path/filename>	Determines the path for a remote host. Optionally, you can specify a new destination filename.
cancel	Cancels the current asynchronous file upload.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “file stats” on page 30
- “show files” on page 279

Usage Guidelines

None.

Examples

None.

file stats

Description

Use the **file stats** command to manipulate statistics report files.

Syntax

file stats upload *<filename> <URL or scp://username:password@hostname/path/filename>*

Arguments

upload *<filename> <URL or scp://username:password@hostname/path/filename>*	Uploads the specified statistics report file to a remote host. Optionally, you can enter a new destination filename.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “show files” on page 279.

Usage Guidelines

None.

Examples

None.

file tcpdump

Description

Use the **file tcpdump** command to manipulate tcpdump output files.

Syntax

file tcpdump delete <*filename*>

file tcpdump upload <*filename*> <*URL or scp://username:password@hostname/path/filename*>

Arguments

delete <*filename*>	Deletes the specified tcpdump output file.
upload <*filename*> <*URL or scp://username:password@hostname/path/filename*>	Uploads the specified statistics report file to a remote host. Optionally, you can specify a new destination filename.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “show files” on page 279.

Usage Guidelines

None.

Examples

None.

file upload cancel

Description

Use the **file upload cancel** command cancels the current asynchronous file upload.

Syntax

file upload cancel

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “file job upload” on page 29
- “show files” on page 279

Usage Guidelines

None.

Examples

None.

help

Description

Use the **help** command to view a description of the interactive help system.

Syntax

help

Arguments

None.

Defaults

None.

Command Mode

User EXEC mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn2 (config) # help
You may request context-sensitive help at any time by pressing '?'
on the command line.  This will show a list of choices for the
word you are on, or a list of top-level commands if you have not
typed anything yet.

If "<cr>" is shown, that means that what you have entered so far
is a complete command, and you may press Enter (carriage return)
to execute it.

Try the following to get started:
  ?
  show ?
  show c?
  show clock?
  show clock ?
  show interfaces ?     (from enable mode)
Tallinn2 (config) #
```

image boot

Description

Use the **image boot** command to specify which system image to boot by default.

Syntax

image boot {**1** | **2** | **next**}

Arguments

1	Sets the next boot partition to 1.
2	Sets the next boot partition to 2.
next	At the next system boot, boots from the partition that isn't running now.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- "boot system" on page 14
- "image install" on page 35
- "reboot" on page 43
- "show image" on page 286
- "show bootvar" on page 266

Usage Guidelines

None.

Examples

None.

image install

Description

Use the **image install** command to download and install an image file onto the inactive system partition.

Syntax

image install *<URL or scp://username:password@hostname/path/filename>*

image install cancel

Arguments

<URL or scp://username:password@hostname/path/filename>	Enter the path for the remote host from which to download and install the image file. You can specify the SCP server by IP address or hostname.
install cancel	Cancel the system upgrade.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “image boot” on page 34
- “image upgrade” on page 36
- “show image” on page 286
- “show bootvar” on page 266

Usage Guidelines

Software image files are .zip files.

Examples

To download the image file, “image-2.4.0.0_15984.zip”, from the remote SCP host, 10.0.55.28, to the inactive system partition:

```
(config) # image install
scp://root:seminole@10.0.55.28/tmp/image-2.4.0.0_15984.zip
```

image upgrade

Description

Use the **image upgrade** command to download, install, and reboot using a new image file.

Syntax

image upgrade *<URL or scp://username:password@hostname/path/filename>*

Arguments

<URL or scp://username:password@hostname/path/filename>	Enter the path for the remote host from which to download and install the image file. You can specify the SCP server by IP address or hostname.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “image boot” on page 34
- “image install” on page 35
- “show image” on page 286
- “show bootvar” on page 266

Usage Guidelines

Software image files are .zip files.

Examples

To download the image file, “image-2.4.0.0_45678.zip”, from the remote SCP host, 10.0.55.44, to the inactive system partition, install it, and reboot to using it:

```
(config) # image upgrade
scp://root:seminole@10.0.55.44/tmp/image-2.4.0.0_45678.zip
```

job

Description

Use the **job** command to configure scheduled jobs.

Syntax

job <*job ID*>
no job <*job ID*>

job <*job ID*> **command** <*sequence ID*> <*command string*>
no job <*job ID*> **command** <*sequence ID*>

job <*job ID*> **comment** <*comment string*>
no job <*job ID*> **comment**

job <*job ID*> **date-time** <*hr*>:<*mm*>:<*ss*> [<*yyyy*>/<*mm*>/<*dd*>]
no job <*job ID*> **date-time**

job <*job ID*> **enable**
no job <*job ID*> **enable**

job <*job ID*> **fail-continue**
no job <*job ID*> **fail-continue**

job <*job ID*> **name** <*friendly job-name*>
no job <*job ID*> **name**

Arguments

job <*job ID*>	Specifies the job number, which is a non-negative integer. If the job doesn't already exist, it creates it. Use the **no** form of this command to delete the job.
command <*sequence ID*> <*command string*>	Configures commands for the job. Since jobs may consist of multiple commands, you must assign each command a number that determines its order in the job. Use the **no** form of this command to remove commands from the job.
comment <*comment string*>	Adds a comment for the specified job. Use the **no** form of this command to remove the associated comment from the job.
date-time <*hr*>:<*mm*>:<*ss*> [<*yyyy*>/<*mm*>/<*dd*>]	Sets the time and date for executing the job, based on a 24-hour clock. If you don't set the date, the job executes at the first appropriate time. Use the **no** form of this command to clear the scheduled time for the job.
enable	Sets a job to the enabled state. A job must be enabled before you can execute it. Use the **no** form of this command to disable the job.

fail-continue	Sets the job to keep executing if a command fails. Use the **no** form of this command to stop job on the first command failure.
name <*friendly job-name*>	Sets the friendly name for this job. Use the **no** form of this command to remove the associated friendly name for this job.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “job execute” on page 39
- “show jobs” on page 299.

Usage Guidelines

If a <*command string*> or <*comment string*> includes spaces, enclose the entire string’s text in quotation marks.

Examples

To create the job, “overnight”, to install a new image file, “image-2.0.0.0_15984.zip”, from “www.company.com/images/” into the inactive system partition:

```
(config) # job overnight command 1 "image install
www.company.com/images/image-2.0.0.0_15984.zip"
```

job execute

Description

Use the **job execute** command to execute the job immediately (if the job has been enabled).

Syntax

job <*job ID*> **execute**

Arguments

job <*job ID*>	Specifies the name of the job.
execute	Immediately execute the job (if enabled).

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “job” on page 37
- “show jobs” on page 299

Usage Guidelines

You must enable a command before you can execute it. Refer to “job” on page 37.

Examples

None.

license

Description

Use the **license** command to install or remove a license key.

Syntax

license delete <*license number*>

license install <*license key*>
no license install

Arguments

delete <*license number*>	Removes a license key by ID number.
key <*license key*>	Installs a new license key. Use the **no** form of the command to remove license keys.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

radius-server

Description

Use the **radius-server** command to configure RADIUS server settings for user authentication.

Syntax

radius-server host <*IP address*> [**auth-port** <*port*>] [**key** <*string*>] [**retransmit** <*0..3*>] [**timeout** <*1..15*>]

radius-server {**key** <*string*> | **retransmit** <*0..3*> | **timeout** <*1..15*>}

no radius-server host <*IP address*> [**auth-port** <*port*>]

no radius-server {**key** | **retransmit** | **timeout**}

Arguments

host <*IP address*>	Configures host, at specified IP address, to send RADIUS authentication requests. Use the **no** form of this command to stop sending RADIUS authentication requests to host.
auth-port <*port*>	Specifies the authentication port to use with this RADIUS server. Use the **no** form of this command to stop sending RADIUS authentication requests to the authentication port.
key <*string*>	Specifies the shared secret key to use with this RADIUS server. Use the **no** form of this command to remove the global RADIUS server key.
retransmit <*0..3*>	Specifies the maximum number of retries that can be made in the attempt to connect to this RADIUS server. The range is 0 to 3. Use the **no** form of this command to reset the global RADIUS server retransmit count to its default.
timeout <*1..15*>	Specifies the number of seconds to wait before the connection times out with this RADIUS server, because of keyboard inactivity. The range is 1 to 15 seconds. Use the **no** form of this command to reset the global RADIUS server timeout setting to its default.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show radius” on page 329.

Usage Guidelines

None.

Examples

To define the RADIUS shared secret as “mysecret”:

```
(config) # radius-server key mysecret
```

To specify the RADIUS server’s IP address as 208.20.20.4 with authentication port 500 and a timeout of 10 seconds:

```
(config) # radius-server host 208.20.20.4 auth-port 500 timeout 10
```

To set the number of times the global RADIUS server retransmits to its default value:

```
(config) # no radius-server retransmit
```

reboot

Description

Use the **reboot** command to reboot or shutdown the system.

Syntax

reboot [**clean** | **force** | **halt** | **halt noconfirm** | **noconfirm**]

Arguments

reboot	Reboots the system.
clean	Reboots the system and cleans out the Network Memory.
force	Forces an immediate reboot of the system, even if it's busy.
halt	Shuts down the system.
halt noconfirm	Shuts down the system without asking about unsaved changes.
noconfirm	Reboots the system without asking about unsaved changes.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- "reboot" on page 43
- "boot system" on page 14

Usage Guidelines

None.

Examples

None.

reload

Description

Use the **reload** command to reboot or shutdown the system.

Syntax

reload [**clean** | **force** | **halt** | **halt noconfirm** | **noconfirm**]

Arguments

reload	Reboots the system.
clean	Reboots the system and cleans out the Network Memory.
force	Forces an immediate reboot of the system, even if it's busy.
halt	Shuts down the system.
halt noconfirm	Shuts down the system without asking about unsaved changes.
noconfirm	Reboots the system without asking about unsaved changes.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- "boot system" on page 14
- "reload" on page 44

Usage Guidelines

None.

Examples

None.

system disk

Description

Use the **system disk** command to insert or remove a disk from the RAID array.

Syntax

system disk <*disk ID*> {**insert | remove**}

Arguments

<*disk ID*>	Designates the host name for the appliance.
insert	Insert disk into RAID array.
remove	Remove disk from RAID array.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “system disk” on page 232
- “show system” on page 347

Usage Guidelines

None.

Examples

To add disk 9 back into an NX-8500’s RAID array:

```
(config) # system disk 9 insert
```

tacacs-server

Description

Use the **tacacs-server** command to configure hosts TACACS+ server settings for user authentication.

Syntax

tacacs-server host <*IP address*> [**auth-port** <*port*>] [**auth-type** {**ascii** | **pap**}] [**key** <*string*>] [**retransmit** <*0..3*>] [**timeout** <*1..15*>]

tacacs-server {**key** <*string*> | **retransmit** <*0..3*> | **timeout** <*1..15*>}

no tacacs-server host <*IP address*> [**auth-port** <*port*>]

no tacacs-server {**key** | **retransmit** | **timeout**}

Arguments

host <*IP address*>	Configures host, at specified IP address, to send TACACS+ authentication requests. Use the **no** form of this command to stop sending TACACS+ authentication requests to host.
auth-port <*port*>	Specifies the authentication port to use with this TACACS+ server. Use the **no** form of this command to stop sending TACACS+ authentication requests to the authentication port.
auth-type {ascii | pap}	Specifies the authentication type to use with this TACACS+ server. The options are: • **ascii** – ASCII authentication • **pap** – PAP (Password Authentication Protocol) authentication
key <*string*>	Specifies the shared secret key to use with this TACACS+ server. Use the **no** form of this command to remove the global TACACS+ server key.
retransmit <*0..3*>	Specifies the maximum number of retries that can be made in the attempt to connect to this TACACS+ server. The range is 0 to 3. Use the **no** form of this command to reset the global TACACS+ server retransmit count to its default.
timeout <*1..15*>	Specifies the number of seconds to wait before the connection times out with this TACACS+ server, because of keyboard inactivity. The range is 1 to 15 seconds. Use the **no** form of this command to reset the global TACACS+ server timeout setting to its default.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show tacacs” on page 350.

Usage Guidelines

When you don’t specify a host IP, then configurations for **host**, **key**, and **retransmit** are global for TACACS+ servers.

Examples

To define the TACACS+ shared secret as “mysecret”:

```
(config) # tacacs-server key mysecret
```

To specify that the TACACS+ server with the IP address of 10.10.10.10 uses PAP authentication and tries to retransmit a maximum of 9 times:

```
(config) # (config) # tacacs-server host 10.10.10.10 auth-type pap retransmit
9
```

To reset, to its default, the number of seconds after which the TACACS+ server times out after keyboard inactivity:

```
(config) # no tacacs-server timeout
```

tca

Description

Use the **tca** command to set the parameters for threshold crossing alerts.

Use the **no** form of this command to return a special instance (that is, specific values for a named tunnel) to the **default** values.

Syntax

tca <*tca-name*> **default** {**rising** | **falling**} **raise-threshold** <*value*> **clear-threshold** <*value*> [**sample-count** <*number of samples*>]

tca <*tca-name*> <*tunnel-name*> {**rising** | **falling**} **raise-threshold** <*value*> **clear-threshold** <*value*> [**sample-count** <*number of samples*>]

tca <*tca-name*> {**pass-through** | **pass-through-unshaped**} {**rising** | **falling**} **raise-threshold** <*value*> **clear-threshold** <*value*> [**sample-count** <*number of samples*>]

no tca <*tca-name*> {**default** | <*tunnel-name*>}

no tca <*tca-name*> {**default** | <*tunnel-name*>} [**rising** | **falling**]

tca <*tca-name*> {**default** | <*tunnel-name*>} {**enable** | **disable**}

tca <*tca-name*> {**pass-through** | **pass-through-unshaped**} {**enable** | **disable**}

Arguments

tca <*tca-name*>

Specifies which threshold crossing alert to configure. Some apply to one or more types of traffic. Others only have default values.

The options are:

- **file-system-utilization**
  How much of the file system space has been used, expressed as a percentage.
- **lan-side-rx-throughput**
  LAN–side Receive throughput, in kilobits per second (**kbps**).
- **latency**
  Tunnel latency, in milliseconds (**ms**).
- **loss-post-fec**
  Tunnel loss, as **tenths of a percent**, *after* applying Forward Error Correction (FEC).
- **loss-pre-fec**
  Tunnel loss, as **tenths of a percent**, *before* applying Forward Error Correction (FEC).
- **oop-post-poc**
  Tunnel out-of-order packets, as **tenths of a percent**, *after* applying Packet Order Correction (POC).
- **oop-pre-poc**
  Tunnel out-of-order packets, as **tenths of a percent**, *before* applying Packet Order Correction (POC).
- **optimized flows**
  Total number of optimized flows.
- **reduction**
  Tunnel reduction, in percent (**%**).
- **total-flows**
  Total number of flows.
- **utilization**
  Tunnel utilization, as a percent (**%**).
- **wan-side-tx-throughput**
  WAN–side transmit throughput, in kilobits per second (**kbps**).

default

Sets the **tca** <*tca-name*> argument values for any tunnels that weren't specifically named in configuring an argument. For example, if you configured latency values for **tunnel_1** but not for **tunnel_2** and **tunnel_3**, then configuring **default** would only apply values to **tunnel_2** and **tunnel_3**.

<*tunnel-name*>

For specifying an individual tunnel for threshold configuration.

falling

Specifies a threshold crossing alarm for when the stat value falls too low.

rising

Specifies a threshold crossing alarm for when the stat value rises too high.

raise-threshold <*value*>

Specifies at what value to raise an alert.

clear-threshold <*value*>

After an alarm has been raised, specifies at what value to clear the alert.

- For a **rising** alarm, the clear-threshold value is equal to or less than the raise-threshold.
- For a **falling** alarm, the clear-threshold value is equal to or more than the raise-threshold

sample-count <*number of samples*>

Sets the number of samples that the metric must sustain below (or above) the threshold in order to raise (or clear) the alert.

enable	Enables this threshold control alert instance.
disable	Disables this threshold control alert instance.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show tca” on page 351.

Usage Guidelines

- This table lists the default state of each type of threshold crossing alert:

TCA	Type	Unit	Default [ON, OFF]	allow rising	allow falling
wan-side-throughput	system	kbps	OFF	4	4
lan-side-throughput	system	kbps	OFF	4	4
optimized-flows	system	flows	OFF	4	4
total-flows	system	flows	OFF	4	4
file-system-utilization	system	%	**ON**[a]	4	
latency	tunnel	msec	**ON**	4	
loss-pre-fec	tunnel	1/10th %	OFF	4	
loss-post-fec	tunnel	1/10th %	OFF	4	
oop-pre-poc	tunnel	1/10th %	OFF	4	
oop-post-poc	tunnel	1/10th %	OFF	4	
utilization	tunnel	%	OFF	4	4
reduction	tunnel	%	OFF		4

a. Cannot be disabled.

- Use the **no** form of this command to return a special instance (that is, specific values for a named tunnel) back to the **default** values.
- Use **no tca** <*tca-name*> **default** to delete the TCA instance.

Examples

To raise an alert when the percent reduction for *tunnel_a* falls below 60% and to clear the alarm as soon as reduction reaches 70%:

```
(config) # tca reduction tunnel_a falling raise-threshold 60 clear-threshold
70
```

terminal

Description

Use the **terminal** command to set terminal parameters.

Syntax

terminal length <*number of lines*>

terminal type <*terminal type*>
no terminal type

terminal width <*number of characters*>

Arguments

terminal length <*number of lines*>	Sets the number of lines for this terminal.
terminal type <*terminal type*>	Sets the terminal type. The options are **xterm**, **ansi**, and **vt100**. Use the **no** form of the command to clear the terminal type.
terminal width <*number of characters*>	Sets the number of maximum number of characters in a line (row) for this terminal.

Defaults

The default terminal length is 24 rows.

The default terminal width is 80 characters.

The default terminal type is **xterm**.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “show terminal” on page 354.

Usage Guidelines

None.

Examples

To set the line width to 120 characters for this terminal:

```
(config) # terminal width 120
```

username

Description

Use the **username** command to configure user accounts.

Use the **no** form of the command to delete the specific user account.

Syntax

username <*username*> **capability** {**admin** | **monitor**}
no username <*username*> **capability**

username <*username*> **disable**
no username <*username*> **disable**

username <*username*> **password**

username <*username*> **password 0** <*cleartext password*>

username <*username*> **password 7** <*encrypted password*>

no username <*username*>

Arguments

username <*username*>	Specifies the user ID to whom you want to grant capability. Use **no username** <*username*> to delete this user account.
capability admin	Grants admin user privileges to this user account. Use the **no** form of the command to reset capability for this user account to the default.
capability monitor	Grants monitor user privileges to this user account. Use the **no** form of the command to reset capability for this user account to the default.
disable	Disables the ability to login to this user account. Use the **no** form of the command to reenable this account.
password	When followed immediately by a carriage return, specifies to prompt for the login password rather than entering it on the command line.
password 0 <*cleartext password*>	Specifies a login password in clear text.
password 7 <*encrypted password*>	Specifies a login password with an encrypted string. Once the password is entered, the original characters are not recoverable by looking through the history or scrolling back in the file.

Defaults

The default username and the default password are both **admin**.

Command Mode

Global Configuration Mode

See Also

See “show usernames” on page 358.

Usage Guidelines

Some guidance about password creation:

- Passwords should be a minimum of 8 characters
- There should be at least one lower case letter and one upper case letter
- There should be at least one digit
- There should be at least one special character
- Consecutive letters in the password should not be dictionary words

Examples

To delete the user account, *franklin*:

```
config) # no username franklin
```

web

Description

Use the **web** command to configure the Web-based management User Interface.

Syntax

web auto-logout <*number of minutes*>
no web auto-logout

web {**enable** | **disable**}

web http {**enable** | **disable**}

web https {**enable** | **disable**}

web session max <*5–50*>
no web session max

Arguments

auto-logout <*number of minutes*>	Sets the length of user inactivity before auto-logout in minutes. The acceptable range is 10 – 60 minutes. Use the **no** form of the command to reset the automatic logout feature for Web sessions to the default setting of 1000 minutes.
disable	Disables the Web User Interface.
enable	Enables the Web User Interface.
http {**enable** | **disable**}	Enables or disables HTTP access to the Web User Interface.
https {**enable** | **disable**}	Enables or disables HTTPS (secure HTTP) access to the Web User Interface.
session max <*5–50*>	Specifies, as an integer, the maximum number of simultaneous Web sessions. Select a number between 5 and 50. Use the **no** form of the command to reset the maximum number of sessions to the default of 10.

Defaults

- The default auto-logout setting is 15 minutes.
- Web HTTP is disabled.
- Web HTTPS is enabled.
- The default HTTP port is 80.
- The default HTTPS port is 443.
- The maximum number of simultaneous Web sessions for an appliance is 10.

Command Mode

Global Configuration Mode

See Also

See “show web” on page 367.

Usage Guidelines

The acceptable range is between one minutes and 1440 minutes (one day).

Examples

To set the maximum length of keyboard inactivity to 7 hours before automatic logout:

```
(config) # web auto-logout 420
```

write

Description

Use the **write** command to save or display the commands in the running configuration.

Syntax

write memory

write terminal

Arguments

memory	Saves the running configuration to the active configuration file.
terminal	Displays the commands needed to recreate current running configuration.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

When you execute **write terminal** command, the CLI displays commands in the following categories:

- Network interface configuration
- Routing configuration
- Other IP configuration
- Logging configuration
- AAA configuration
- System network configuration
- Tunnel creation
- Tunnel configuration
- Pass-through configuration
- Network management configuration

Examples

None.

CHAPTER 3

Configuration Commands

This chapter describes the commands that allow you to configure the Silver Peak NX Series appliances.

access-list

Description

Use the **access-list** command to configure Access Lists and their rules.

Use the **no access-list** command to delete a specific ACL rule or an entire ACL.

Syntax

access-list *<acl name> <priority value>* {**permit** | **deny**} **protocol** {*<IP protocol number>* | *<protocol name>*} {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [**dscp** {*<dscp value>* | **any**}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **protocol** {*<IP protocol number>* | *<protocol name>*} {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **protocol ip** {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [**app** {*<application name>* | **any**}] [**dscp** {*<dscp value>* | **any**}][**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **protocol ip** {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [**app** {*<application name>* | **any**}] [**dscp** {*<dscp value>* | **any**}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **protocol ip** {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **protocol** {**tcp** | **udp**} {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [{*<source port number>* | **any**} {*<destination port number>* | **any**}] [**dscp** {*<dscp value>* | **any**}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **protocol** {**tcp** | **udp**} {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [{*<source port number>* | **any**} {*<destination port number>* | **any**}] [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **app** {*<application name>* | **any**}

access-list *<acl name> <priority value>* {**permit** | **deny**} **dscp** {*<dscp value>* | **any**} [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

access-list *<acl name> <priority value>* {**permit** | **deny**} **vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}

access-list *<acl name> <priority value>* **comment** *<comment text>*

no access-list *<acl name>* [*<priority value>*]

Arguments

access-list <*acl name*> <*priority value*>	Specifies the name of the ACL and the priority value for the (ACL) rule that you want to add or modify. You can set any priority value between 1 and 65535.
permit	Permits access to this ACL rule.
deny	For traffic that matches this ACL rule, discontinue further processing ***by this ACL***, and continue to look for a match in the subsequent policy entries.
comment	Add a comment for specified access list entry.
protocol {<*IP protocol number*> | <*IP protocol name*> | **ip** | **tcp** | **udp**}	Specifies the protocol to match: • The available IP protocol numbers include 1 through 254. • The available IP protocol names include: ah, egp, eigrp, encap esp, etherip, fc, gre icmp, idpr, idpr-cmtp, idrp igmp, igp, ip-comp, ip-mobility ipip, ipip4, ipx-in-ip, irtp iso-ip, iso-tp4, I2tp, mhrp ospf, pim, rdp, rsvp sctp, tlsp, vrrp • When you specify **protocol ip**, the assumption is that you are allowing *any* IP protocol. In that case, you also need to specify an application. If you don't, the CLI defaults to specifying **any** application.
{<*source IP address/netmask*> | **any**}	Matches against traffic that has a specific source IP address and netmask (in slash notation). For example, enter *10.2.0.0 0.0.255.255* as *10.2.0.0/16*. If you want to include traffic to all destinations, use **any**.
{<*destination IP address/netmask*> | **any**}	Matches against traffic that has a specific destination IP address and netmask (in slash notation). For example, *10.2.0.0/16*. If you want to include traffic to all destinations, use **any**.
{<*source port number*> | **any**} {<*destination port number*> | **any**}	When you specify **protocol tcp** or **protocol udp**, you can limit the traffic to specific source and/or destination ports. **any** is a wildcard.
app {<*application name*> | **any**}	Specifies a default or user-defined application name, or the name of a user-defined application group. **any** is a wildcard.
dscp {<*dscp value*> | **any**}	Specifies a DSCP value. The available values include: • af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs1, cs2, cs3, cs4, cs5, cs6, cs7, or ef. • **any** is a wildcard.

vlan {**any**|*<1..4094>*|*<interface.tag>*|*<any.tag>*|*<interface.any>*|*<interface.native>*}	Matches an interface and 802.1q VLAN tag. The available values include: • *<1..4094>* the number assigned to a VLAN • *<interface.tag>* as in **lan0.10** • *<any.tag>* as in **any.10** • *<interface.any>* as in **lan0.any** • *<interface.native>* as in **lan0.native** • **any** is a wildcard.
any	Is a wildcard.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show access-list” on page 256.

Usage Guidelines

You name a rule with a *priority*, which not only identifies the rule, but also specifies its sequence in that ACL. Within an ACL, every priority value must be unique. In other words, no two rules in a given ACL can have the same priority value. We recommend that you don’t make the priority values contiguous, so that you can later insert a new rule between two existing rules, without needing to change the priority values you’ve already set. For example, you might create an ACL with rules (priorities) 10, 20, 30, and 40. If you need to add several rules at a later time, you can easily place them between any of the existing rules.

If you need to replace an existing rule, just name the new rule with the same priority as the one you want to replace. The CLI overwrites the existing rule with your new one.

If you specify a priority to create a rule for an ACL that doesn’t already exist, the CLI creates the new ACL and populates it with the new rule.

Use the **no** form of this command to delete a rule within an ACL. If you delete the last rule of an ACL, that ACL is removed. If you don’t specify a priority value in the **no** command, the entire ACL is deleted.

IP Address and Netmasks

Source and destination IP addresses are immediately followed by a netmask "/n" where *n* is the number of contiguous non-wildcard bits counting from the left-most bit. For example, 10.10.10.0 /24 refers to the 10.10.10 class C subnet. Use the keyword **any** to specify that all bits are wildcards.

Using Deny

Since access lists define the matching criteria and not the action, you should remember that **deny** in this context does not actually “drop” traffic. Rather, the **deny** keyword is effectively a sort of break statement, preventing further processing by that particular ACL, and sending the traffic to look for matches against subsequent **policy** entries.

For example, if you wanted to accelerate all IP traffic except for ICMP traffic, you could enter the following commands:

```
access-list a1 100 deny protocol icmp any any
access-list a1 200 permit protocol ip any any
.
.
.
route-map map1 10 match acl a1
route-map map1 10 set tunnel tun1.
.
.
```

In this example, any ICMP traffic that attempts to match the ACL, *a1*, would immediately stop processing at the **deny** statement and would pass through.

Examples

To create a rule for an ACL named *acl2*, that matches against all IGP traffic that has a DSCP value of *be* (best effort):

```
(config) # access-list acl2 10 permit protocol igp any any dscp be
```

To accelerate all IP traffic except for ICMP traffic:

```
(config) # access-list a1 100 deny protocol icmp any any
(config) # access-list a1 200 permit protocol ip any any
```

To create a rule to match all IP traffic coming from the source 10.2.0.0 0.0.255.255:

```
(config) # access-list a2 40 permit protocol ip 10.2.0.0/16 any
```

To create a rule to match all UDP traffic going to port 53:

```
(config) # access-list a1 500 protocol udp any any any 53
```

To delete the priority 100 rule from the ACL named *ac18*:

```
(config) # no access-list acl8 100
```

active-flows

Description

Use the **active-flows** command to configure all active flows.

Syntax

active-flows {**reset-all**}

Arguments

reset-all	Resets all non-TCP accelerated active flows.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

application

Description

Use the **application** command to configure applications on the appliance.

Use the **no application** command to delete an application.

Syntax

application <*application priority*> <*application name*> **dscp** <*dscp value*>

application <*application priority*> <*application name*> **protocol** <*IP protocol number or name*>

application <*application priority*> <*application name*> **protocol** <*IP protocol number or name*> **src-ip** {<*source IP address ranges*> | **any**} [**src-port** {<*source port range*> | **any**}]

application <*application priority*> <*application name*> **protocol** <*IP protocol number or name*> **src-ip** {<*source IP address ranges*> | **any**} **src-port** {<*source port range*> | **any**} **dst-ip** {<*destination IP address ranges*> | **any**} [**dst-port** {<*destination port range*> | **any**}]

application <*application priority*> <*application name*> **protocol** <*IP protocol number or name*> **src-ip** {<*source IP address ranges*> | **any**} **src-port** {<*source port range*> | **any**} **dst-ip** {<*destination IP address ranges*> | **any**} **dst-port** {<*destination port range*> | **any**} [**dscp** <*dscp value*>]

application <*application priority*> <*application name*> **protocol** <*IP protocol number or name*> **src-ip** {<*source IP address ranges*> | **any**} **src-port** {<*source port range*> | **any**} **dst-ip** {<*destination IP address ranges*> | **any**} **dst-port** {<*destination port range*> | **any**} **dscp** <*dscp value*> [**vlan** {**any** | <*1..4094*> | <*interface.tag*> | <*any.tag*> | <*interface.any*> | <*interface.native*>}]

no application <*application priority*>

Arguments

<*application priority*>	Specifies the priority value of the application.
<*application name*>	Specifies the name of the application.
protocol <*IP protocol number or name*>	Specifies the application protocol.
src-ip {<*source IP address ranges*>	You can specify a comma-delimited list. For example: `192.1.2.0/24,192.10.10.100-200` If you want to include all addresses, use **any**.
src-port {<*source port ranges*>	Comma separated port ranges. If you want to include all ports, use **any**.
dst-ip {<*destination IP address ranges*>	You can specify a comma-delimited list. For example: `192.1.2.0/24,192.10.10.100-200` If you want to include all addresses, use **any**.
dst-port {<*destination port ranges*>	Comma separated port ranges. If you want to include all ports, use **any**.

dscp {*<dscp value>* | **any**}	Specifies a DSCP value. The available values include: • af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs1, cs2, cs3, cs4, cs5, cs6, cs7, or ef. • **any** is a wildcard.
vlan {**any**|*<1..4094>*|*<interface.tag>* |*<any.tag>*|*<interface.any>*| *<interface.native>*}	Matches an interface and 802.1q VLAN tag. The available values include: • *<1..4094>* the number assigned to a VLAN • *<interface.tag>* as in **lan0.10** • *<any.tag>* as in **any.10** • *<interface.any>* as in **lan0.any** • *<interface.native>* as in **lan0.native** • **any** is a wildcard.
any	Is a wildcard.

Defaults

None.

Command Mode

User EXEC mode

Privileged EXEC mode

Global Configuration Mode

See Also

See “show application” on page 259.

Usage Guidelines

None.

Examples

To create an application, *surf*, for traffic that comes from the IP address, 192.4.4.11:

```
NX3600 > application 10 surf protocol any src-ip 192.4.4.11
```

application-group

Description

Use the **application-group** command to specify a group of (one or more) applications.

Use **no application-group** to remove one or more applications from an application group or to delete the group, itself.

Syntax

application-group <*application group name*> <*app1*> [, <*app2*>, <*app3*>…]

no application-group <*application group name*> [, <*app1*>, <*app2*>…]

Arguments

<*application group name*>	Defines a unique group name. The name is checked against existing application groups and, if the name does not exist, the CLI creates it. If the name does exist, then the application(s) you specify are added to the existing group.
<*app*>	Specifies an existing application name, whether it's built-in or user-defined.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- "access-list" on page 60
- "show application" on page 259

Usage Guidelines

If your ACLs or policy maps contain match conditions that involve multiple applications, you can simplify the match conditions with *application groups*. Application groups are identifiers that you can create to represent a list of applications.

You create an application group by naming the group and specifying at least one application that belongs in it. After creating it, you can modify the application group by adding or removing applications.

To add applications to an application group that already exists, enter the name of the application group, followed by the applications you are adding. For example, to add two applications to the application group, *omega*, you might use the following command:

```
(config) # application-group omega http, tftp
```

If *omega* did not exist, the CLI would create it and it would contain these two applications.

If you then wanted to remove *http* from *omega*, you would issue the following command:

```
(config) # no application-group omega http
```

The **application-group** command has the following restrictions:

- If you specify more than one application at a time for an application group, you must separate the applications with commas. If you just use spaces, the CLI will respond with an error message.
- If you attempt to delete an application that is not in the application group that you specify, then the CLI displays an error message.

Examples

To create an application group, *encrypted*, that contains the applications SSH, HTTPS, and SFTP:

```
(config) # application-group encrypted ssh, https, sftp
```

To add two applications to the existing application group, *omega*:

```
(config) # application-group omega http, tftp
```

banner login

Description

Use the **banner login** command to create a message for the system login banner, such as legal or welcome text.

Use the **no** form of this command to reset the system login banner.

Syntax

banner login <*message string*>

no banner login

Arguments

<*message string*>	Specifies the message to display before a user logs into the appliance. A message that includes spaces requires quotes at the beginning and end of the message string.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the “banner motd” on page 70.

Usage Guidelines

None.

Examples

To configure the banner message, *Gotcha!*, to display at login:

```
(config) # banner login Gotcha!
```

To configure the banner message, *“How about some coffee?”*, to display at login:

```
(config) # banner login “How about some coffee?”
```

banner motd

Description

Use the **banner motd** command to create a "Message of the Day" banner.

Use the **no** form of this command to reset the system Message of the Day banner.

Syntax

banner motd <*message string*>

no banner motd

Arguments

<*message string*>	Specifies the message to display for the Message of the Day. A message that includes spaces requires quotes at the beginning and end of the message string. The Message of the Day appears after successful login.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See "banner login" on page 69.

Usage Guidelines

None.

Examples

To configure the Message of the Day, *Greetings*, to display at login:

```
(config) # banner motd Greetings
```

To configure the banner message, *"Time for a margarita"*, to display at login:

```
(config) # banner motd "Time for a margarita"
```

bridge

Description

Use the **bridge** command to configure bridge mode.

Syntax

bridge propogate-linkdown {enable | disable}

bridge transition-fdb-age <*1-300*>

bridge transition-time <*1-300*>

Arguments

propogate-linkdown {enable | disable}	When enabled, forces the WAN interface link to go down when the corresponding LAN interface goes down, and vice versa.
transition-fdb-age <*1-300*>	Specifies the maximum age of a MAC entry, in seconds, during the time that a link is going down.
transition-time <*1-300*>	Specifies, in seconds, the time to wait after the first link goes down before propagating the second link down.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show bridge” on page 267.
- “clear” on page 15

Usage Guidelines

None.

Examples

To configure 30 seconds as the time to wait before propagating the WAN interface’s link down to the LAN:

```
(config) # bridge transition-time 30
```

cdp

Description

Use the **cdp** command to configure Cisco Discovery Protocol (CDP) parameters.

Syntax

cdp {enable | disable}

cdp holdtime <*10-255*>

cdp timer <*5-254*>

Arguments

enable | disable	Globally enables or disables Cisco Discovery Protocol.
holdtime <*10-255*>	Specifies the length of time, in seconds, that the receiver must keep this packet.
timer <*5-254*>	Specifies the rate at which CDP packets are sent, in packets per second.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show cdp” on page 269
- “clear” on page 15

Usage Guidelines

None.

Examples

To specify that CDP packets be sent at 240 packets per second:

```
(config) # cdp timer 240
```

cifs signing delegation domain

Description

Use the **cifs signing delegation domain** command to give the appliance the ability to optimize a signed CIFS connection.

Syntax

cifs signing delegation domain join domain-name <*name of domain to join*> **username** <*username*> **password** <*password of user for join*>

cifs signing delegation domain join domain-name <*domain name*> **username** <*username*> **password** <*password of user for join*> **dchost** <*IP address of Domain Controller for join*>

cifs signing delegation domain leave domain-name <*name of domain to leave*>

Arguments

join domain-name <*domain fooname*>	Specifies the name of the domain that the appliance must join as a first step to enabling this feature.
leave domain-name <*domain fooname*>	Specifies the name of the domain that the appliance will no longer be part of.
username <*username*>	Specifies username required for joining the domain.
password <*username*>	Specifies password required for joining the domain.
dchost <*IP address of Domain Controller of join*>	Specifies the IP address of the Domain Controller that controls the CIFS connection.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show cifs signing delegation” on page 271.
- “system smb-signing” on page 247
- “show system” on page 347

Usage Guidelines

This command must be executed together with the **system smb-signing** command.

Examples

None.

clock set

Description

Use the **clock set** command to set the system time and/or date.

Syntax

clock set <*hh*>:<*mm*>:<*ss*> [<*yyyy*>/<*mm*>/<*dd*>]

Arguments

<*hh*>**:**<*mm*>**:**<*ss*>	Sets the hour, minute, and second of the current time, but leaves the date unchanged. Time is based on a 24-hour clock.
<*yyyy*>/<*mm*>/<*dd*>	Sets the system's date by year/month/date.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- "clock timezone" on page 75
- "show clock" on page 273

Usage Guidelines

None.

Examples

To set the time and date to exactly one minute after midnight on the morning of August 11, 2007:

```
(config) # clock set 00:01:00 2007/08/11
```

clock timezone

Description

Use the **clock timezone** command to set the time zone for the system.

Use the **no** form of the command to reset the time to its default of Greenwich Mean Time, GMT (also known as UTC).

Syntax

clock timezone <*region*> . . .
no clock timezone

Arguments

<*region*>	Specify the region, country, locality, or timezone for the system.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “clock set” on page 74
- “show clock” on page 273

Usage Guidelines

You set the timezone by selecting from a series of menus. To see the list of possible values for timezone, perform the following procedure:

1 Enter the following command at the command line:

```
<appliance> (config) # clock timezone ?
```

The CLI displays a list of world regions, followed by the command prompt, as in the following example:

```
Africa
America
Antarctica
Arctic
Asia
Atlantic_Ocean
Australia
Europe
GMT-offset
```

```
Indian_Ocean
Pacific_Ocean
UTC
```

2 Choose a region from the list and append the region to the command, along with a question mark (?). For example, to specify America, you would enter the following command:

```
<appliance> (config) # clock timezone America ?
```

The CLI displays the regions in America, such as in the following example:

```
Caribbean
Central
North
South
```

3 Continue specifying the appropriate menu selections, ending each command with a question mark to display the next menu. When the CLI displays <*cr*>, press **Enter** to complete the command.

The CLI is case-sensitive.

Examples

None.

cluster

Description

Use the **cluster** command to configure a cluster of appliances for flow redirection.

Use the **no** form of this command to delete a peer appliance from a cluster.

Syntax

cluster interface <*interface*>

cluster peer <*IP address, IP address, ...*>
no cluster peer <*IP address*>

Arguments

interface <*interface*>	Specifies an interface for intra-cluster communication. Generally, Silver Peak recommends using **mgmt1**.
peer <*IP address*>	Specifies a comma-delimited list of peer IP addresses. Use the **no** form of the command to delete a peer from a cluster.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “flow-redirection” on page 86.
- “clear” on page 15
- “show cluster” on page 274
- “show flow-redirection” on page 283

Usage Guidelines

If you specify **mgmt1** as the cluster interface, then when created a list of peers, use the **mgmt1** IP addresses in the comma-delimited list.

Examples

- To configure **mgmt1** as the cluster interface:

```
Silver-Peak # cluster interface mgmt1
```

- To create a cluster from appliances with the cluster interfaces, 10.10.10.3, 10.10.20.2, and 10.10.30.5:

```
Silver-Peak # cluster peer 10.10.10.3, 10.10.20.2, 10.10.30.5
```

configure terminal

Description

Use the **configure terminal** command to enter configuration mode. Use the **no** form of this command to leave the configuration mode.

Syntax

configure terminal

no configure

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

To exit the configuration mode, you may also use the **exit** command.

The CLI also accepts these two shortened versions of **configure terminal**:

```
Silver-Peak # config t
Silver-Peak # co t
```

As a result, the prompt changes to

```
Silver-Peak (config) #
```

Examples

None.

disable

Description

Use the **disable** command to exit the Privileged EXEC mode.

Syntax

disable

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

See Also

See the following related commands:

- “enable” on page 81
- “enable password” on page 82

Usage Guidelines

When you use the **disable** command, you enter the User EXEC mode.

Examples

To go from Privileged EXEC Mode to User EXEC mode (command followed by result):

```
Silver-Peak # disable
Silver-Peak >
```

enable

Description

Use the **enable** command to enter Privileged EXEC mode.

Syntax

enable

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

See Also

See the following related commands:

- “disable” on page 80
- “enable password” on page 82

Usage Guidelines

The CLI also accepts this shortened version of **enable**:

```
Silver-Peak > en
```

Examples

To go from User EXEC Mode to Privileged EXEC mode (command followed by result):

```
Silver-Peak > enable
Silver-Peak #
```

enable password

Description

Use the **enable password** command to set the password required to enter Privileged EXEC mode.

Use the **no** form of the command to remove the requirement of a password to enter Privileged EXEC mode.

Syntax

enable password <*password*>
no enable password

enable password 0 <*cleartext password*>

enable password 7 <*encrypted password*>

Arguments

password <*password*>	Sets the password required to enter enable mode. By default, it will be in cleartext. Use the **no** form of this command to remove the requirement of a password to enter Privileged EXEC mode.
password 0 <*cleartext password*>	Sets the enable password with a cleartext string.
password 7 <*encrypted password*>	Sets the enable password with an encrypted string. Encrypted password entries aren't visible when viewing a history of commands.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- "disable" on page 80
- "enable" on page 81

Usage Guidelines

- To require the cleartext password, ratchet, for entering *enable* mode:

```
<silver-peak> (config) # enable password 0 ratchet
```

- To remove the need for a password for entering *enable* mode:

```
<silver-peak> (config) # no enable password
```

exit

Description

Use the **exit** command to log out of the CLI from the User EXEC or Privileged EXEC modes. If you use the exit command from the Global Configuration mode, you enter the Privileged EXEC mode.

Syntax

exit

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

flow-export

Description

Use the **flow-export** command to configure the export of data to NetFlow collectors.

Syntax

flow-export active-flow-timeout *<1-30 minutes>*

flow-export destination {**1** | **2**} *<Collector IP address> <Collector port>*
no flow-export destination {**1** | **2**}

flow-export {**disable** | **enable**}

flow-export engine-id *<0-255>*

flow-export engine-type *<0-255>*

flow-export traffic-type *<lan-rx | lan-tx | wan-rx | wan-tx>*
no flow-export traffic-type *<lan-rx | lan-tx | wan-rx | wan-tx>*

Arguments

active-flow-timeout *<1-30>*	Specifies the flow-export active flow timeout. The range is 1 to 30 minutes.
destination {1 | 2} *<Collector IP address> <Collector port>*	Specifies the IP address and port for the NetFlow collector. You can configure up to two collectors. Use the **no** form of this command to disable the export of NetFlow records to either Collector 1 or Collector 2.
disable	Disables the export of NetFlow records.
enable	Enables the export of NetFlow records.
engine-id *<0-255>*	Specifies the VIP or LC slot number of the flow switching engine.
engine-type *<0-255>*	Specifies the flow-export engine type. They are: • **0** for RP, and • **1** for VIP/LC.
traffic-type *<lan-rx | lan-tx | wan-rx | wan-tx>*	Specifies which interface to turn on for flow exporting. Use the **no** form of this command to turn off a specific interface's flow exporting.

Defaults

When you enable flow exporting, it defaults to the WAN Tx interface.

Command Mode

Global Configuration Mode

See Also

See “show flow-export” on page 282.

Usage Guidelines

The appliance lets you turn on up to four interfaces for flow exporting. However, you must specify each interface by using a separate command.

Examples

To configure NetFlow Collector #2, located at 10.10.10.4, using port 146:

```
(config) # flow-export destination 2 10.10.10.4 146
```

To disable the export of NetFlow records to Collector #1:

```
(config) # flow-export destination 1
```

To turn on the **WAN Tx** and **LAN Rx** interfaces for flow exporting:

```
(config) # flow-export traffic-type wan-tx (carriage return)
(config) # flow-export traffic-type lan-rx
```

flow-redirection

Description

Use the **flow-redirection** command to configure flow redirection.

Syntax

flow-redirection {enable | disable}

flow-redirection wait-time <*0-500*>

Arguments

enable	Enables flow redirection.
disable	Disables flow redirection.
wait-time <*1-500*>	Specifies flow redirection wait time in milliseconds.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “cluster” on page 77
- “clear” on page 15
- “show flow-redirection” on page 283
- “show cluster” on page 274

Usage Guidelines

Redirection enabled simply enables and disables redirection on the selected appliance.

Examples

None.

hostname

Description

Use the **hostname** command to set host name for the appliance.

Use the **no** form of this command to remove the host name from the appliance.

Syntax

hostname <*hostname*>

no hostname

Arguments

<*hostname*>	Designates the host name for the appliance, not including the domain name.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show hosts” on page 284.

Usage Guidelines

Hostnames may contain letters, numbers, periods ('.'), and hyphens ('-'), but may not begin with a hyphen. Hostnames may **not** contain spaces.

The hostname is limited to 24 characters.

When you remove the hostname, the system reverts to the identifier assigned before shipping. For example, *silverpeak-2f8598*.

Examples

To rename the appliance to *Chicago*:

```
(config) # hostname Chicago
```

iflabel

Description

Use the **iflabel** command to assign labels to interfaces.

Syntax

iflabel add {**lan-label** | **wan-label**} *<label string with no spaces>*

Arguments

add	Add interface label.
delete	Delete interface label.
lan-label	Add LAN interface label.
wan-label	Add WAN interface label.
<label string with no spaces>	Specifies the name of this interface. For example: *video* or *data*.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show iflabels” on page 285

Usage Guidelines

No spaces allowed in the label string.

Examples

To add a WAN label, *Internet*:

```
(config) # iflabel wan-label internet
```

interface cdp

Description

Use the **interface cdp** command to enable or disable Cisco Discovery Protocol (CDP) for this interface.

Syntax

interface <*interface name*> **cdp** {**enable** | **disable**}

Arguments

<*interface name*>	Specifies the name of this interface.
enable	Enables CDP on this network interface.
disable	Disables CDP on this network interface.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “cdp” on page 72
- “show cdp” on page 269
- “show interfaces cdp” on page 289
- “clear” on page 15

Usage Guidelines

To see a list of the available interface names you may use, enter the following command:

```
<silver-peak> (config) # interface ?
```

Examples

None.

interface dhcp

Description

Use the **interface dhcp** command to enable Dynamic Host Configuration Protocol (DHCP) for this interface.

Use the **no** form of this command to disable DHCP for this interface.

Syntax

interface <*interface name*> **dhcp**

interface <*interface name*> **dhcp renew**

no interface <*interface name*> **dhcp**

Arguments

<*interface name*>	Specifies the name of this interface.
renew	Renews DHCP for this interface.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface ip address” on page 93
- “interface mac address” on page 96
- “show interfaces” on page 287

Usage Guidelines

To see a list of the available interface names you may use, enter the following command:

```
<silver-peak> (config) # interface ?
```

Examples

None.

interface harden

Description

Use the **interface harden** command to enable hardening for this WAN interface.

Use the **no** form of this command to disable hardening for this WAN interface.

Syntax

interface <*interface name*> **harden**

no interface <*interface name*> **harden**

Arguments

<*interface name*>	Specifies the name of this interface.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show interfaces” on page 287.

Usage Guidelines

WAN hardening is an option that provides additional protection against unsafe connections from remote sites. When WAN hardening is enabled, only traffic arriving from a Silver Peak IPsec tunnels is allowed to enter.

When Silver Peak appliances are deployed in Router Mode, you have the option of hardening any WAN–side interface. This means:

- For traffic inbound from the WAN, the appliance ***only*** accepts encapsulated traffic arriving from another Silver Peak appliance, via an IPsec tunnel. All other connections are rejected.
- For traffic outbound to the WAN, the appliance only allows IPsec tunnel packets and management traffic.
- Any data from the internet that gets backhauled via a Silver Peak IPSec tunnel will reach its destination at the hardened sites. This allows for integration with other security tools, such as firewalls, at the data center.
- Data sourced directly from the internet, or any other connection that doesn’t flow through a Silver Peak IPsec tunnel, is discarded when it hits the hardened interface. Only data from authenticated Silver Peak IPsec tunnels is allowed to pass across a hardened interface.

Examples

None.

interface inbound-max-bw

Description

Use the **interface inbound-max-bw** command to configure the maximum bandwidth for inbound traffic.

Syntax

interface <*interface name*> **inbound-max-bw** <*BW in kbps*>

Arguments

<*BW in kbps*>	Specifies the bandwidth in kilobits per second.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show interfaces” on page 287.

Usage Guidelines

None.

Examples

None.

interface ip address

Description

Use the **interface ip address** command to configure IP address and netmask for this interface.

Use the **no** form of this command to erase the IP address and netmask for this interface.

Syntax

interface <*interface name*> **ip address** <*ip address*> <*netmask*>

interface <*interface name*> **ip address** <*ip address*> <*netmask*> **nexthop** <*ip address*>

no interface <*interface name*> **ip address**

Arguments

<*interface name*>	Specifies the name of this interface.
<*ip address*> <*netmask*>	Specifies the source IPv4 address and netmask in standard or slash notation. For example, *10.2.0.0 0.0.255.255* could be entered as *10.2.0.0 /16.*
nexthop <*ip address*>	Next-hop address for this interface. It continues the IP format (IPv4 or IPv6) of the address for which it is the next hop.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface dhcp” on page 90
- “interface mac address” on page 96
- “show interfaces” on page 287

Usage Guidelines

To see a list of the available interface names you may use, enter the following command:

```
<silver-peak> (config) # interface ?
```

Examples

None.

interface label

Description

Use the **interface label** command to configure a label for the interface.

Use the **no** form of this command to remove the label from this interface.

Syntax

interface <*interface name*> **label** <*label string*>

no interface <*interface name*> **label** <*label string*>

Arguments

<*interface name*>	Specifies the name of this interface.
label <*label string*>	Specifies the label given to the interface. For example, *internet* or *voice*.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces” on page 287.

Usage Guidelines

None.

Examples

None.

interface lan-if

Description

Use the **interface lan-if** command to specify that this interface only allow LAN traffic when deploying the appliance in in-line router mode.

Use the **no** form of this command to remove the limitation from this interface.

Syntax

interface <*interface name*> **lan-if**

no interface <*interface name*> **lan-if**

Arguments

<*interface name*>	Specifies the name of this interface.
lan-if	Specifies that the interface only allow LAN traffic.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface wan-if” on page 129
- “show interfaces” on page 287.

Usage Guidelines

Only used for in-line router mode.

Examples

None.

interface mac address

Description

Use the **interface mac address** command to configure the MAC (Media Access Control) address for a selected interface.

Use the **no** form of this command to erase the MAC address for this interface.

Note This command is not supported on physical (NX) Silver Peak appliances.

Syntax

interface <*interface name*> **mac address** <*MAC address of interface to use*>

no interface <*interface name*> **mac address**

Arguments

<*interface name*>	Specifies the name of this interface.
mac address <*MAC address of interface to use*>	Specifies the MAC address.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface dhcp” on page 90
- “interface ip address” on page 93
- “show interfaces” on page 287

Usage Guidelines

None.

Examples

None.

interface mtu

Description

Use the **interface mtu** command to configure MTU (Maximum Transmission Unit) for this interface.

Use the **no** form of this command to reset the MTU for this interface to its default.

Syntax

interface <*interface name*> **mtu** <*MTU in bytes*>

no interface <*interface name*> **mtu**

Arguments

<*interface name*>	Specifies the name of this interface.
mtu <*MTU in bytes*>	In bytes, the largest size packet that can be sent. The range is 700 to 2400.

Defaults

The default MTU is **1500**.

Command Mode

Global Configuration Mode

See Also

See “show interfaces” on page 287.

Usage Guidelines

To see a list of the available interface names you may use, enter the following command:

```
<silver-peak> (config) # interface ?
```

Examples

None.

interface outbound-max-bw

Description

Use the **interface outbound-max-bw** command to configure maximum bandwidth for outbound traffic.

Syntax

interface <*interface name*> **outbound-max-bw** <*BW in kbps*>

Arguments

<*BW in kbps*>	Specifies the bandwidth in kilobits per second.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces” on page 287

Usage Guidelines

None.

Examples

None.

interface pass-through

Description

Use the **interface pass-through** command to configure the pass-through parameters for the WAN interface.

Syntax

interface pass-through {**max-bandwidth** <*kbps*> | **min-bandwidth** <*kbps*>}

Arguments

max-bandwidth <*kbps*>	Configures maximum bandwidth in kilobits per second.
min-bandwidth <*kbps*>	Configures minimum bandwidth in kilobits per second.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces” on page 287
- “show interfaces pass-through” on page 291

Usage Guidelines

If you try to configure too high a maximum bandwidth, the CLI returns a message telling you what the maximum allowable value is, given the configured System Bandwidth.

Examples

To set the maximum bandwidth for pass-through traffic at the wan0 interface to 9000 kilobits per second:

```
(config) # interface pass-through max-bandwidth 9000
```

interface shutdown

Description

Use the **interface shutdown** command to disable an interface.

Use the **no** form of this command to enable this interface.

Syntax

interface <*interface name*> **shutdown**

no interface <*interface name*> **shutdown**

Arguments

<*interface name*>	Specifies the name of this interface.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show interfaces” on page 287.

Usage Guidelines

To see a list of the available interface names you may use, enter the following command:

```
<silver-peak> (config) # interface ?
```

Examples

None.

interface speed-duplex

Description

Use the **interface speed-duplex** command to configure the speed and duplex of this interface.

Syntax

interface <*interface name*> **speed-duplex** <*speed/duplex*>

Arguments

<*interface name*>	Specifies the name of this interface.
<*speed/duplex*>	Specifies the speed and duplex of this interface. Use one of the following settings, depending on your appliance model: • **auto/auto** • **10/full** • **100/full** • **1000/full** • **10000/full**

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show interfaces” on page 287.

Usage Guidelines

To see a list of the available interface names you may use, enter the following command:

```
<silver-peak> (config) # interface ?
```

Examples

None.

interface tunnel admin

Description

Use the **interface tunnel admin** command to configure the tunnel administrative mode.

Use the **no** form of this command to reset the tunnel administrative mode to default.

Syntax

interface tunnel <*tunnel name*> **admin** {**up** | **down**}

no interface tunnel <*tunnel name*> **admin**

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
up	Enables the tunnel.
down	Disables the tunnel.

Defaults

The default for Admin is **down**.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

To enable the tunnel, *Rosenkrantz*, for diagnostics only:

```
(config) # interface tunnel Rosenkrantz admin diag
```

interface tunnel alias

Description

Use the **interface tunnel alias** command to configure an alias for the tunnel for display purposes.

Syntax

interface tunnel <*tunnel name*> **alias** <*tunnel alias*>

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
<*tunnel alias*>	Specifies the alias to display for this tunnel.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces tunnel” on page 294

Usage Guidelines

None.

Examples

None.

interface tunnel bind-tunnel

Description

Use the **interface tunnel bind-tunnel** command to bind a tunnel to a bonded tunnel.

Use the **no** form of this command to unbind a tunnel from a bonded tunnel.

Syntax

interface tunnel <*tunnel name*> **bind-tunnel** <*tunnel name*>

no interface tunnel <*tunnel name*> **bind-tunnel** <*tunnel name*>

Arguments

<*tunnel name*>	Specifies the name for this tunnel.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces tunnel” on page 294

Usage Guidelines

None.

Examples

None.

interface tunnel control-packet

Description

Use the **interface tunnel control-packet** command to configure the appliance's tunnel health and control packets.

Syntax

interface tunnel <*tunnel name*> **control-packet dscp** <*DSCP marking for this tunnel*>

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
dscp <*DSCP marking for this tunnel*>	Specifies the DSCP option for the tunnel's control packets: • **af11** AF11 dscp (001010) • **af12**AF12 dscp (001100) • **af13**AF13 dscp (001110) • **af21**AF21 dscp (010010) • **af22**AF22 dscp (010100) • **af23**AF23 dscp (010110) • **af31**AF31 dscp (011010) • **af32**AF32 dscp (011100) • **af33**AF33 dscp (011110) • **af41**AF41 dscp (100010) • **af42**AF42 dscp (100100) • **af43**AF43 dscp (100110) • **be**BE dscp (000000) • **cs1**CS1 dscp (001000) • **cs2**CS2 dscp (010000) • **cs3**CS3 dscp (011000) • **cs4**CS4 dscp (100000) • **cs5**CS5 dscp (101000) • **cs6**CS6 dscp (110000) • **cs7**CS7 dscp (111000) • **ef**EF dscp (101110)

Defaults

The default (and recommended) tunnel health DSCP setting is **be**.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces tunnel” on page 294

Usage Guidelines

None.

Examples

None.

interface tunnel create

Description

Use the **interface tunnel create** command to create a tunnel interface.

Syntax

interface tunnel <*tunnel name*> **create** <*(local) IP address*> <*(remote) IP address*>

interface tunnel <*tunnel name*> **create** <*(local) IP address*> <*(remote) IP address*> <*MinBW in kbps*> {<*MaxBW in kbps*> | **auto**}

interface tunnel <*tunnel name*> **create appliance-ip** <*(remote) IP address*>

interface tunnel <*tunnel name*> **create appliance-ip** <*(remote) IP address*> <*MinBW in kbps*> {<*MaxBW in kbps*> | **auto**}

interface tunnel <*tunnel name*> **create bonded-tunnel tag-name** <*overlay name*> [**bonded-id** <*overlay ID*>]

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
<*(local) IP address*>	Specifies the IP address of the local appliance.
<*(remote) IP address*>	Specifies the IP address of the remote appliance.
<*MinBW in kbps*>	Specifies the tunnel's minimum bandwidth in kilobits per second.
<*MaxBW in kbps*>	Specifies the tunnel's maximum bandwidth in kilobits per second.
appliance-ip	Specifies the remote IP address for this tunnel.
auto	Auto-negotiates maximum bandwidth in kilobits per second.
bonded-tunnel tag-name <*overlay name*>	Specifies a tag name for a bonded tunnel.
bonded-id <*overlay ID*>	Specifies the overlay ID for a bonded tunnel.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- "show interfaces tunnel" on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

None.

interface tunnel gre-protocol

Description

Use the **interface tunnel gre-protocol** command to configure the GRE protocol ID for a tunnel.

Use the **no** form of this command to reset the GRE protocol ID for this tunnel to its default.

Syntax

interface tunnel <*tunnel name*> **gre-protocol** <*Layer-2 protocol ID*>

no interface tunnel <*tunnel name*> **gre-protocol**

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
<*Layer-2 protocol ID*>	Specifies the Layer-2 protocol ID in the GRE header (decimal). For example, *2048* for *IP*.

Defaults

The default Layer-2 protocol ID in the GRE header (decimal) is **2048**.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel ipsec” on page 110
- “interface tunnel mode” on page 115
- “interface tunnel revert” on page 120
- “interface tunnel udp-flow” on page 124
- “interface tunnel udp-port” on page 125
- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

None.

interface tunnel ipsec

Description

Use the **interface tunnel ipsec** command to create IPSec (Internet Protocol Security) options for this tunnel.

Syntax

interface tunnel <*tunnel name*> **ipsec** {**disable | enable**}

interface tunnel <*tunnel name*> **ipsec enable preshared-key** <*key*>

interface tunnel <*tunnel name*> **ipsec enable replay-check-window** {**64 | 1024 | disable | auto**}

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
disable	Disables IPSec for this tunnel.
enable	Enables IPSec for this tunnel.
enable preshared-key <*key*>	Configures preshared key for IPSec for this tunnel.
replay-check-window {64 | 1024 | disable | auto}	Configures the IPSec anti-replay-check window for this tunnel. The IPSec Anti-replay window provides protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. The decryptor keeps track of which packets it has seen on the basis of these numbers. The default window size is **64** packets.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel gre-protocol” on page 109
- “interface tunnel mode” on page 115
- “interface tunnel revert” on page 120
- “interface tunnel udp-flow” on page 124
- “interface tunnel udp-port” on page 125
- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Configurable IPSEC anti-replay Window

In environments with significant out-of-order packet delivery, IPSec may drop packets that are outside of the anti-replay window.

- To determine whether packets are falling outside of the antireplay window, execute the following CLI command:

  ```
  show interfaces tunnel <tunnel name> stats ipsec
  ```

  and look for increases in “Total bytes dropped in replay check”.

- To change the IPSec anti-replay window, use the following CLI command:

```
interface tunnel <tunnel name> ipsec replay-check-window
<64|1024|disable|auto>
```

Examples

None.

interface tunnel max-bandwidth

Description

Use the **interface tunnel max-bandwidth** command to configure maximum bandwidth for this tunnel.

Syntax

interface tunnel <*tunnel name*> **max-bandwidth** {<*kbps*> | **auto**}

Arguments

tunnel <tunnel name>	Specifies the name for this tunnel.
max-bandwidth <*kbps*>	Specifies the maximum bandwidth in kilobits per second for this interface tunnel. The value must be a number between *0* and *4294967295*.
max-bandwidth auto	Auto-negotiates the maximum bandwidth in kilobits per second for this interface tunnel.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel min-bandwidth” on page 113
- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

None.

interface tunnel min-bandwidth

Description

Use the **interface tunnel min-bandwidth** command to configure minimum bandwidth for this tunnel.

Syntax

interface tunnel <*tunnel name*> **min-bandwidth** <*kbps*>

Arguments

tunnel <*tunnel name*>	Specifies the name for this tunnel.
min-bandwidth <*kbps*>	Specifies the minimum bandwidth in kilobits per second for this interface tunnel. The value must be a number between *0* and *4294967295*.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel max-bandwidth” on page 112
- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

None.

interface tunnel mode

Description

Use the **interface tunnel mode** command to configure the encapsulation mode for this tunnel as either GRE or UDP.

Use the **no** form of this command to reset the mode for this tunnel to its default.

Syntax

interface tunnel <*tunnel name*> **mode** {**gre** | **udp**}

no interface tunnel <*tunnel name*> **mode**

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
mode gre	Specifies the Generic Routing Encapsulation (GRE) mode.
mode udp	Specifies the User Datagram Protocol (UDP) mode

Defaults

The default mode is **gre**.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel gre-protocol” on page 109
- “interface tunnel ipsec” on page 110
- “interface tunnel revert” on page 120
- “interface tunnel udp-flow” on page 124
- “interface tunnel udp-port” on page 125
- “show interfaces tunnel” on page 294

Usage Guidelines

None.

Examples

To configure the tunnel, *Paris_London*, for UDP mode:

```
(config) # interface tunnel Paris_London mode udp
```

To reset the tunnel, *Paris_London*, to the default mode, GRE:

```
(config) # no interface tunnel Paris_London mode
```

interface tunnel mtu

Description

Use the **interface tunnel mtu** command to configure Maximum Transmission Unit (MTU) for this tunnel.

Use the **no** form of this command to reset the MTU for this tunnel to its default.

Syntax

interface tunnel <*tunnel name*> **mtu** <*MTU in bytes*>

no interface tunnel <*tunnel name*> **mtu**

Arguments

<*tunnel name*>	Specifies the name for this tunnel. The range is 700 to 2400.
<*MTU in bytes*>	Specifies the Maximum Transmission Unit (MTU) in bytes.

Defaults

The default MTU is **1500**.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel revert” on page 120
- “show interfaces tunnel” on page 294

Usage Guidelines

None.

Examples

None.

interface tunnel packet

Description

Use the **interface tunnel packet** command to configure packet options for this tunnel.

Use the **no** form of this command to negate or reset the packet options for this tunnel.

Syntax

interface tunnel <*tunnel name*> **packet coalesce** {**disable | enable**}

interface tunnel <*tunnel name*> **packet coalesce wait** <*TIME in msecs*>
no interface tunnel <*tunnel name*> **packet coalesce wait**

interface tunnel <*tunnel name*> **packet fec** {**disable | enable | auto**}

interface tunnel <*tunnel name*> **packet fec ratio** {**1:1 | 1:10 | 1:2 | 1:20 | 1:5**}
no interface tunnel <*tunnel name*> **packet fec ratio**

interface tunnel <*tunnel name*> **packet reorder wait** <*TIME in msec*>
no interface tunnel <*tunnel name*> **packet reorder wait**

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
coalesce {**disable** | **enable**}	Disables or enables packet coalescing for this tunnel.
coalesce wait <*TIME in msecs*>	Specifies the coalesce wait time in milliseconds. The value must be a number between 0 and 65535. Use the **no** form of this command to reset the coalesce wait time to its default.
fec {**disable** | **enable**}	Disables or enables the packet forwarding error correction (FEC) options.
fec auto	Configures the packet forwarding error correction (FEC) options to adjust automatically. When set, it auto-tunes up to the value specified by **fec ratio**.
fec ratio {**1:1 | 1:10 | 1:20 | 1:5 | 1:2**}	Sets the packet forwarding error correction (FEC) ratios to one of the available options: 1:1, 1:10, 1:20, 1:5, or 1:2. Use the **no** form of this command to reset the FEC ratio value to its default.
reorder wait <*TIME in msec*>	Configures the packet reorder wait time. Use the **no** form of this command to reset the packet reorder wait time to its default.

Defaults

The default packet coalesce wait time is 0 milliseconds.

The default packet reorder wait time is 0 milliseconds.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel admin” on page 102
- “interface tunnel control-packet” on page 105
- “interface tunnel create” on page 107
- “interface tunnel gre-protocol” on page 109
- “interface tunnel ipsec” on page 110
- “interface tunnel max-bandwidth” on page 112
- “interface tunnel min-bandwidth” on page 113
- “interface tunnel mode” on page 115
- “interface tunnel mtu” on page 117
- “interface tunnel packet” on page 118
- “interface tunnel revert” on page 120
- “interface tunnel threshold” on page 122
- “interface tunnel udp-flow” on page 124
- “interface tunnel udp-port” on page 125
- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

To reset the packet coalesce wait time for the tunnel, *big-pipe*, to the default value of 0 (zero):

```
<silver-peak> (config) # no interface tunnel big-pipe packet coalesce wait
```

interface tunnel revert

Description

Use the **interface tunnel revert** command to configure the default values to the factory settings.

Syntax

interface tunnel <*tunnel name*> **revert**

Arguments

<*tunnel name*>	Specifies the name of this tunnel.

Defaults

Factory defaults

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces tunnel” on page 294

Usage Guidelines

None.

Examples

None.

interface tunnel tag-name

Description

Use the **interface tunnel tag-name** command to apply a tag name to a tunnel.

Syntax

interface tunnel <*tunnel name*> **tag-name** <*tag name*>

Arguments

<*tunnel name*>	Specifies the name of this tunnel.
tag-name <*tag name*>	Specifies the tunnel by calling out the WAN port names at each end of the tunnel.

Defaults

Factory defaults

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces tunnel” on page 294

Usage Guidelines

None.

Examples

None.

interface tunnel threshold

Description

Use the **interface tunnel threshold** command to configure threshold options for this tunnel.

Syntax

interface tunnel <*tunnel name*> **threshold fastfail** {**disable | enable**}

interface tunnel <*tunnel name*> **threshold fastfail-wait** {**base-ms** <*wait time in milliseconds*> **| rtt-x** <*multiple of RTT*>}

interface tunnel <*tunnel name*> **threshold jitter** <*jitter in milliseconds*>

interface tunnel <*tunnel name*> **threshold latency** <*latency in milliseconds*>

interface tunnel <*tunnel name*> **threshold loss** <*loss in percentage*>

interface tunnel <*tunnel name*> **threshold retry-count** <*retry-count*>

Arguments

<*tunnel name*>	Specifies the name of this tunnel.
fastfail {**disable** | **enable**}	Disables or enables fast failover for this tunnel.
fastfail-wait base-ms <*wait time in milliseconds*>	Configures fast failover wait-times in milliseconds for this tunnel.
fastfail-wait rtt-x <*multiple of RTT*>	Configures fast failover wait-times in Return Trip Time (RTT) multiples for this tunnel.
jitter <*jitter in milliseconds*>	Specifies the jitter threshold for this tunnel in milliseconds.
latency <*latency in milliseconds*>	Specifies the latency threshold for this tunnel in milliseconds.
loss <*loss in percentage*>	Specifies the loss threshold for this tunnel in percentage.
retry-count <*retry-count*>	Specifies the number of retries.

Defaults

The default number of retries is 10.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

None.

interface tunnel udp-flow

Description

Use the **interface tunnel udp-flow** command to configure the number of UDP flows for this tunnel.

Use the **no** form of this command to reset the number of UDP flows for this tunnel to its default.

Syntax

interface tunnel <*tunnel name*> **udp-flow** < *flows*>

no interface tunnel <*tunnel name*> **udp-flow**

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
<*flows*>	Sets the number of UDP flows, between 1 and 1024.

Defaults

The default number of flows is *256*.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel revert” on page 120
- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

To set the maximum number of UDP flows for the tunnel, *HastaLaVista*:

```
(config) # interface tunnel HastaLaVista udp-flow 1024
```

To reset the number of UDP flows to the default of 256 for the tunnel, *HastaLaVista*:

```
(config) # no interface tunnel HastaLaVista udp-flow
```

interface tunnel udp-port

Description

Use the **interface tunnel udp-port** command to configure the UDP destination port for this tunnel.

Use the **no** form of this command to reset the UDP destination port for this tunnel to its default.

Syntax

interface tunnel <*tunnel name*> **udp-port** <*UDP destination port*>

no interface tunnel <*tunnel name*> **udp-port**

Arguments

<*tunnel name*>	Specifies the name for this tunnel.
<*UDP destination port*>	Specifies the UDP destination port for this tunnel.

Defaults

The default UDP destination port is *4163*.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface tunnel create” on page 107
- “interface tunnel gre-protocol” on page 109
- “interface tunnel ipsec” on page 110
- “interface tunnel mode” on page 115
- “interface tunnel revert” on page 120
- “interface tunnel udp-flow” on page 124
- “show interfaces tunnel” on page 294

Usage Guidelines

To see a list of the available tunnel names you may use, enter the following command:

```
<silver-peak> (config) # interface tunnel ?
```

Examples

To make UDP port 407 the destination for the tunnel, *MataHari*:

```
<silver-peak> (config) # interface tunnel MataHari udp-port 407
```

interface vrrp

Description

Use the **interface vrrp** commands to configure network interface Virtual Router Redundancy Protocol (VRRP) instances.

Syntax

interface <*interface name*> **vrrp** <*1–255*> **admin** {**down | up**}
no interface <*interface name*> **vrrp** <*1–255*>

interface <*interface name*> **vrrp** <*1–255*> **authentication** <*text*>
no interface <*interface name*> **vrrp** <*1–255*> **authentication**

interface <*interface name*> **vrrp** <*1–255*> **debug action {dump_info | clear_stats | mem_stats}**

interface <*interface name*> **vrrp** <*1–255*> **debug packet_trace**
no interface <*interface name*> **vrrp** <*1–255*> **debug packet_trace**

interface <*interface name*> **vrrp** <*1–255*> **description** <*text*>
no interface <*interface name*> **vrrp** <*1–255*> **description**

interface <*interface name*> **vrrp** <*1–255*> **ip** <*IP address*>

interface <*interface name*> **vrrp** <*1–255*> **preempt**
no interface <*interface name*> **vrrp** <*1–255*> **preempt**

interface <*interface name*> **vrrp** <*1–255*> **priority** <*1–254*>
no interface <*interface name*> **vrrp** <*1–255*> **priority**

interface <*interface name*> **vrrp** <*1–255*> **timers advertise** <*1–255*>
no interface <*interface name*> **vrrp** <*1–255*> **timers advertise**

interface <*interface name*> **vrrp** <*1–255*> **timers holddown** <*1–255*>
no interface <*interface name*> **vrrp** <*1–255*> **timers holddown**

Arguments

<*interface name*>	Specifies the name of this interface. Currently, **wan0** is the sole available interface.
vrrp <*1-255*>	The ID for the VRRP. Valid numbers are from 1 through 255, inclusive.
admin down	Disables the VRRP instance.
admin up	Enables the VRRP instance.
authentication <*text*>	Configures an authentication string. This text string is limited to a maximum of eight characters. Use the **no** form of this command to delete the authentication string.

debug action {dump_info | clear_stats | mem_stats}	For the VRRP instance specified: • **dump_info** – dumps all info into a log file • **clear_stats** – clears debug statistics • **mem_stats** – creates a log file of all memory usage information
debug packet_trace	Enables a VRRP packet trace to a log file. Use the **no** form of this command to disable the dumping of the Rx/Tx VRRP packet to a log file.
description <*text*>	Sets the VRRP description string. Use the **no** form of this command to delete the VRRP description string.
ip <*IP address*>	Creates a VRRP router or modifies a VRRP virtual IP address.
preempt	Enables preemption of the lower-priority Master. Use the **no** form of this command to disable preemption of lower priority Master.
priority <*1-254*>	Sets the priority of this appliance. Use the **no** form of this command to reset priority level to the default value of 128.
timers advertise <*1-255*>	Specifies the advertisement interval in seconds. Use the **no** form of the command to reset to the the default value of 1 second.
timers holddown <*1-255*>	Sets the wait time (in seconds) before asserting ownership. Use the **no** form of this command to reset hlddown to the default value of 10.

Defaults

The default priority is 128.

The default advertisement interval is 1 second.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces” on page 287
- “show interfaces vrrp” on page 297
- “show vrrp” on page 363

Usage Guidelines

The **interface vrrp** commands are only valid when the appliance is in router mode. Also, they only support the wan0 interface.

To see a list of the available interface names you may use, enter the following command:

```
<silver-peak> (config) # interface ?
```

Examples

To delete the vrrp authentication strong for the VRRP ID, 7:

```
(config) # no interface wan0 vrrp 7 authentication
```

To reset the appliance priority level to the default value for the VRRP ID, 243:

```
(config) # no interface wan0 vrrp 243 priority
```

interface wan-if

Description

Use the **interface wan-if** command to specify that this interface only allow WAN traffic when deploying the appliance in in-line router mode.

Use the **no** form of this command to remove the limitation from this interface.

Syntax

interface <*interface name*> **wan-if**

no interface <*interface name*> **wan-if**

Arguments

<*interface name*>	Specifies the name of this interface.
wan-if	Specifies that the interface only allow WAN traffic.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “interface lan-if” on page 95
- “show interfaces” on page 287

Usage Guidelines

Only used for in-line router mode.

Examples

None.

ip datapath route

Description

Use the **ip datapath route** command to configure next-hop address(es) for LAN-side networks that are not directly connected to a bridge-mode appliance.

Use the **no** form of **ip datapath route** command to remove datapath static route.

Syntax

ip datapath route <*network prefix*> <*netmask or mask length*> < *next hop IP address*>

ip datapath route <*network prefix*> <*netmask or mask length*> < *next hop IP address*> **metric** <*1..255*> [**if** <*interface name*>]

no ip datapath route <*network prefix*> <*netmask or mask length*> [< *destination*>]

Arguments

<*network prefix*>	Specifies network prefix. This has the format, nnn.nnn.nnn.0.
<*netmask or mask length*>	Specifies netmask, or the mask length in slash notation.
<*next hop IP address*>	Specifies next-hop IP address.
metric <*1-255*>	Specifies datapath static route metric. Specifies an integer cost metric (ranging from 1 to 255) for the route, which is used when choosing among multiple routes in the routing table that most closely match the destination address of a packet being forwarded. The route with the lowest metric is chosen. The metric can reflect the number of hops, the speed of the path, path reliability, path throughput, or administrative properties.
if <*interface name*>	Specifies the datapath static route interface.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ip default-gateway” on page 132
- “ip domain-list” on page 133
- “ip mgmt-ip” on page 135
- “ip route” on page 137
- “show ip” on page 298

Usage Guidelines

None.

Examples

To configure a datapath route from the 10.10.10.0 network to the next-hop IP, 172.11.15.13, use one of the following:

```
(config) # ip datapath route 10.10.10.0 /24 172.11.15.13
(config) # ip datapath route 10.10.10.0 255.255.255.0 172.11.15.13
```

ip default-gateway

Description

Use the **ip default-gateway** command to set the default route to the specified next-hop or interface.

Use the **no** form of this command to remove the current default route.

Syntax

ip default-gateway <*next-hop IP address or interface name*> [< *interface name*>]

no ip default-gateway

Arguments

<*next-hop IP address or interface name*>	Specifies the IP address for the default gateway route.
<*interface name*>	Either **mgmt0** or **mgmt1**. The interface named here forces the next-hop to use the named management interface, binding the next-hop.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ip datapath route” on page 130
- “ip mgmt-ip” on page 135
- “ip route” on page 137
- “show ip” on page 298

Usage Guidelines

None.

Examples

To set the default gateway to 10.10.4.5:

```
(config) # ip default-gateway 10.10.4.5
```

ip domain-list

Description

Use the **ip domain-list** command to add a domain name to use when resolving hostnames.

Use the **no** form of this command to remove a domain name.

Syntax

ip domain-list <*domain name*>

no ip domain-list <*domain name*>

Arguments

<*domain name*>	Defines a domain name. For example, *silver-peak*.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ip host” on page 134
- “ip name-server” on page 136
- “show hosts” on page 284

Usage Guidelines

None.

Examples

To add the domain name, “silver-peak”:

```
(config) # ip domain-list silver-peak
```

ip host

Description

Use the **ip host** command to configure a static hostname or IP address mapping.

Use the **no** form of this command to remove static hostname or IP address mapping.

Syntax

ip host <*host name*> <*IP address*>

no ip host <*host name*> <*IP address*>

Arguments

<*host name*>	Defines a static host name for the IP host.
<*IP address*>	Specifies an IP address for the IP host.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ip domain-list” on page 133
- “ip name-server” on page 136
- “show hosts” on page 284
- “show ip” on page 298

Usage Guidelines

Useful for a URL definition where you want to use a name instead of an IP address.

Examples

To be able to use the name, “redshoes”, for the IP address, 10.10.10.4:

```
(config) # ip host redshoes 10.10.10.4
```

ip mgmt-ip

Description

Use the **ip mgmt-ip** command to configure a LAN IP address for management traffic.

Use the **no** form of this command to remove the LAN IP address configuration for management traffic.

Syntax

ip mgmt-ip *<IP address>*

no ip mgmt-ip

Arguments

<IP address>	Specifies an IP address for the IP host.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ip datapath route” on page 130
- “ip default-gateway” on page 132
- “ip route” on page 137
- “show hosts” on page 284
- “show ip” on page 298

Usage Guidelines

None.

Examples

None.

ip name-server

Description

Use the **ip name-server** command to add a DNS server.

Use the **no** form of this command to remove a DNS server.

Syntax

ip name-server <*IP address*>

no ip name-server <*IP address*>

Arguments

<*IP address*>	Specifies an IP address for the DNS server.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ip domain-list” on page 133
- “ip host” on page 134
- “show hosts” on page 284

Usage Guidelines

The system allows a maximum of three DNS servers and tells you when you try to request more.

The appliance tries to access DNS servers, as needed, in the order they were configured. Also, if you remove the first host in a list of three, the second host becomes the first host. A newly added host always goes to the bottom of the list.

Examples

To add a Domain Name Server with the IP address, 172.30.56.89:

```
(config) # ip name-server 172.30.56.89
```

ip route

Description

Use the **ip route** command to add a static route. Static routes help the appliance route management traffic out of the appliance to different subnets.

Use the **no** form of this command to remove a static route.

Syntax

ip route <*network prefix*> <*netmask or mask length*> <*next hop IP address or interface name*>

ip route <*network prefix*> <*netmask or mask length*> <*next hop IP address or interface name*> [<*interface name*>]

no ip route <*network prefix*> <*netmask*> [<*destination*>]

Arguments

<*network prefix*>	Specifies a network prefix to the IP route. This has the format, nnn.nnn.nnn.0.
<*netmask or mask length*>	Specifies a netmask or a mask length in slash notation.
<*next hop IP address or interface name*>	Specifies the next-hop IP address for the IP route.
<*next hop IP address or interface name*> <*interface name*>	Binds the next-hop to the named interface, in this case, either **mgmt0** or **mgmt1**.
<*destination*>	Specifies the final IP address of the IP route.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ip datapath route” on page 130
- “ip default-gateway” on page 132
- “ip domain-list” on page 133
- “ip host” on page 134
- “ip mgmt-ip” on page 135
- “ip name-server” on page 136
- “show hosts” on page 284
- “show ip” on page 298

Usage Guidelines

None.

Examples

To define a static route for an internal subnet with IP address 172.16.15.0 and netmask 255.255.255.0 using an internal router with IP address 172.16.30.7:

```
(config) # ip route 172.11.15.0 /24 172.11.30.7
```

nat-map

Description

The appliance can perform ***source network address translation*** (Source NAT or SNAT) on inbound or outbound traffic.

Two use cases illustrate the need for NAT:

1 **Inbound NAT**. The appliance automatically creates a source NAT map when retrieving subnet information from the Silver Peak Cloud portal. This ensures that traffic destined to SaaS servers has a return path to the appliance from which that traffic originated.

2 **Outbound NAT**. The appliance and server are in the cloud, and the server accesses the internet. For example, a Citrix thin client accesses its cloud-based server, and the server accesses the internet.

For deployments in the cloud, ***best practice is to NAT all traffic*** — either inbound (WAN-to-LAN) or outbound (LAN-to-WAN), depending on the direction of initiating request. This avoids black-holing that can result from cloud-specific IP addressing requirements.

- Enabling NAT on inbound traffic applies NAT policies to pass-through traffic as well as optimized traffic, ensuring that black-holing doesn't occur. Enabling NAT on outbound traffic only applies to pass-through traffic.
- If Fallback is enabled, the appliance moves to the next IP (if available) when ports are exhausted on the current NAT IP.

In general, when applying NAT policies, configure separate WAN and LAN interfaces to ensure that NAT works properly. You can do this by deploying the appliance in Router mode in-path with two (or four) interfaces.

There are two types of NAT policies:

- **Dynamic** – created automatically by the system for inbound NAT when the ***SaaS Optimization*** feature is enabled and SaaS service(s) are selected for optimization. The appliance polls the Silver Peak Unity Cloud Intelligence service for a directory of SaaS services, and NAT policies are created for each of the subnets associated with selected SaaS service(s), ensuring that traffic destined for servers in use by those SaaS services has a return path to the appliance.
- **Manual** – created by the administrator for specific IP addresses / ranges or subnets. When assigning priority numbers to individual policies within a NAT map, first view dynamic policies to ensure that the manual numbering scheme doesn't interfere with dynamic policy numbering (that is, the manually assigned priority numbers cannot be in the range: 40000-50000). The default (no-NAT) policy is numbered 65535.

NAT maps are comprised of ordered entries. Each map entry consists of a *match* statement paired with a *set* action. Set actions are specific to the type of map.

A NAT map entry can match traffic that satisfies either a pre-defined ACL or any of the following attributes:

- ICMP or IP Protocol
- Source IP Address / Subnet
- Destination IP Address / Subnet
- Application (standard or user-defined, or a user-defined application group)
- Source Port Number
- Destination Port Number
- DSCP value
- VLAN

If you want to reuse the same match criteria in more than one map, you can pre-define ACLs, which are, essentially, reusable match statements.

Set actions are specific to the type of map. A NAT map has set actions for the following features:

- NAT type
- NAT direction
- NAT IP
- Fallback

Map entries are ordered according to their assigned *priorities*. Priorities identify, as well as order, entries within a map. Across entries, all priority values must be unique (in other words, no two *entries* in a given map can have the same priority value). match

In the following example, we'll add a new entry, with a priority of *50*, to the default map, *map1*. The first statement matches all traffic associated with the application, *AOL*. The second statement causes the source address and the source port to change in the IP header of that inbound traffic:

```
(config) # nat-map map1 50 match app aol
(config) # nat-map map1 50 set nat-type source-nat direction inbound
```

If you enter a new priority statement for an existing map, the CLI adds that entry to the map. However, if the map already has a *match* or *set* statement with the same priority, the new entry overwrites the previous one (and the CLI does not provide a warning).

If you want to create a new map, the CLI creates the map the first time you name it in a match statement.

Every map automatically includes a default entry with the priority, 65535, the highest possible number.

By default, one map is always active. You can change the active map at any time, simply by activating a different map.

See Also

See the following related commands:

- “nat-map match” on page 142
- “nat-map set” on page 144
- “nat-map activate” on page 146
- “nat-map comment” on page 147
- “no nat-map” on page 148
- “nat-map modify-priority” on page 150
- “show nat-map” on page 314

nat-map match

Description

Use the **nat-map match** command to create a NAT map entry that uses match criteria to delineate traffic. Also use this command to change the matching conditions associated with an existing entry.

Syntax

nat-map *<NAT map name> <priority value>* **match acl** *<ACL name>*

nat-map *<NAT map name> <priority value>* **match app** *<application>*

nat-map *<NAT map name> <priority value>* **match dscp {any |** *<dscp value>***}**

nat-map *<NAT map name> <priority value>* **match protocol icmp {***<source IP address and mask length>* **| any | any-ipv4 | any-ipv6} {***<dest IP address and mask length>* **| any | any-ipv4 | any-ipv6} [dscp {any |** *<dscp value>***}] [vlan** {**any** | *<1..4094>* | *<interface>.tag* | *<any>.tag* | *<interface>.any* | *<interface>.native*}**]**

nat-map *<NAT map name> <priority value>* **match protocol ip {***<source IP address and mask length>* **| any | any-ipv4 | any-ipv6} {***<dest IP address and mask length>* **| any | any-ipv4 | any-ipv6} [app** *<application name>***] [dscp {any |** *<dscp value>***}] [vlan** {**any** | *<1..4094>* | *<interface>.tag* | *<any>.tag* | *<interface>.any* | *<interface>.native*}**]**

Arguments

<NAT map name>	Specifies the name of the NAT map.
<priority value>	Designates a priority value for the map entry. Acceptable values are from *1* to *65534*. By default, the appliance reserves *65535* for the default entry.
match acl *<ACL name>*	Creates an entry that uses an existing ACL to match traffic. Also use this command to change the ACL associated with an existing entry.
match app *<application name>*	Creates an entry that uses a built-in or user-defined application—or an application group—to match traffic. Also use this command to change the application associated with an existing entry.
match dscp {*<dscp value>* | **any**}	Creates or modifies an entry that matches traffic with a specific DSCP marking. You can use any of the following values: • af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs1, cs2, cs3, cs4, cs5, cs6, cs7, *or* ef. • **any** is a wildcard.
match protocol icmp {*<source IP address and mask length>* **| any | any-ipv4 | any-ipv6}**	Creates or modifies a NAT map that matches the ICMP protocol. • **any** matches any IPv4 or IPv6 address • **any-ipv4** matches any IPv4 address • **any-ipv6** matches any IPv6 address

match protocol ip {*<source IP address and mask length>* | **any | any-ipv4 | any-ipv6}**	Creates or modifies a NAT map that matches the IP protocol. • **any** matches any IPv4 or IPv6 address • **any-ipv4** matches any IPv4 address • **any-ipv6** matches any IPv6 address
match vlan {**any** | *<1..4094>* | *<interface>.tag* | *<any>.tag* | *<interface>.any* | *<interface>.native*}	Creates or modifies an entry that matches an interface and 802.1q VLAN tag. The available values include: • *<1..4094>* the number assigned to a VLAN • <interface>.tag as in **lan0.10** • <any>.tag as in **any.10** • <interface>.any as in **lan0.any** • *<interface>.native* as in **lan0.native** • **any** is a wildcard.
<source IP address and mask length>	Specifies the source IP address and netmask in slash notation. For example, 192.1.2.0/24 or 2001:db8::/32
<destination IP address and mask length>	Specifies the destination IP address and netmask in slash notation. For example, 192.1.2.0/24 or 2001:db8::/32.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “nat-map” on page 139
- “nat-map set” on page 144
- “nat-map activate” on page 146
- “nat-map comment” on page 147
- “no nat-map” on page 148
- “nat-map modify-priority” on page 150
- “show nat-map” on page 314

Usage Guidelines

None.

Examples

None.

nat-map set

Description

Use the **nat-map set** command specifies or modifies an entry's action. You cannot create a **set** command for an entry until you first issue a **match** command.

Syntax

nat-map <*NAT map name*> <*priority value*> **set nat-type source-nat direction {inbound | outbound | none}**

nat-map <*NAT map name*> <*priority value*> **set nat-type source-nat direction inbound nat-ip {**<*interface IP address*>** | auto | tunnel_endpoint} fallback {enable | disable}**

nat-map <*NAT map name*> <*priority value*> **set nat-type source-nat direction outbound nat-ip {**<*interface IP address*>** | auto} fallback {enable | disable}**

nat-map <*NAT map name*> <*priority value*> **set nat-type source-nat direction none nat-ip {**<*interface IP address*>** | auto} fallback {enable | disable}**

nat-map <*NAT map name*> <*priority value*> **set nat-type no-nat direction inbound nat-ip {**<*interface IP address*>** | auto | tunnel_endpoint} fallback {enable | disable}**

nat-map <*NAT map name*> <*priority value*> **set nat-type no-nat direction outbound nat-ip {**<*interface IP address*>** | auto} fallback {enable | disable}**

nat-map <*NAT map name*> <*priority value*> **set nat-type no-nat direction none nat-ip {**<*interface IP address*>** | auto} fallback {enable | disable}**

Arguments

nat-map <*NAT map name*>	Specifies the name of the NAT map.
<*priority value*>	Designates a priority value for the map entry. Acceptable values are from *1* to *65534*. By default, the appliance reserves *65535* for the default entry.
set	Configures the NAT map with the arguments that follow.
nat-type	Specifies the NAT type.
source-nat	Specifies the Source NAT on traffic coming into the LAN.
no-nat	Disables NAT on all traffic.
direction	Specifies the NAT direction: • **inbound** Applies NAT to traffic coming into LAN. • **outbound** Applies NAT to traffic going out into WAN. • **none** Disables NAT.
nat-ip <*interface IP address*>	Specifies the NAT IP address. To display the existing interface addresses, you can type, **nat-ip ?**
nat-ip {auto | tunnel_endpoint}	Specifies how the system should choose the NAT IP address.

fallback enable	Specifies fallback to the next available NAT IP address upon port exhaustion with the current NAT IP address.
fallback disable	Specifies not to fallback to the next available NAT IP address upon port exhaustion.

Defaults

The default is **no** network address translation.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “nat-map” on page 139
- “nat-map match” on page 142
- “nat-map activate” on page 146
- “nat-map comment” on page 147
- “no nat-map” on page 148
- “nat-map modify-priority” on page 150
- “show nat-map” on page 314

Usage Guidelines

You cannot create a **set** command for an entry until you first issue a **match** command. And, until you create a **set** command, no Set Actions exist for that entry’s priority.

Usage Guidelines

None.

Examples

None.

nat-map activate

Description

Use the **nat-map activate** command to activate an inactive NAT map.

Syntax

nat-map <*NAT map name*> **activate**

Arguments

<*nat map name*>	Specifies which existing, inactive NAT map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “nat-map” on page 139
- “nat-map match” on page 142
- “nat-map set” on page 144
- “nat-map comment” on page 147
- “no nat-map” on page 148
- “nat-map modify-priority” on page 150
- “show nat-map” on page 314

Usage Guidelines

Only one NAT map can be active at a time. The Silver Peak appliance has a default NAT map, *map1*, that’s active until you create and activate a new NAT map.

Usage Guidelines

None.

Examples

None.

nat-map comment

Description

Use the **nat-map comment** command to add a comment for a specified NAT map entry.

Syntax

nat-map *<NAT map name>* *<priority value>* **comment**

Arguments

<NAT map name>	Specifies the name of the NAT map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “nat-map” on page 139
- “nat-map match” on page 142
- “nat-map set” on page 144
- “nat-map activate” on page 146
- “no nat-map” on page 148
- “nat-map modify-priority” on page 150
- “show nat-map” on page 314

Usage Guidelines

None.

Examples

None.

no nat-map

Description

Use the **no nat-map** command to delete a Network Address Translation (NAT) map or a specific priority entry from a NAT map.

Syntax

no nat-map <*nat map name*>

no nat-map <*nat map name*> <*priority value*>

Arguments

<*nat map name*>	Specifies which NAT map.
<*priority value*>	Designates a priority value for the NAT map entry. Acceptable values are from 1 to 65534. By default, the appliance reserves 65535 for the default entry.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “nat-map” on page 139
- “nat-map match” on page 142
- “nat-map set” on page 144
- “nat-map activate” on page 146
- “nat-map comment” on page 147
- “nat-map modify-priority” on page 150
- “show nat-map” on page 314

Usage Guidelines

You can only delete a NAT map if it’s inactive. Therefore, to delete the active NAT map, you must first activate a different NAT map. For example:

```
(config) # nat-map map3 activate
(config) # no opt-map fred
```

You can also delete a specific entry in a NAT map by using the **no nat-map** command and specifying a priority value. For example, the following statement deletes the priority *100* entry (*match* and *set* statements) from the NAT map, *fred*:

```
(config) # no nat-map fred 100
```

nat-map modify-priority

Description

Use the **nat-map modify-priority** commands to modify an existing NAT map priority value.

Syntax

nat-map <*NAT map name*> <*priority value*> **modify-priority** <*priority value*>

Arguments

<*nat map name*>	Specifies an existing NAT map.
<*current priority value*>	Specifies the current priority value for the entry you want to change.
modify-priority <*new priority value*>	Designates the new priority for this entry. This new priority value must be unique and between 1 to 65534.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “nat-map” on page 139
- “nat-map match” on page 142
- “nat-map set” on page 144
- “nat-map activate” on page 146
- “nat-map comment” on page 147
- “no nat-map” on page 148
- “show nat-map” on page 314

Usage Guidelines

If you try renumber the entry to a priority number that already exists, the CLI informs you that that’s the case and that you can’t make that modification.

Examples

To change the priority of entry 40 to be 60 for the map, *map1*:

```
(config) # nat-map map1 40 modify-priority 60
```

ntp

Description

Use the **ntp** commands to configure Network Time Protocol (NTP) on the appliance.

Use the **no** forms of the command to negate certain NTP options.

Syntax

ntp {**disable | enable**}
no ntp {**disable | enable**}

ntp server <*IP address*>
no ntp server <*IP address*>

ntp server <*IP address*> **ping**

ntp server <*IP address*> **version** <*version number*>

ntp server <*IP address*> **disable**
no ntp server <*IP address*> **disable**

ntp status

Arguments

disable	Disables NTP on the appliance.
enable	Enables NTP on the appliance.
server <*IP address*>	Configures the NTP server node with the default NTP version number. Use the **no** form of this command to remove this NTP server.
server <*IP address*> **ping**	Checks the connectivity of this NTP server.
server <*IP address*> **version** <*version number*>	Configures the NTP server node and specifies the NTP version number of this server.
server <*IP address*> **disable**	Temporarily disables this NTP server. Use the **no** form of this command to reenable this NTP server.
status	Shows the status of NTP servers.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ntpdate” on page 153
- “show ntp” on page 316

Usage Guidelines

Use the **no** form of **ntp enable** and **ntp disable** negate the NTP option. In other words, to disable NTP, you can use the **no ntp enable**; to enable ntp, use the **no ntp disable**.

To remove an NTP server with the address, 170.10.10.4:

```
<silver-peak> (config) # no ntp server 170.10.10.4
```

Usage Guidelines

None.

Examples

None.

ntpdate

Description

Use the **ntpdate** command to set the system clock once from a remote server using Network Time Protocol (NTP).

Syntax

ntpdate <*IP address*>

Arguments

<*IP address*>	Specifies the IP address of the remote NTP server.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “ntp” on page 151
- “show ntp” on page 316

Usage Guidelines

None.

Examples

To synchronize the server to the NTP server, 216.27.190.202:

```
(config) # ntpdate 216.27.190.202
```

opt-map

Description

The Silver Peak appliance allows you to configure how your traffic is optimized by creating *optimization maps*. Optimization maps make it easy for you to explicitly filter for the traffic you want to optimize, and then apply an action to that flow.

Optimization maps — like Route maps and QoS maps — are made up of ordered entries. Each map entry consists of a *match* statement paired with a *set* action. Set actions are specific to the type of map.

A map entry can match traffic that satisfies either a pre-defined ACL or any of the following attributes:

- Protocol
- Source IP Address / Subnet
- Destination IP Address / Subnet
- Source Port Number
- Destination Port Number
- Application (standard or user-defined, or a user-defined application group)
- DSCP value
- VLAN

If you want to reuse the same match criteria in more than one map, you can pre-define ACLs, which are, essentially, reusable match statements.

Set actions are specific to the type of map. An optimization map has set actions related to optimization and compression features:

- Network Memory
- IP header compression
- Payload compression
- TCP acceleration
- Protocol acceleration (CIFS, SSL, SRDF)

Map entries are ordered according to their assigned *priorities*. Priorities identify, as well as order, entries within a map. Across entries, all priority values must be unique (in other words, no two *entries* in a given map can have the same priority value).

In the following example, we'll add a new entry, with a priority of *50*, to the default map, *map1*. The first statement matches all traffic associated with the application, *AOL*. The second statement enables CIFS acceleration as the action for that traffic:

```
(config) # opt-map map1 50 match app aol
(config) # opt-map map1 50 set cifs enable
```

If you enter a new priority statement for an existing optimization map, the CLI adds that entry to the optimization map. However, if the map already has a *match* or *set* statement with the same priority, the new entry overwrites the previous one (and the CLI does not provide a warning).

If you want to create a new optimization map, the CLI creates the map the first time you name it in a match statement.

Every optimization map automatically includes a default entry with the priority, 65535, the highest possible number. That default entry applies all the optimization and compression features to all traffic subject to the optimization map.

By default, optimization maps have additional entries that enable protocol-specific optimizations for CIFS, SSL, iSCSI, SRDF, Citrix, and their common ports.

By default, one optimization map is always active. You can change the active map at any time, simply by activating a different map.

See Also

See the following related commands:

- “opt-map match” on page 156
- “opt-map set” on page 161
- “opt-map activate” on page 164
- “no opt-map” on page 166
- “opt-map modify-priority” on page 167
- “show opt-map” on page 317

opt-map match

Description

Use the **opt-map match** command to create an optimization map entry that uses match criteria to delineate traffic. Also use this command to change the matching conditions associated with an existing entry.

Syntax

opt-map *<opt map name>* *<priority value>* **match acl** *<ACL name>*

opt-map *<opt map name>* *<priority value>* **match app** {*<application name>* | *<application group>*}

opt-map *<opt map name>* *<priority value>* **match dscp** {*<dscp value>* | **any**}

opt-map *<opt map name>* *<priority value>* **match protocol** *<IP protocol number or name>* {*<source ip address/netmask>* | **any**} {*<destination ip address/netmask>* | **any**} [**dscp** {*<dscp value>* | **any**}] [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

opt-map *<opt map name>* *<priority value>* **match protocol ip** {*<source ip address/netmask>* | **any**} {*<destination ip address/netmask>* | **any**} [**app** {*<application name>* | **any**}] [**dscp** {*<dscp value>* | **any**}] [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

opt-map *<opt map name>* *<priority value>* **match protocol** {**tcp** | **udp**} {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [{*<source port number>* | **any**} {*<destination port number>* | **any**}] [**dscp** {*<dscp value>* | **any**}] [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

opt-map *<opt map name>* *<priority value>* **match vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}

Arguments

opt map <*opt map name*>

Specifies which optimization map. If the name doesn't exist, the CLI creates it.

<*priority value*>

Designates a priority value for the optimization map entry. Acceptable values are from *1* to *65534*. By default, the appliance reserves *65535* for the default entry.

match acl <*ACL name*>

Creates an entry that uses an existing ACL to match traffic. Also use this command to change the ACL associated with an existing entry.

match app <*application name*>

Creates an entry that uses a built-in or user-defined application—or an application group—to match traffic. Also use this command to change the application associated with an existing entry.

For a list of built-in applications, see Table 3-1, "Applications on the Silver Peak Appliance," on page 159.

match dscp {<*dscp value*> | **any**}

Creates or modifies an entry that matches traffic with a specific DSCP marking. You can use any of the following values:

- af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs1, cs2, cs3, cs4, cs5, cs6, cs7, *or* ef.
- **any** is a wildcard.

any

any is a wildcard.

match protocol <*IP protocol number or name*>

Creates or modifies an entry that matches traffic with a specific protocol that is **NOT** named specifically as *ip*, *tcp*, or *udp*:

- The available IP protocol numbers include 1 through 254.
- The available IP protocol names include:

ah	egp	eigrp	encap
esp	etherip	fc	gre
icmp	idpr	idpr-cmtp	idrp
igmp	igp	ip-comp	ip-mobility
ipip	ipip4	ipx-in-ip	irtp
iso-ip	iso-tp4	I2tp	mhrp
ospf	pim	rdp	rsvp
sctp	tlsp	vrrp	

match protocol ip	Creates or modifies an entry that matches specific IP addresses. • When you specify **protocol ip**, the assumption is that you are allowing *any* IP protocol. In that case, you also need to specify an application (or application group). If you don't, the CLI defaults to specifying **any** application. • If you don't choose to specify a DSCP value in the full command, then the CLI defaults to specifying **any** DSCP value in the policy entry.
match protocol {**tcp** | **udp**}	Creates or modifies an entry that matches specific TCP or UDP addresses. • If you don't choose to specify source and destination ports in the full command, then the CLI defaults to specifying **0:0** (any source port and any destination port) in the policy entry. • If you don't choose to specify a DSCP value in the full command, then the CLI defaults to specifying **any** DSCP value in the policy entry.
match vlan {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}	Creates or modifies an entry that matches an interface and 802.1q VLAN tag. The available values include: • *<1..4094>* the number assigned to a VLAN • <interface.tag>as in **lan0.10** • <any.tag> as in **any.10** • <interface.any>as in **lan0.any** • *<interface.native>*as in **lan0.native** • **any** is a wildcard.
<source ip address/netmask>	Specifies the source IP address and netmask in slash notation. For example, *10.2.0.0 0.0.255.255* should be entered as *10.2.0.0/16.*
<destination ip address/netmask>	Specifies the destination IP address and netmask in slash notation. For example, *10.2.0.0/16.*

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- "opt-map" on page 154
- "opt-map set" on page 161
- "opt-map activate" on page 164
- "no opt-map" on page 166
- "opt-map modify-priority" on page 167
- "show opt-map" on page 317

Usage Guidelines

You can specify one of the following standard (built-in) applications (alphabetically left to right):

Table 3-1 Applications on the Silver Peak Appliance

3par	aol	aol_im	aspera
avamar	backweb	bit_torrent	bluearc
celerra	centera	cifs_smb	cisco_skinny
citrix	commvault	cuseeme	cvs
datadomain	ddm	ddm_ssl	dns
doom	doubletake	echo	edonkey
fcip	filenet	ftp	ftps
gnutella	h_323	hadoop	hostname
http	https	ibm_db2	ifcp
imap	imap4s	ipsec	irc
irc_ssl	isakmp	iscsi	isns
ivisit	kazaa	kerberos	l2tp
ldap	ldaps	lotus_cc_mail	lotus_notes
matip	ms_exchange	ms_media	ms_messenger
ms_odbc	ms_ole	ms_rpc	ms_sql
ms_terminal_services	ms_zone	nameserver	ndmp
netbios	nfs	nntp	nntps
novell	ntp	openwindows	oracle
pcanywhere	pcmail	pcoip	peoplesoft
pop	pop3s	pptp	printer
quake	recoverpoint	rlogin	routing
rtcp	rtsp	sap	sgcp
sgmp	shell	silverpeak_comm	silverpeak_gms
silverpeak_internal	silverpeak-peer	silverpeak-tcpperf	sip
sip_tls	smtp	smtps	snapmirror
snmp	sql	srdf	ssh
sshell	sun_rpc	sybase	syslog
t_120	tacacs	telnet	telnets
tftp	timbuktu	time	uucp
vnc	vplex	vvr	xwindows
yahoo_games	yahoo_im		

For each **opt-map match** command with a given priority, you must create an **opt-map set** command(s) with the same priority. But, you cannot create the **set** command without having first created the **match** command.

Examples

To create a match criteria with a priority of "100" for the map, "express", that filters for all traffic coming from the LAN with a DSCP marking of "best effort":

```
(config) # opt-map express 100 match dscp be
```

To create a match criteria with a priority of "70" for the map, "express", that filters for the application group, "secure":

```
(config) # opt-map express 70 match app secure
```

To create a match criteria with a priority of "20" for "map2" that filters for all AOL traffic that's headed from the LAN to 172.34.8.0:

```
(config) # opt-map map2 20 match protocol ip any 172.34.8.0 aol
```

Since you haven't specified a DSCP value, the criteria will include all DSCP values, as if you had written it as follows:

```
(config) # opt-map map2 20 match protocol ip any 172.34.8.0 aol any
```

To create a match criteria with a priority of "30" for the map, "arthouse" that filters for all UDP traffic coming from port 41 and having a destination of 122.33.44.0/24:

```
(config) # opt-map arthouse 30 match protocol udp any 122.33.4.0/24 41:0
```

Since you haven't specified a DSCP value, the criteria will include all DSCP values, as if you had written it as follows:

```
(config) # opt-map arthouse 30 match protocol udp any 122.33.4.0/24 41:0
any
```

To create a match criteria with a priority of "10" for the map, "waldo" that filters for all Interior Gateway Protocol (IGP) traffic that has a DSCP marking of "af11":

```
(config) # opt-map waldo 10 match protocol igp any any dscp af11
```

opt-map set

Description

The **opt-map set** command specifies or modifies an entry's set action. You cannot create a **set** command for an entry until you first issue a **match** command.

Syntax

opt-map <*opt map name*> <*priority value*> **set header** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set network-memory** {**disable** | **balanced | min-latency | max-reduction**}

opt-map <*opt map name*> <*priority value*> **set payload** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set tcp** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set protocol-specific** {**none** | **cifs** | **ssl** | **srdf** | **citrix**} [**network-memory** {**disable** | **balanced | min-latency | max-reduction**}]

opt-map <*opt map name*> <*priority value*> **set protocol-specific** {**none** | **cifs** | **ssl** | **srdf** | **citrix**} **network-memory** {**disable** | **balanced | min-latency | max-reduction**} **payload** {**enable** | **disable**} **header** {**enable** | **disable**} **tcp** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp adjust-mss-to-mtu** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp auto-reset-flows** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp congestion-control** {**standard** | **optimized | aggressive**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp ip-black-listing** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp keep-count** <*threshold*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp keep-idle** <*seconds*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp keep-interval** <*seconds*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp lanside-wsfclamp** <*threshold*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp max-l2w-buffer** <*Kbytes*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp max-w2l-buffer** <*Kbytes*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp persist-drop** <*seconds*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp preserve-pkt-boundary** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp propagate-syn** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp reset-to-default**

opt-map <*opt map name*> <*priority value*> **set advanced-tcp route-policy-override** {**enable** | **disable**}

opt-map <*opt map name*> <*priority value*> **set advanced-tcp slow-lan-defense** <*threshold*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp slowlan-windowpenalty** <*threshold*>

opt-map <*opt map name*> <*priority value*> **set advanced-tcp window-scale-factor** <*threshold*>

Arguments

opt map <*opt map name*>	Specifies which optimization map.
<*priority value*>	Specifies an existing priority value for the optimization map entry. Acceptable values are from 1 to 65534. By default, the appliance reserves 65535 for the default entry.
set	Configures the optimization map with the arguments that follow.
header {**enable** | **disable**}	Enables or disables header compression.
network-memory {**disable**|**balanced** | **min-latency** | **max-reduction**}	Sets the type of network memory for matched traffic. The options are: • **disable** Disables Network Memory. • **balanced** Sets Network Memory for a balance between minimum latency and maximum reduction. • **min-latency** Sets Network Memory for minimum latency. • **max-reduction** Sets Network Memory for maximum reduction.
payload {**enable** | **disable**}	Enables or disables payload compression for matched traffic.
protocol-specific {**none**|**cifs**|**ssl**|**srdf** | **citrix**}	For the named protocol (CIFS, SSL, SRDF, Citrix) enables acceleration for matched traffic. To disable acceleration for all four (CIFS, SSL, SRDF, and Citrix), use **none**.
tcp {**enable** | **disable**}	Enables or disables TCP acceleration for matched traffic.
advanced-tcp	Sets advanced TCP acceleration options.
adjust-mss-to-mtu {**enable** | **disable**}	Enables or disables the adjustment of the MSS to the tunnel MTU.
auto-reset-flows {**enable** | **disable**}	Enables or disables the auto-reset of TCP flows.
congestion-control {**enable** | **disable**}	Enables or disables congestion control for WAN.
e2e-fin-handling {**enable** | **disable**}	Enables or disables end-to-end FIN handling.
ip-black-listing {**enable** | **disable**}	Enables or disables IP blacklisting.
keep-count <*threshold*>	Specifies the maximum number of TCP keep-alive probes.
keep-idle <*seconds*>	Specifies the TCP keep-alive time, in seconds, to the first probe.
keep-interval <*seconds*>	Specifies the time interval between TCP keep-alive probes.

lanside-wsfclamp	For the LAN-side Window Scale Factor clamp, specifies the window scale factor value (**1**... **14**). To disable, use **0**.
max-l2w-buffer <*Kbytes*>	Specifies the maximum LAN-to-WAN buffer size, in kilobytes.
max-w2l-buffer <*Kbytes*>	Specifies the maximum WAN-to-LAN buffer size, in kilobytes.
persist-drop <*seconds*>	Specifies the maximum TCP persist timeout.
preserve-pkt-boundary {**enable** | **disable**}	Enables or disables the preserving of packet boundaries.
propagate-syn {**enable** | **disable**}	Enables or disables the Propagate SYN feature.
reset-to-default	Resets all advanced TCP options to default values.
route-policy-override {**enable** | **disable**}	Enables or disables the route policy override feature.
slow-lan-defense <*threshold*>	Sets the slow LAN defense threshold value (0 .. 12, 0=Off).
slowlan-winpenalty <*threshold*>	For the Slow LAN Window Penalty, specifies the window scale factor value (**1**... **10**). To disable, use **0**.
window-scale-factor <*threshold*>	Set the window scale factor value (1 .. 14).

Defaults

By default, the optimization map entry enables protocol-specific acceleration for CIFS and SSL.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “opt-map” on page 154
- “opt-map match” on page 156
- “opt-map activate” on page 164
- “no opt-map” on page 166
- “opt-map modify-priority” on page 167
- “show opt-map” on page 317

Usage Guidelines

You cannot create a **set** command for an entry until you first issue a **match** command. And, until you create a **set** command, no Set Actions exist for that entry’s priority.

Examples

None.

opt-map activate

Description

Use the **opt-map activate** command to activate an inactive optimization map.

Syntax

opt-map <*opt map name*> **activate**

Arguments

<*opt map name*>	Specifies which existing, inactive optimization map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “opt-map” on page 154
- “opt-map match” on page 156
- “opt-map set” on page 161
- “no opt-map” on page 166
- “opt-map modify-priority” on page 167
- “show opt-map” on page 317

Usage Guidelines

Only one optimization map can be active at a time. The Silver Peak appliance has a default optimization map, *map1*, that’s active until you create and activate a new optimization map.

Examples

To activate the new optimization map, *rambo*:

```
(config) # opt-map rambo activate
```

opt-map comment

Description

Use the **opt-map comment** command to add a comment for a specified NAT map entry.

Syntax

opt-map <*opt map name*> <*priority value*> **comment**

Arguments

<*opt map name*>	Specifies the name of the optimization map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “opt-map” on page 154
- “opt-map match” on page 156
- “opt-map set” on page 161
- “opt-map activate” on page 164
- “no opt-map” on page 166
- “opt-map modify-priority” on page 167
- “show opt-map” on page 317

Usage Guidelines

None.

Examples

None.

no opt-map

Description

Use the **no opt-map** command to delete an optimization map or a specific priority entry from an optimization map.

Syntax

no opt-map <*opt map name*>

no opt-map <*opt map name*> <*priority value*>

Arguments

<*opt map name*>	Specifies which optimization map.
<*priority value*>	Designates a priority value for the map entry. Acceptable values are from 1 to 65534. By default, the appliance reserves 65535 for the default entry.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “opt-map” on page 154
- “opt-map match” on page 156
- “opt-map set” on page 161
- “opt-map activate” on page 164
- “opt-map modify-priority” on page 167
- “show opt-map” on page 317

Usage Guidelines

You can only delete an optimization map if it’s inactive. Therefore, to delete the active optimization map, you must first activate a different optimization map. For example:

```
(config) # opt-map ginger activate
(config) # no opt-map fred
```

You can also delete a specific entry in an optimization map by using the **no opt-map** command and specifying a priority value. For example, the following statement deletes the priority *100* entry (*match* and *set* statements) from the optimization map, *fred*:

```
(config) # no opt-map fred 100
```

opt-map modify-priority

Description

Use **opt-map modify-priority** command to modify the priority value of an existing entry in the optimization map.

Syntax

opt-map <*opt map name*> <*current priority value*> **modify-priority** <*new priority value*>

Arguments

<*opt map name*>	Specifies an existing optimization map.
<*current priority value*>	Specifies the current priority value for the entry you want to change.
modify-priority <*new priority value*>	Designates the new priority for this entry. This new priority value must be unique and between 1 to 65534.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “opt-map” on page 154
- “opt-map match” on page 156
- “opt-map set” on page 161
- “opt-map activate” on page 164
- “no opt-map” on page 166
- “show opt-map” on page 317

Usage Guidelines

If you try renumber the entry to a priority number that already exists, the CLI informs you that that’s the case and that you can’t make that modification.

Examples

To change the priority of entry 40 to be 60 for the map, *wiser*:

```
(config) # opt-map wiser 40 modify-priority 60
```

preposition ftp

Description

Use the **preposition ftp** command to configure the pre-positioning FTP interface. The appliances' FTP server capability enables administrators to FTP files or directories into Network Memory, pre-positioning the data to get the benefit of second-pass network performance.

Syntax

preposition ftp {enable | disable}

preposition ftp anonymous {disable | enable}

preposition ftp max-clients <*integer*>

Arguments

disable	Disables the pre-positioning FTP interface.
enable	Enables the pre-positioning FTP interface.
anonymous disable	Disables the anonymous pre-positioning FTP interface.
anonymous enable	Enables the anonymous pre-positioning FTP interface.
max-clients <*integer*>	Specifies the maximum number of FTP connections allowed. The value must be an integer between *1* and *10*.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See "show preposition" on page 325.

Usage Guidelines

- It's important to make sure that the relevant tunnels are admin-ed up before FTP transfer.
- When a user is able to ftp anonymously, they are not authenticated. Otherwise, the user must be a valid user on the appliance.

Examples

None.

qos-map

Description

The Silver Peak appliance allows you to configure the Quality of Service (QoS) for your traffic by creating *QoS maps*. QoS maps make it easy for you to explicitly match the traffic that you want to queue, and then (1) send that traffic to a particular queue, and (2) specify the DSCP markings for WAN and LAN packets.

You can create elaborate combinations of match criteria, using IP addresses, ports, protocol, and/or DSCP markings. You can also create more complex matches within ACLs. Or, you can choose to simplify your match criteria by using well-known or user-defined applications, or application groups. By default, one QoS map is always active, and you can change the active map at any time, simply by activating a different map.

Each QoS map may have multiple entries. A map entry consists of one or more *match* statements, which specifies packet fields to be matched, and one *set* statement, which specifies the traffic class, or queue, for the traffic. You can also specify DSCP markings for the LAN (inner) and WAN (outer, or tunnel) packets.

For example, in the following example, the first statement matches all traffic that is associated with the application, *AOL*. The second statement specifies a traffic class ID of 9 for that traffic:

```
(conf) # qos-map fred 50 match app aol
(conf) # qos-map fred 50 set traffic-class 9
```

You create a new QoS map with a single, default entry which serves as a catch-all. In this example, if the QoS map, *fred*, did not exist, the CLI would create it when you entered the match statement.

Entries in a map are ordered according to their assigned *priorities*. Priorities are used to identify, as well as to order entries within a map. All priority values must be unique (in other words, no two entries in a given map can have the same priority value). In the above example, the priority for the entries is *50*.

If you enter a new priority statement for an existing QoS map, the CLI adds that entry to the QoS map. However, if you enter a statement that has the same priority as one that already exists, the new entry overwrites the previous one (and the CLI does not provide a warning).

A QoS map entry can match traffic that satisfies either a pre-defined ACL or any of the following attributes:

- IP Protocol
- Source IP Address
- Destination IP Address
- Source Port Number
- Destination Port Number
- Application
- DSCP value
- VLAN

See Also

See the following related commands:

- “qos-map match” on page 171
- “qos-map set” on page 176
- “qos-map activate” on page 178
- “no qos-map” on page 180
- “qos-map modify-priority” on page 181
- “show qos-map” on page 326

To edit the ten available traffic classes, use the **shaper** command.

qos-map match

Description

Use the **qos-map match** command to create a QoS map entry that uses match criteria to delineate traffic. Also use this command to change the matching conditions associated with an existing entry.

Syntax

qos-map <*qos map name*> <*priority value*> **match acl** <*ACL name*>

qos-map <*qos map name*> <*priority value*> **match app** {<*application name*> | <*application group*>}

qos-map <*qos map name*> <*priority value*> **match dscp** {<*dscp value*> | **any**}

qos-map <*qos map name*> <*priority value*> **match protocol** <*IP protocol number or name*> {<*source ip address/netmask*> | **any**} {<*destination ip address/netmask*> | **any**} [**dscp** {<*dscp value*> | **any**}] [**vlan** {**any** | <*1..4094*> | <*interface.tag*> | <*any.tag*> | <*interface.any*> | <*interface.native*>}]

qos-map <*qos map name*> <*priority value*> **match protocol ip** {<*source ip address/netmask*> | **any**} {<*destination ip address/netmask*> | **any**} [**app** {<*application name*> | **any**}] [**dscp** {<*dscp value*> | **any**}] [**vlan** {**any** | <*1..4094*> | <*interface.tag*> | <*any.tag*> | <*interface.any*> | <*interface.native*>}]

qos-map <*qos map name*> <*priority value*> **match protocol** {**tcp** | **udp**} {<*source IP address/netmask*> | **any**} {<*destination IP address/netmask*> | **any**} [{<*source port number*> | **any**} {<*destination port number*> | any}] [**dscp** {<*dscp value*> | any}] [**vlan** {any | <*1..4094*> | <*interface.tag*> | <*any.tag*> | <*interface.any*> | <*interface.native*>}]

qos-map <*qos map name*> <*priority value*> **match vlan** {**any** | <*1..4094*> | <*interface.tag*> | <*any.tag*> | <*interface.any*> | <*interface.native*>}

Arguments

qos map <*qos map name*>	Specifies which QoS map. If the name doesn't exist, the CLI creates it.
<*priority value*>	Designates a priority value for the map entry. Acceptable values are from *1* to *65534*. By default, the appliance reserves *65535* for the default entry.
match acl <*ACL name*>	Creates an entry that uses an existing ACL to match traffic. Also use this command to change the ACL associated with an existing entry.
match app <*application name*>	Creates an entry that uses a built-in or user-defined application—or an application group—to match traffic. Also use this command to change the application associated with an existing entry. For a list of built-in applications, see Table 3-1, "Applications on the Silver Peak Appliance," on page 159.
match dscp {<*dscp value*> | **any**}	Creates or modifies an entry that matches traffic with a specific DSCP marking. You can use any of the following values: • af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs1, cs2, cs3, cs4, cs5, cs6, cs7, *or* ef. • **any** is a wildcard.

any	**any** is a wildcard.
match protocol <*IP protocol number or name*>	Creates or modifies an entry that matches traffic with a specific protocol that is **NOT** named specifically as *ip*, *tcp*, or *udp*: • The available IP protocol numbers include 1 through 254. • The available IP protocol names include:

ah	egp	eigrp	encap
esp	etherip	fc	gre
icmp	idpr	idpr-cmtp	idrp
igmp	igp	ip-comp	ip-mobility
ipip	ipip4	ipx-in-ip	irtp
iso-ip	iso-tp4	I2tp	mhrp
ospf	pim	rdp	rsvp
sctp	tlsp	vrrp	

match protocol ip	Creates or modifies an entry that matches specific IP addresses. • When you specify **protocol ip**, the assumption is that you are allowing *any* IP protocol. In that case, you also need to specify an application (or application group). If you don't, the CLI defaults to specifying **any** application. • If you don't choose to specify a DSCP value in the full command, then the CLI defaults to specifying **any** DSCP value in the policy entry.
match protocol {**tcp** | **udp**}	Creates or modifies an entry that matches specific TCP or UDP addresses. • If you don't choose to specify source and destination ports in the full command, then the CLI defaults to specifying **0:0** (any source port and any destination port) in the policy entry. • If you don't choose to specify a DSCP value in the full command, then the CLI defaults to specifying **any** DSCP value in the policy entry.
match vlan {**any** | <*1..4094*> | <*interface.tag*> | <*any.tag*> | <*interface.any*> | <*interface.native*>}	Creates or modifies an entry that matches an interface and 802.1q VLAN tag. The available values include: • <*1..4094*>the number assigned to a VLAN • <interface.tag>as in **lan0.10** • <any.tag>as in **any.10** • <interface.any>as in **lan0.any** • <*interface.native*>as in **lan0.native** • **any** is a wildcard.
<*source ip address/netmask*>	Specifies the source IP address and netmask in slash notation. For example, *10.2.0.0 0.0.255.255* should be entered as *10.2.0.0/16.*
<*destination ip address/netmask*>	Specifies the destination IP address and netmask in slash notation. For example, *10.2.0.0/16.*

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “qos-map” on page 169
- “qos-map set” on page 176
- “qos-map activate” on page 178
- “no qos-map” on page 180
- “qos-map modify-priority” on page 181
- “show qos-map” on page 326

Usage Guidelines

You can specify one of the following standard (built-in) applications (listed alphabetically left to right):

Table 3-2 Applications on the Silver Peak Appliance

3par	aol	aol_im	aspera
avamar	backweb	bit_torrent	bluearc
celerra	centera	cifs_smb	cisco_skinny
citrix	commvault	cuseeme	cvs
datadomain	ddm	ddm_ssl	dns
doom	doubletake	echo	edonkey
fcip	filenet	ftp	ftps
gnutella	h_323	hadoop	hostname
http	https	ibm_db2	ifcp
imap	imap4s	ipsec	irc
irc_ssl	isakmp	iscsi	isns
ivisit	kazaa	kerberos	l2tp
ldap	ldaps	lotus_cc_mail	lotus_notes
matip	ms_exchange	ms_media	ms_messenger
ms_odbc	ms_ole	ms_rpc	ms_sql
ms_terminal_services	ms_zone	nameserver	ndmp
netbios	nfs	nntp	nntps
novell	ntp	openwindows	oracle
pcanywhere	pcmail	pcoip	peoplesoft
pop	pop3s	pptp	printer
quake	recoverpoint	rlogin	routing

Table 3-2 Applications on the Silver Peak Appliance (Continued)

rtcp	rtsp	sap	sgcp
sgmp	shell	silverpeak_comm	silverpeak_gms
silverpeak_internal	silverpeak-peer	silverpeak-tcpperf	sip
sip_tls	smtp	smtps	snapmirror
snmp	sql	srdf	ssh
sshell	sun_rpc	sybase	syslog
t_120	tacacs	telnet	telnets
tftp	timbuktu	time	uucp
vnc	vplex	vvr	xwindows
yahoo_games	yahoo_im		

For each **qos-map match** command with a given priority, you must create a **qos-map set** command with the same priority. But, you cannot create a **set** command without having first created the **match** command.

Examples

To create a match criteria with a priority of "100" for the map, "express", that filters for all traffic coming from the LAN with a DSCP marking of "best effort":

```
(config) # qos-map express 100 match dscp be
```

To create a match criteria with a priority of "70" for the map, "express", that filters for the application group, "secure":

```
(config) # qos-map express 70 match app secure
```

To create a match criteria with a priority of "20" for "map2" that filters for all AOL traffic that's headed from the LAN to 172.34.8.0:

```
(config) # qos-map map2 20 match protocol ip any 172.34.8.0 aol
```

Since you haven't specified a DSCP value, the criteria will include all DSCP values, as if you had written it as follows:

```
(config) # qos-map map2 20 match protocol ip any 172.34.8.0 aol any
```

To create a match criteria with a priority of "30" for the map, "arthouse" that filters for all UDP traffic coming from port 41 and having a destination of 122.33.44.0/24:

```
(config) # qos-map arthouse 30 match protocol udp any 122.33.4.0/24 41:0
```

Since you haven't specified a DSCP value, the criteria will include all DSCP values, as if you had written it as follows:

```
(config) # qos-map arthouse 30 match protocol udp any 122.33.4.0/24 41:0
any
```

To create a match criteria with a priority of “10” for the map, “waldo” that filters for all Interior Gateway Protocol (IGP) traffic that has a DSCP marking of “af11”:

```
(config) # qos-map waldo 10 match protocol igp any any dscp af11
```

qos-map set

Description

The **qos-map set** command specifies or modifies the set statement in a QoS map entry. You cannot use a **set** command until you first issue a **match** command.

Syntax

qos-map <*qos map name*> <*priority value*> **set traffic-class** <*traffic class ID*>

qos-map <*qos map name*> <*priority value*> **set traffic-class** <*traffic class ID*> **lan-qos** {**trust-lan** | <*dscp value*>} **wan-qos** {**trust-lan** | <*dscp value*>}

qos-map <*qos map name*> <*priority value*> **set lan-qos** {**trust-lan** | <*dscp value*>}

qos-map <*qos map name*> <*priority value*> **set wan-qos** {**trust-lan** | <*dscp value*>}

Arguments

qos-map <*qos map name*>	Specifies which QoS map.
<*priority value*>	Specifies an existing priority value for the map entry. Acceptable values are from 1 to 65534. By default, the appliance reserves 65535 for the default entry.
traffic-class <*traffic class ID*>	Specifies the traffic class, or queue, to which matched traffic is sent. Traffic classes are identified by integer values from *1* through *10*.
lan-qos {**trust-lan**	<*dscp value*>}	With **lan-qos**, **trust-lan** indicates that the DSCP marking should not change. In other words, the DSCP setting in the inner, encapsulated packet that comes in is the same one that goes out. You can assign any of the following DSCP values: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs1, cs2, cs3, cs4, cs5, cs6, cs7, *or* ef.
wan-qos {**trust-lan**	<*dscp value*>}	With **wan-qos**, **trust-lan** indicates that the marking of the outer packet follows the marking of the inner packet. You can assign any of the following DSCP values: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs1, cs2, cs3, cs4, cs5, cs6, cs7, *or* ef.

Defaults

By default, the **set** part of the default optimization map entry (priority 65535) is:

- **qos-map set traffic-class 1 lan-qos trust-lan wan-qos trust-lan**

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “qos-map” on page 169
- “qos-map match” on page 171
- “qos-map activate” on page 178
- “no qos-map” on page 180
- “qos-map modify-priority” on page 181
- “show qos-map” on page 326

Usage Guidelines

You cannot create a **set** command for an entry until you first issue a **match** command. And, until you create a **set** command, no Set Actions exist for that entry’s priority.

- When creating an entry (priority) with the Appliance Manager Graphical User Interface, the QoS map defaults are:
  - Traffic class = 1
  - LAN QoS = trust-lan
  - WAN QoS = trust-lan
- When you create the first **qos-map set** command ***for a priority*** with the CLI and you use a syntax that doesn’t specify all three Set Actions, the CLI automatically creates the rest as defaults in the background.

For example, if your first set command for priority “10” in “map1” is:

```
(config) # qos-map map1 10 set lan-qos be
```

then, the CLI also creates the following two additional entries behind the scenes:

```
(config) # qos-map map1 10 set traffic-class 1
(config) # qos-map map1 10 set wan-qos trust-lan
```

You can verify these results by using the command, “show qos-map” on page 326.

For pass-through traffic, any **lan-qos** specification is ignored. Any **wan-qos** specification is placed in the ToS field of the packet.

Examples

None.

qos-map activate

Description

Use the **qos-map activate** command to activate an inactive QoS map.

Syntax

qos-map <*qos map name*> **activate**

Arguments

<*qos map name*>	Specifies which existing, inactive QoS map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “qos-map” on page 169
- “qos-map match” on page 171
- “qos-map set” on page 176
- “no qos-map” on page 180
- “qos-map modify-priority” on page 181
- “show qos-map” on page 326

Usage Guidelines

Only one QoS map can be active at time. The Silver Peak appliance has a default QoS map, *map1*, that is active until you create and activate a new QoS map.

Examples

To activate the new QoS map, *houdini*:

```
(config) # qos-map houdini activate
```

qos-map comment

Description

Use the **qos-map comment** command to add a comment for a specified QoS map entry.

Syntax

qos-map *<qos map name>* *<priority value>* **comment**

Arguments

<qos map name>	Specifies the name of the QoS map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “qos-map” on page 169
- “qos-map match” on page 171
- “qos-map set” on page 176
- “qos-map activate” on page 178
- “no qos-map” on page 180
- “qos-map modify-priority” on page 181
- “show qos-map” on page 326

Usage Guidelines

None.

Examples

None.

no qos-map

Description

Use the **no qos-map** command to delete a QoS map or a specific priority entry from a QoS map.

Syntax

no qos-map *<qos map name>*

no qos-map *<qos map name> <priority value>*

Arguments

<qos map name>	Specifies which QoS map.
<priority value>	Designates a priority value in the map entry. Acceptable values are from 1 to 65534. By default, the appliance reserves 65535 for the default entry, which cannot be removed.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “qos-map” on page 169
- “qos-map match” on page 171
- “qos-map set” on page 176
- “qos-map activate” on page 178
- “qos-map modify-priority” on page 181
- “show qos-map” on page 326

Usage Guidelines

You can only delete a QoS map if it’s inactive. To delete the active QoS map, you must first activate a different QoS map. For example:

```
(config) # qos-map ginger activate
(config) # no qos-map fred
```

You can also delete a specific entry in a QoS map by using the **no qos-map** command and specifying a priority value. For example, the following statement deletes the priority *100* entry (*match* and *set* statements) from the QoS map, *fred*:

```
(config) # no qos-map fred 100
```

qos-map modify-priority

Description

Use **qos-map modify-priority** command to modify the priority value of an existing entry.

Syntax

qos-map <*qos map name*> <*current priority value*> **modify-priority** <*new priority value*>

Arguments

<*qos map name*>	Specifies an existing QoS map.
<*current priority value*>	Specifies the current priority value for the entry you want to change.
<*new priority value*>	Designates the new priority for this entry. This new priority value must be unique and between 1 to 65534.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “qos-map” on page 169
- “qos-map match” on page 171
- “qos-map set” on page 176
- “qos-map activate” on page 178
- “no qos-map” on page 180
- “show qos-map” on page 326

Usage Guidelines

If you try renumber the entry to a priority number that already exists, the CLI informs you that that’s the case and that you can’t make that modification.

Examples

To change the priority of entry 40 to be 60 for the map, *DesMoines*:

```
(config) # opt-map DesMoines 40 modify-priority 60
```

.

route-map

Description

The Silver Peak appliance allows you to manage your packet flow by creating *route maps*. Route maps make it easy for you to identify exactly the traffic that you need to manage. You can create elaborate combinations of match criteria, using IP addresses, ports, protocol, and/or DSCP markings. You can also create more complex matches within ACLs. Or, you can choose to simplify your match criteria by using well-known or user-defined applications, or application groups. By default, one route map is always active, and you can change the active map at any time, simply by activating a different map.

Each route map may have multiple entries. A map entry consists of one or more *match* statements, which specifies packet fields to be matched, and one *set* statement, which takes action on the matched traffic, such as sending it to a tunnel or dropping it.

For example, in the following example, the first statement matches all traffic that is associated with the application, *AOL*. The second statement sends that AOL traffic through the tunnel named *Holland*:

```
(conf) # route-map fred 50 match app aol
(conf) # route-map fred 50 set tunnel Holland
```

You create a new route map with a single, default entry which serves as a catch-all. In this example, if the route map, *fred*, did not exist, the CLI would create it when you entered the match statement.

Entries in a map are ordered according to their assigned *priorities*. Priorities are used to identify, as well as to order entries within a map. All priority values must be unique (in other words, no two entries in a given map can have the same priority value). In the above example, the priority for the entries is *50*.

If you enter a new priority statement for an existing route map, the CLI adds that entry to the route map. However, if you enter a statement that has the same priority as one that already exists, the new entry overwrites the previous one (and the CLI does not provide a warning).

A route map entry can match traffic that satisfies either a pre-defined ACL or any of the following attributes:

- IP protocol
- Source IP address and subnet mask
- Destination IP address and subnet mask
- Source port number
- Destination port number
- Application
- DSCP value
- VLAN

See Also

See the following related commands:

- “route-map match” on page 184
- “route-map set” on page 189
- “route-map activate” on page 192
- “no route-map” on page 194
- “route-map modify-priority” on page 195

route-map match

Description

Use the **route-map match** command to create a route map entry that uses match criteria to delineate traffic. Also use this command to change the matching conditions associated with an existing entry.

Syntax

route-map *<route map name>* *<priority value>* **match acl** *<ACL name>*

route-map *<route map name>* *<priority value>* **match app** {*<application name>* | *<application group>*}

route-map *<route map name>* *<priority value>* **match dscp** {*<dscp value>* | **any**}

route-map *<route map name>* *<priority value>* **match protocol** *<IP protocol number or name>* {*<source ip address/netmask>* | **any**} {*<destination ip address/netmask>* | **any**} [**dscp** {*<dscp value>* | **any**}] [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

route-map *<route map name>* *<priority value>* **match protocol ip** {*<source ip address/netmask>* | **any**} {*<destination ip address/netmask>* | **any**} [**app** {*<application name>* | **any**}] [**dscp** {*<dscp value>* | **any**}] [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

route-map *<route map name>* *<priority value>* **match protocol** {**tcp** | **udp**} {*<source IP address/netmask>* | **any**} {*<destination IP address/netmask>* | **any**} [{*<source port number>* | **any**} {*<destination port number>* | **any**}] [dscp {*<dscp value>* | **any**}] [**vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}]

route-map *<route map name>* *<priority value>* **match vlan** {**any** | *<1..4094>* | *<interface.tag>* | *<any.tag>* | *<interface.any>* | *<interface.native>*}

Arguments

route map *<route map name>*	Specifies which route map. If the name doesn't exist, the CLI creates it.
<priority value>	Designates a priority value for the map entry. Acceptable values are from *1* to *65534*. By default, the appliance reserves *65535* for the default entry.
match acl *<ACL name>*	Creates an entry that uses an existing ACL to match traffic. Also use this command to change the ACL associated with an existing entry.
match app *<application name>*	Creates an entry that uses a built-in or user-defined application—or an application group—to match traffic. Also use this command to change the application associated with an existing entry. For a list of built-in applications, see Table 3-1, "Applications on the Silver Peak Appliance," on page 159.
match dscp {*<dscp value>* | **any**}	Creates or modifies an entry that matches traffic with a specific DSCP marking. You can use any of the following values: • **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **be**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**. • **any** is a wildcard.

any	**any** is a wildcard.
match protocol <*IP protocol number or name*>	Creates or modifies an entry that matches traffic with a specific protocol that is **NOT** named specifically as *ip*, *tcp*, or *udp*: • The available IP protocol numbers include 1 through 254. • The available IP protocol names include:

ah	egp	eigrp	encap
esp	etherip	fc	gre
icmp	idpr	idpr-cmtp	idrp
igmp	igp	ip-comp	ip-mobility
ipip	ipip4	ipx-in-ip	irtp
iso-ip	iso-tp4	I2tp	mhrp
ospf	pim	rdp	rsvp
sctp	tlsp	vrrp	

match protocol ip	Creates or modifies an entry that matches specific IP addresses. • When you specify **protocol ip**, the assumption is that you are allowing *any* IP protocol. In that case, you also need to specify an application (or application group). If you don't, the CLI defaults to specifying **any** application. • If you don't choose to specify a DSCP value in the full command, then the CLI defaults to specifying **any** DSCP value in the policy entry.
match protocol {**tcp** | **udp**}	Creates or modifies an entry that matches specific TCP or UDP addresses. • If you don't choose to specify source and destination ports in the full command, then the CLI defaults to specifying **0:0** (any source port and any destination port) in the policy entry. • If you don't choose to specify a DSCP value in the full command, then the CLI defaults to specifying **any** DSCP value in the policy entry.
match vlan {**any** | <*1..4094*> | <*interface.tag*> | <*any.tag*> | <*interface.any*> | <*interface.native*>}	Creates or modifies an entry that matches an interface and 802.1q VLAN tag. The available values include: • <*1..4094*> the number assigned to a VLAN • <interface.tag> as in **lan0.10** • <any.tag> as in **any.10** • <interface.any> as in **lan0.any** • <*interface.native*> as in **lan0.native** • **any** is a wildcard.
<*source ip address/netmask*>	Specifies the source IP address and netmask in slash notation. For example, *10.2.0.0 0.0.255.255* should be entered as *10.2.0.0/16.*
<*destination ip address/netmask*>	Specifies the destination IP address and netmask in slash notation. For example, *10.2.0.0/16.*

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “route-map” on page 182
- “route-map set” on page 189
- “route-map activate” on page 192
- “no route-map” on page 194
- “route-map modify-priority” on page 195
- “show route-map” on page 330

Usage Guidelines

You can specify one of the following standard (built-in) applications (listed alphabetically left to right):

Table 3-3 Applications on the Silver Peak Appliance

3par	aol	aol_im	aspera
avamar	backweb	bit_torrent	bluearc
celerra	centera	cifs_smb	cisco_skinny
citrix	commvault	cuseeme	cvs
datadomain	ddm	ddm_ssl	dns
doom	doubletake	echo	edonkey
fcip	filenet	ftp	ftps
gnutella	h_323	hadoop	hostname
http	https	ibm_db2	ifcp
imap	imap4s	ipsec	irc
irc_ssl	isakmp	iscsi	isns
ivisit	kazaa	kerberos	l2tp
ldap	ldaps	lotus_cc_mail	lotus_notes
matip	ms_exchange	ms_media	ms_messenger
ms_odbc	ms_ole	ms_rpc	ms_sql
ms_terminal_services	ms_zone	nameserver	ndmp
netbios	nfs	nntp	nntps
novell	ntp	openwindows	oracle
pcanywhere	pcmail	pcoip	peoplesoft
pop	pop3s	pptp	printer
quake	recoverpoint	rlogin	routing

Table 3-3 Applications on the Silver Peak Appliance (Continued)

rtcp	rtsp	sap	sgcp
sgmp	shell	silverpeak_comm	silverpeak_gms
silverpeak_internal	silverpeak-peer	silverpeak-tcpperf	sip
sip_tls	smtp	smtps	snapmirror
snmp	sql	srdf	ssh
sshell	sun_rpc	sybase	syslog
t_120	tacacs	telnet	telnets
tftp	timbuktu	time	uucp
vnc	vplex	vvr	xwindows
yahoo_games	yahoo_im		

For each **route-map match** command with a given priority, you must create a **route-map set** command with the same priority. But, you cannot create a **set** command without having first created the **match** command.

Examples

To create a match criteria with a priority of "100" for the map, "vinnie", that filters for all traffic coming from the LAN with a DSCP marking of "best effort":

```
(config) # route-map vinnie 100 match dscp be
```

To create a match criteria with a priority of "70" for the map, "vinnie", that filters for the application group, "secure":

```
(config) # route-map vinnie 70 match app secure
```

To create a match criteria with a priority of "20" for "map2" that filters for all AOL traffic that's headed from the LAN to 172.34.8.0:

```
(config) # route-map map2 20 match protocol ip any 172.34.8.0 aol
```

Since you haven't specified a DSCP value, the criteria will include all DSCP values, as if you had written it as follows:

```
(config) # route-map map2 20 match protocol ip any 172.34.8.0 aol any
```

To create a match criteria with a priority of "30" for the map, "arthouse" that filters for all UDP traffic coming from port 41 and having a destination of 122.33.44.0/24:

```
(config) # route-map arthouse 30 match protocol udp any 122.33.4.0/24 41:0
```

Since you haven't specified a DSCP value, the criteria will include all DSCP values, as if you had written it as follows:

```
(config) # route-map arthouse 30 match protocol udp any 122.33.4.0/24 41:0
any
```

To create a match criteria with a priority of “10” for the map, “autobahn” that filters for all Interior Gateway Protocol (IGP) traffic that has a DSCP marking of “af11”:

```
(config) # route-map autobahn 10 match protocol igp any any dscp af112
```

route-map set

Description

The **route-map set** command specifies or modifies the SET part of an entry in a given route map. You cannot use a **set** command until you first issue a **match** command.

Syntax

route-map <*route map name*> <*priority value*> **set auto-opt-balance [if-down {pass-through | pass-through-unshaped | drop}]**

route-map <*route map name*> <*priority value*> **set auto-opt-low-latency [if-down {pass-through | pass-through-unshaped | drop}]**

route-map <*route map name*> <*priority value*> **set auto-opt-low-loss [if-down {pass-through | pass-through-unshaped | drop}]**

route-map <*route map name*> <*priority value*> **set auto-opt-overlay-id** <*overlay name*> [**if-down** {**pass-through** | **pass-through-unshaped** | **drop**}]

route-map <*route map name*> <*priority value*> **set auto-opt-preferred-if {**<*interface name*> **| wan0}**

route-map <*route map name*> <*priority value*> **set auto-optimize** [**if-down** {**pass-through** | **pass-through-unshaped** | **drop**}]

route-map <*route map name*> <*priority value*> **set drop**

route-map <*route map name*> <*priority value*> **set pass-through** {**shaped** | **unshaped**}

route-map <*route map name*> <*priority value*> **set peer-balance** <*peer hostname*> [**if-down** {**pass-through** | **pass-through-unshaped** | **drop** | **continue**}]

route-map <*route map name*> <*priority value*> **set peer-low-latency** <*peer hostname*> [**if-down** {**pass-through** | **pass-through-unshaped** | **drop** | **continue**}]

route-map <*route map name*> <*priority value*> **set peer-low-loss** <*peer hostname*> [**if-down** {**pass-through** | **pass-through-unshaped** | **drop** | **continue**}]

route-map <*route map name*> <*priority value*> **set tunnel** <*tunnel name*> [**if-down** {**pass-through** | **pass-through-unshaped** | **drop** | **continue**}]

Arguments

route-map <*route map name*>	Specifies which route map.
<*priority value*>	Specifies an existing priority value for the map entry. Acceptable values are from 1 to 65534. By default, the appliance reserves 65535 for the default entry.
set auto-opt-balance	Auto-routes (optimizes) the traffic, load balancing.
set auto-opt-low-latency	Auto-routes (optimizes) the traffic, select tunnel with lowest latency.
set auto-opt-low-loss	Auto-routes (optimizes) the traffic, select tunnel with lowest loss.

set auto-opt-overlay-id <*overlay name*>	Auto-routes (optimizes) the traffic, select the named overlay.
set auto-opt-preferred-if	Auto-routes (optimizes) the traffic, select desired interface for auto-opt.
set auto-optimize	Auto-routes (optimizes) the traffic.
set tunnel <*tunnel name*>	Specifies the name of an existing tunnel. Use the **route-map set tunnel** command when you send matched traffic to a tunnel or a pair of redundant tunnels.
if-down {**pass-through** | **pass-through-unshaped** | **drop** | **continue**}	Establishes what action the Silver Peak appliance takes if the primary tunnel (and its backup tunnel, if there is one) is down. You can specify the following options with **if-down**: • **pass-through** - Traffic is passed through with QoS shaping. • **pass-through-unshaped** - Traffic is passed through with no QoS shaping. • **drop** - The packets are dropped. • **continue** - Continue processing next entry. The default option, if you don't specify one, is **pass-through** (shaped).
set pass-through {**shaped** | **unshaped**}	Use the **route-map set passthrough** command if you want matching traffic to pass through the Silver Peak appliance unaccelerated. To limit the bandwidth of the traffic according to the passthrough bandwidth settings of the shaper, choose **shaped**; otherwise, choose **unshaped**.
set peer-balance <*peer hostname*>	Specifies that the appliance load balance with its named peer. To view a list of peers, enter a space and question mark at the end of this argument.
set peer-low-latency <*peer hostname*>	When the appliance has a peer, use the one with the lowest latency.
set peer-low-loss <*peer hostname*>	When the appliance has a peer, use the one with the lowest loss.
set drop	Use when you want to drop matched traffic.

Defaults

The default action for **if-down** is to send the traffic through as pass-through and shaped.

Command Mode

Global Configuration Mode

See Also

- "route-map" on page 182
- "route-map match" on page 184
- "route-map activate" on page 192
- "no route-map" on page 194
- "route-map modify-priority" on page 195
- "show route-map" on page 330

Usage Guidelines

- You cannot use a **set** command until you first issue a **match** command.
- By default, the set part of the default route map entry (with priority *65535*) is **auto-optimize**, which means that the appliances determine the appropriate, available tunnel for the traffic. You can modify this to drop or pass-through unshaped as follows:

  route-map <*route map name*> **65535 set drop**

  route-map <*route map name*> **65535 set pass-through-unshaped**

Examples

None.

route-map activate

Description

Use the **route-map activate** command to activate a route map.

Syntax

route-map <*route_map_name*> **activate**

Arguments

<*route map name*>	Specifies which route map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “route-map” on page 182
- “route-map match” on page 184
- “route-map set” on page 189
- “no route-map” on page 194
- “route-map modify-priority” on page 195
- “show route-map” on page 330

Usage Guidelines

Only one route map can be active at time. The Silver Peak appliance has a default route map, *map1*, that is active until you create and activate a new route map.

Examples

To activate the new route map, *whichway*:

```
(config) # qos-map whichway activate
```

route-map comment

Description

Use the **route-map comment** command to add a comment for a specified QoS map entry.

Syntax

route-map <*route map name*> <*priority value*> **comment**

Arguments

<*route map name*>	Specifies the name of the route map.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “route-map” on page 182
- “route-map match” on page 184
- “route-map set” on page 189
- “route-map activate” on page 192
- “no route-map” on page 194
- “route-map modify-priority” on page 195
- “show route-map” on page 330

Usage Guidelines

None.

Examples

None.

no route-map

You can use the **no route-map** command to delete a route map or a specific priority entry from a route map.

Syntax

no route-map <*route_map_name*>

no route-map <*route map name*> <*priority value*>

Arguments

<*route map name*>	Specifies which existing route map.
<*priority value*>	Designates a priority value for the map entry. Acceptable values are from 1 to 65534. By default, the appliance reserves 65535 for the default entry.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “route-map” on page 182
- “route-map match” on page 184
- “route-map set” on page 189
- “route-map activate” on page 192
- “route-map modify-priority” on page 195
- “show route-map” on page 330

Usage Guidelines

You can only delete a route map if it’s inactive. To delete the active route map, you must first activate a different route map. For example:

```
(config) # route-map ginger activate
(config) # no route-map fred
```

You can also delete a specific entry in a route map by using the **no route-map** command and specifying a priority value. For example, the following statement deletes the priority *100* entry (*match* and *set* statements) from the route map, *fred*:

```
(config) # no route-map fred 100
```

route-map modify-priority

Description

Use **route-map modify-priority** command to modify the priority value of an existing entry.

Syntax

route-map *<route map name>* *<current priority value>* **modify-priority** *<new priority value>*

Arguments

<route map name>	Specifies the name of an existing route map.
<current priority value>	Specifies the current priority value for the entry you want to change.
<new priority value>	Designates the new priority for this entry. This new priority value must be unique and between 1 to 65534.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “route-map” on page 182
- “route-map match” on page 184
- “route-map set” on page 189
- “route-map activate” on page 192
- “no route-map” on page 194
- “show route-map” on page 330

Usage Guidelines

If you try renumber the entry to a priority number that already exists, the CLI informs you that that’s the case and that you can’t make that modification.

Examples

To change the priority of entry 40 to be 60 for the map, *lunar*:

```
(config) # route-map lunar 40 modify-priority 60
```

saas

Description

Use **saas** command to configure the system SaaS options.

Syntax

saas {**enable** | **disable**}

saas rtt-interval <*seconds*>

saas rtt-num-req-per-host <*number*>

Arguments

disable	Disables SaaS.
enable	Enables SaaS.
rtt-interval < *seconds*>	Specifies the RTT (Round Trip Time) daemon interval in seconds.
rtt-num-req-per-host <*number*>	Specifies the number of requests to send to each host to calculate the average RTT.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

shaper inbound

Description

Use **shaper inbound** command to shape individual WAN, LAN, or management interfaces, or to shape the aggregate WAN interface.

Use the **no** command to remove an inbound shaper.

Syntax

shaper inbound <*shaper name*> {**enable** | **disable**}

shaper inbound <*shaper name*> **accuracy** <*usec*>

shaper inbound <*shaper name*> **max-bandwidth** <*kbps*>

shaper inbound <*shaper name*> **traffic-class** <*1-10*> **excess-weight** <*weight*>

shaper inbound <*shaper name*> **traffic-class** <*1-10*> **max-bandwidth** <*% of interface bandwidth*>

shaper inbound <*shaper name*> **traffic-class** <*1-10*> **max-wait** <*ms*>

shaper inbound <*shaper name*> **traffic-class** <*1-10*> **min-bandwidth** <*% of interface bandwidth*>

shaper inbound <*shaper name*> **traffic-class** <*1-10*> **priority** <*1-10*>

no shaper inbound {<*shaper name*> | **default** | **wan**}

Arguments

disable	Disables inbound shaper.
enable	Enables inbound shaper.
<*shaper name*>	Refers to the shaper for a specific interface, such as **wan0**, **wan1**, **twan0**, **twan1**, **bwan0**, **lan0**, **lan1**, **tlan0**, **tlan1**, **blan0**, **mgmt0**, **mgmt1**. Use **wan** for shaping the aggregate WAN interface.
accuracy <*usec*>	Specifies shaper accuracy in microseconds.
traffic-class <*1-10*>	Specifies the shaper traffic class.
excess-weight <*weight*>	Specifies the shaper traffic class excess weight. If there is remaining bandwidth after satisfying the minimum bandwidth, then the excess is distributed among the traffic classes in proportion to the weightings specified . Values range from 1 to 10,000.
max-bandwidth <*% of interface bandwidth*>	Specifies the traffic class's maximum bandwidth in kilobits per second. You can limit the maximum bandwidth that a traffic class will use by specifying a percentage. The bandwidth usage for the traffic class never exceeds this value.

max-wait <*ms*>	Specifies the maximum wait time in milliseconds. Any packets waiting longer than the specified Max Wait Time are dropped.
min-bandwidth <*% of interface bandwidth*>	Specifies the shaper's minimum bandwidth in kilobits per second. Each traffic class is guaranteed this percentage of bandwidth, allocated in the order of priority. However, if the sum of the percentages is greater than 100%, then lower-priority traffic classes might not receive their guaranteed bandwidth if it is all consumed by higher-priority traffic.
priority <*1-10*>	Specifies the shaper traffic class priority. This determines the order in which each class's minimum bandwidth is allocated - 1 is first, 10 is last.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See "show shaper" on page 336.

Usage Guidelines

The inbound Shaper provides a simplified way to globally configure QoS (Quality of Service) on the appliances.

- It shapes inbound traffic by allocating bandwidth across ten traffic classes.
- The system applies these QoS settings globally before decompressing all the inbound tunnelized and pass-through-shaped traffic --- shaping it as it arrives from the WAN.

Examples

None.

shaper outbound

Description

Use **shaper outbound**command to shape individual WAN, LAN, or management interfaces, or to shape the aggregate WAN interface.

Use the **no** command to remove an outbound shaper.

Syntax

shaper outbound <*shaper name*> {**enable** | **disable**}

shaper outbound <*shaper name*> **accuracy** <*usec*>

shaper outbound <*shaper name*> **max-bandwidth** <*kbps*>

shaper outbound <*shaper name*> **traffic-class** <*1-10*> **excess-weight** <*weight*>

shaper outbound <*shaper name*> **traffic-class** <*1-10*> **max-bandwidth** <*% of interface bandwidth*>

shaper outbound <*shaper name*> **traffic-class** <*1-10*> **max-wait** <*ms*>

shaper outbound <*shaper name*> **traffic-class** <*1-10*> **min-bandwidth** <*% of interface bandwidth*>

shaper outbound <*shaper name*> **traffic-class** <*1-10*> **priority** <*1-10*>

no shaper outbound {<*shaper name*> | **default** | **wan**}

Arguments

disable	Disables outbound shaper.
enable	Enables outbound shaper.
<*shaper name*>	Refers to the shaper for a specific interface, such as **wan0**, **wan1**, **twan0**, **twan1**, **bwan0**, **lan0**, **lan1**, **tlan0**, **tlan1**, **blan0**, **mgmt0**, **mgmt1**. Use **wan** for shaping the aggregate WAN interface. Availability of the non-WAN interfaces (as arguments) is to facilitate preparations for migrating from one appliance model to another, or one deployment mode to another.
accuracy <*usec*>	Specifies shaper accuracy in microseconds.
traffic-class <*1-10*>	Specifies the shaper traffic class.
excess-weight <*weight*>	Specifies the shaper traffic class excess weight. If there is remaining bandwidth after satisfying the minimum bandwidth, then the excess is distributed among the traffic classes in proportion to the weightings specified . Values range from 1 to 10,000.

max-bandwidth <*% of interface bandwidth*>	Specifies the traffic class's maximum bandwidth in kilobits per second. You can limit the maximum bandwidth that a traffic class will use by specifying a percentage. The bandwidth usage for the traffic class never exceeds this value.
max-wait <*ms*>	Specifies the maximum wait time in milliseconds. Any packets waiting longer than the specified Max Wait Time are dropped.
min-bandwidth <*% of interface bandwidth*>	Specifies the shaper's minimum bandwidth in kilobits per second. Each traffic class is guaranteed this percentage of bandwidth, allocated in the order of priority. However, if the sum of the percentages is greater than 100%, then lower-priority traffic classes might not receive their guaranteed bandwidth if it is all consumed by higher-priority traffic.
priority <*1-10*>	Specifies the shaper traffic class priority. This determines the order in which each class's minimum bandwidth is allocated - 1 is first, 10 is last.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See "show shaper" on page 336.

Usage Guidelines

The Shaper provides a simplified way to globally configure QoS (Quality of Service) on the appliances.

- It shapes outbound traffic by allocating bandwidth as a percentage of the system bandwidth.
- The system applies these QoS settings globally after compressing (deduplicating) all the outbound tunnelized and pass-through-shaped traffic --- shaping it as it exits to the WAN.
- Availability of the non-WAN interfaces (as arguments) is to facilitate preparations for migrating from one appliance model to another, or one deployment mode to another.

Examples

None.

snmp-server

Description

Use the **snmp-server** command to configure SNMP server options.

Syntax

snmp-server community <*community name*> [**ro**]
no snmp-server community

snmp-server contact <*name of contact*>
no snmp-server contact

snmp-server enable
no snmp-server enable

snmp-server enable traps
no snmp-server enable traps

snmp-server encrypt {**md5** | **sha**} {**plaintext** <*password*> | **prompt**}

snmp-server host <*IP address*> [**disable**]
no snmp-server host <*IP address*> [**disable**]

snmp-server host <*IP address*> **traps** [**version** <*traps version*>] <*community string*>

snmp-server listen enable
no snmp-server listen enable

snmp-server listen interface <*interface*>
no snmp-server listen interface <*interface*>

snmp-server location <*location of system*>
no snmp-server location

snmp-server traps event raise-alarm
no snmp-server traps event raise-alarm

Arguments

community <*community name*> [**ro**]	Configures the name for the SNMP read-only community, which is required to make SNMP queries. Use the **no** form of this command to reset the community string to its default.
contact <*name of contact*>	Sets a value for the *syscontact* variable in MIB-II. Use the **no** form of this command to clear the contents of the syscontact variable.
enable	Enables the SNMP server. Use the **no** form of this command to disable the SNMP server.
enable traps	Enables the sending of SNMP traps from this system. Use the **no** form of this command to disable sending of SNMP traps from this system.
encrypt {**md5** | **sha**}	Generate the encrypted form of the password from plain text, using one of the following hash types: • **md5** Message-Digest algorithm 5 (a hash function with a 128-bit hash value) • **sha** Secure Hash Algorithm, SHA-1
host <*IP address*>	Configures the hosts to which to send SNMP traps. Use the **no** form of this command to stop sending SNMP traps to a specified host.
host <*IP address*> **disable**	Temporarily disables sending of traps to this host. Use the **no** form of this command to reenable sending of SNMP traps to a specified host.
host <*IP address*> **traps** <*community string*>	Sends SNMP traps to the specified host. The community string noted here is also a community name (string name); it's used for particular trap destination hosts.
host <*IP address*> **traps version {1** | **2c**} <*community string*>	Specifies the SNMP version of traps to send to this host: • **1** is SNMPv1 • **2c** is SNMPv2c The community string noted here is also a community name (string name); it's used for particular trap destination hosts.
listen enable	Enables SNMP interface restriction access to this system. Use the **no** form of this command to disable SNMP interface restriction access to this system.
listen interface <*interface*>	Specifies the interface you want to add to the SNMP server access restriction list. The supported interfaces are **mgmt0** and **mgmt1**. Use the **no** form of this command to remove an interface to the SNMP server access restriction list.
location <*location of system*>	Specifies the value for the syslocation variable in MIB-II. Use the **no** form of this command to clear the contents of the syslocation variable.
plaintext <*password*>	Specifies the plaintext password to be encrypted.

prompt	Asks to specify the password securely with the following prompt, at which the user will enter text.
traps event raise-alarm	Generates a trap for each alarm that is raised and cleared. Use the **no** form of this command to negate this setting.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “snmp-server user v3” on page 204
- “show snmp” on page 338

Usage Guidelines

You need an SNMP manager application such as HP OpenView™ to browse the MIB II data and receive traps. There are many shareware and freeware SNMP manager applications available from the internet.

Examples

None.

snmp-server user v3

Description

Use the **snmp-server user v3** command to configure SNMP access on a per-user basis for v3 security parameters.

Syntax

snmp-server user <*username*> **v3 enable**
no snmp-server user <*username*> **v3 enable**

snmp-server user <*username*> **v3 auth** {**md5 | sha**} <*password*>

snmp-server user <*username*> **v3 auth** {**md5 | sha**} <*password*> **priv** {**des | aes-128**} [<*password*>]

snmp-server user <*username*> **v3 encrypted auth** {**md5 | sha**} <*password*>

snmp-server user <*username*> **v3 encrypted auth** {**md5 | sha**} <*password*> **priv** {**des | aes-128**} [<*password*>]

snmp-server user <*username*> **v3 prompt auth** {**md5 | sha**} <*password*>

snmp-server user <*username*> **v3 prompt auth** {**md5 | sha**} <*password*> **priv** {**des | aes-128**} [<*password*>]

Arguments

auth	Configures SNMP v3 security parameters, specifying passwords in plaintext on the command line. **NOTE:** Passwords are always stored encrypted.
auth {md5 | sha} <*password*>	Configures the use of either the MD5 or SHA-1 hash algorithm, and sets a plaintext password to use for authentication. If followed by a carriage return, it uses the default privacy algorithm, with the same privacy password as that specified here for authentication. The default privacy program is AES-128.
priv {des | aes-128} [<*password*>]	Configures the use of either DES or AES-128 encryption for privacy. • If you don't specify a password, it uses the same privacy password as that specified for authentication. • If you do specify a password, it is in plaintext.
enable	Enables SNMP v3 access for this user. Use the **no** form of this command to disable this user's SNMP v3 access.
encrypted	Configures SNMP v3 security parameters, specifying passwords in encrypted form.
prompt	Configures SNMP v3 security parameters, specifying passwords securely in follow-up prompt rather than on the command line.

Defaults

The default privacy (encryption) program is **AES-128**.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “snmp-server” on page 201
- “show snmp” on page 338

Usage Guidelines

- Only **admin** is allowed as an SNMP v3 user.
- Passwords must be at least eight (8) characters in length.

Examples

- To configure the passwords for **admin**’s SNMP v3 security paramenters as a follow-up after entering the command:

```
Tallinn2 (config) # snmp-server user admin v3 prompt auth md5 priv des
Auth password: ********
      Confirm: ********
Privacy password: **********
         Confirm: **********
Tallinn2 (config) #
```

ssl auth-certificate

Description

Use the **ssl auth-certificate** command to configure SSL certificate authority parameters.

Syntax

ssl auth-certificate delete all

ssl auth-certificate delete subject-name <*certificate subject name*>

ssl auth-certificate install cert-file <*certificate file or URL*>

ssl auth-certificate install pfx-file <*PFX file or URL*>

ssl auth-certificate install pfx-file <*PFX file or URL*> **mac-password** <*MAC password*>

ssl auth-certificate list [**brief** | **detail** | **subject-name** <*certificate subject name*>]

ssl auth-certificate list subject-name <*certificate subject name*> [**brief** | **detail**]

ssl auth-certificate list subject-name <*certificate subject name*> **issuer-name** <*certificate issuer name*> [**brief** | **detail**]

Arguments

delete all	Deletes all certificate authority data.
subject-name <*certificate subject name*>	Specifies certificate subject name.
issuer-name <*certificate issuer name*>	Specifies certificate issuer name.
install {cert-file <*certificate file or URL*> | **pfx-file** <*PFX file or URL*>}	Installs the certificate authority data by using either a certificate file or a PFX file.
key-passphrase <*private key file or URL*>	Specifies the private key pass phrase.
mac-password <*MAC password*>	Specifies the MAC password.
list	Lists the certificate authority data.
brief	Lists certificate authorities in brief format.
detail	Lists certificate authorities in detailed format.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssl builtin-signing” on page 208
- “ssl cert-substitution” on page 209
- “ssl host-certificate” on page 210
- “ssl signing-certificate” on page 212
- “ssl subs-certificate” on page 214
- “show ssl” on page 341

Usage Guidelines

None.

Examples

None.

ssl builtin-signing

Description

Use the **ssl builtin-signing** command to configure the SSL host to use the built-in certificate to sign.

Syntax

ssl builtin-signing {enable | disable}

Arguments

enable	Enables the SSL host to use the built-in certificate to sign.
disable	Disables the SSL host to use the built-in certificate to sign.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssl auth-certificate” on page 206
- “ssl cert-substitution” on page 209
- “ssl host-certificate” on page 210
- “ssl signing-certificate” on page 212
- “ssl subs-certificate” on page 214
- “show ssl” on page 341

Usage Guidelines

None.

Examples

None.

ssl cert-substitution

Description

Use the **ssl cert-substitution** command to configure SSL certificate substitution.

Syntax

ssl cert-substitution {enable | disable}

Arguments

enable	Enables the SSL certificate substitution.
disable	Disables the SSL certificate substitution.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssl auth-certificate” on page 206
- “ssl builtin-signing” on page 208
- “ssl host-certificate” on page 210
- “ssl signing-certificate” on page 212
- “ssl subs-certificate” on page 214
- “show ssl” on page 341

Usage Guidelines

None.

Examples

None.

ssl host-certificate

Description

Use the **ssl host-certificate** command to configure SSL host certificate parameters.

Syntax

ssl host-certificate delete all

ssl host-certificate delete subject-name <*certificate subject name*>

ssl host-certificate delete subject-name <*certificate subject name*> **issuer-name** <*certificate issuer name*>

ssl host-certificate install cert-file <*certificate file or URL*> **key-file** <*private key file or URL*> [**key-passphrase** <*private key file or URL*>]

ssl host-certificate install pfx-file <*PFX file or URL*>

ssl host-certificate install pfx-file <*PFX file or URL*> **mac-password** <*MAC password*> [**crypt-password** <*encryption password*>]

ssl host-certificate list [**brief** | **detail** | **subject-name** <*certificate subject name*>]

ssl host-certificate list subject-name <*certificate subject name*> [**brief** | **detail**]

ssl host-certificate list subject-name <*certificate subject name*> **issuer-name** <*certificate issuer name*> [**brief** | **detail**]

Arguments

delete all	Deletes all host certificate data.
subject-name <*certificate subject name*>	Specifies certificate subject name.
issuer-name <*certificate issuer name*>	Specifies certificate issuer name.
install {cert-file <*certificate file or URL*> | **pfx-file** <*PFX file or URL*>}	Installs the host certificate data by using either a certificate file or a PFX file.
key-file <*private key file or URL*>	Specifies the private key.
key-passphrase <*private key file or URL*>	Specifies the private key pass phrase.
mac-password <*MAC password*>	Specifies the MAC password
crypt-password <*encryption password*>	Specifies the encryption password
list	Lists the host certificate data.
brief	Lists certificate authorities in brief format.
detail	Lists certificate authorities in detailed format.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssl auth-certificate” on page 206
- “ssl builtin-signing” on page 208
- “ssl cert-substitution” on page 209
- “ssl signing-certificate” on page 212
- “ssl subs-certificate” on page 214
- “show ssl” on page 341

Usage Guidelines

None.

Examples

None.

ssl signing-certificate

Description

Use the **ssl signing-certificate** command to configure SSL signing certificate parameters.

Syntax

ssl signing-certificate delete all

ssl signing-certificate delete subject-name <*certificate subject name*>

ssl signing-certificate delete subject-name <*certificate subject name*> **issuer-name** <*certificate issuer name*>

ssl signing-certificate install cert-file <*certificate file or URL*> **key-file** <*private key file or URL*> [**key-passphrase** <*private key file or URL*>]

ssl signing-certificate install pfx-file <*PFX file or URL*>

ssl signing-certificate install pfx-file <*PFX file or URL*> **mac-password** <*MAC password*> [**crypt-password** <*encryption password*>]

ssl signing-certificate list [**brief** | **detail** | **subject-name** <*certificate subject name*>]

ssl signing-certificate list subject-name <*certificate subject name*> [**brief** | **detail**]

ssl signing-certificate list subject-name <*certificate subject name*> **issuer-name** <*certificate issuer name*> [**brief** | **detail**]

Arguments

delete all	Deletes all signing certificate data.
subject-name <*certificate subject name*>	Specifies certificate subject name.
issuer-name <*certificate issuer name*>	Specifies certificate issuer name.
install {cert-file <*certificate file or URL*> | **pfx-file** <*PFX file or URL*>}	Installs the host certificate data by using either a certificate file or a PFX file.
key-file <*private key file or URL*>	Specifies the private key.
key-passphrase <*private key file or URL*>	Specifies the private key pass phrase.
mac-password <*MAC password*>	Specifies the MAC password
crypt-password <*encryption password*>	Specifies the encryption password
list	Lists the host certificate data.
brief	Lists certificate authorities in brief format.
detail	Lists certificate authorities in detailed format.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssl auth-certificate” on page 206
- “ssl builtin-signing” on page 208
- “ssl cert-substitution” on page 209
- “ssl host-certificate” on page 210
- “ssl subs-certificate” on page 214
- “show ssl” on page 341

Usage Guidelines

None.

Examples

None.

ssl subs-certificate

Description

Use the **ssl subs-certificate** command to configure SSL substitute certificate parameters.

Syntax

ssl subs-certificate list [**brief** | **detail** | **subject-name** <*certificate subject name*>]

ssl subs-certificate list subject-name <*certificate subject name*> [**brief** | **detail**]

ssl subs-certificate list subject-name <*certificate subject name*> **issuer-name** <*certificate issuer name*> [**brief** | **detail**]

Arguments

subject-name <*certificate subject name*>	Specifies certificate subject name.
issuer-name <*certificate issuer name*>	Specifies certificate issuer name.
list	Lists the host certificate data.
brief	Lists certificate authorities in brief format.
detail	Lists certificate authorities in detailed format.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssl auth-certificate” on page 206
- “ssl builtin-signing” on page 208
- “ssl cert-substitution” on page 209
- “ssl host-certificate” on page 210
- “ssl signing-certificate” on page 212
- “show ssl” on page 341

Usage Guidelines

None.

Examples

None.

subnet

Description

Use the **subnet** command to configure subnets.

Use the **no** form of this command to remove a specific subnet.

Syntax

subnet <*ip prefix/length*> **advertize {enable | disable}**

subnet <*ip prefix/length*> **comment**

subnet <*ip prefix/length*> **exclude {enable | disable}**

subnet <*ip prefix/length*> **local {enable | disable}**

subnet <*ip prefix/length*> **metric** <*0-100*>

no subnet <*ip prefix/length*>

Arguments

<*ip prefix/length*>	Specifies IP address and subnet. For example, 10.0.10.0/24.
advertize	Subnet is ok to advertize.
advertize disable	Disables subnet advertizing.
advertize enable	Enables subnet advertizing.
comment	Adds a comments for a specified subnet entry.
exclude enable	Excludes a subnet from auto optimization.
exclude disable	Includes a subnet for auto optimization.
local	Subnet is local.
local disable	Disable local determination.
local enable	Enables local determination.
metric <*0-100*>	Specifies a subnet routing metric. Value can be between 0 and 100. Lower metric values have priority.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “subnet ipv6” on page 218.
- “show subnet” on page 345.

Usage Guidelines

Use these commands to build each appliance’s subnet table.

Examples

None.

subnet ipv6

Description

Use the **subnet ipv6** command to configure IPv6 subnets.

Use the **no** form of this command to remove a specific subnet.

Syntax

subnet ipv6 <*ip prefix/length*> **advertize {enable | disable}**

subnet ipv6 <*ip prefix/length*> **comment**

subnet ipv6 <*ip prefix/length*> **exclude {enable | disable}**

subnet ipv6 <*ip prefix/length*> **local {enable | disable}**

subnet ipv6 <*ip prefix/length*> **metric** <*0-100*>

no subnet ipv6 <*ip prefix/length*>

Arguments

<*ip prefix/length*>	Specifies IP address and subnet. For example, 10.0.10.0/24.
advertize	Subnet is ok to advertize.
advertise disable	Disables subnet advertizing.
advertise enable	Enables subnet advertizing.
comment	Adds a comments for a specified subnet entry.
exclude enable	Excludes a subnet from auto optimization.
exclude disable	Includes a subnet for auto optimization.
local	Subnet is local.
local disable	Disable local determination.
local enable	Enables local determination.
metric <*0-100*>	Specifies a subnet routing metric. Value can be between 0 and 100. Lower metric values have priority.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “subnet” on page 216.
- “show subnet” on page 345.

Usage Guidelines

Use these commands to build each appliance’s subnet table.

Examples

None.

system 10gigabit

Description

Use the **system 10gigabit** command to configure the appliance 10-Gigabit option.

Syntax

system 10gigabit {enable | disable}

Arguments

enable | disable	Globally enables or disables the 10-Gigabit option.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

This is applicable for platforms that have both 1Gbps and 10Gbps datapath interfaces. This includes the NX-9610, NX-8700, and NX-9700.

For example, the NX-9610 has 6 physical LAN/WAN interfaces and can run in one of two modes (either 4 x 1Gbps fiber interfaces ***or*** 2 x 10Gbps fiber interfaces). Use this command to switch between them. Also this command requires a reboot.

Examples

- To run the 2 x 10Gbps fiber interfaces:

```
(config) # system 10gigabit enable
```

- To run the 4 x 1Gbps fiber interfaces:

```
(config) # system 10gigabit disable
```

system arp-table-size

Description

Use the **system arp-table-size** command to configure the maximum system ARP table size.

Syntax

system arp-table-size <*maximum arp table size 1024 – 10240000*>

Arguments

<*maximum arp table size 1024 – 10240000*>	Configure maximum ARP table size. The range is 1024 to 10240000 entries.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

None.

Examples

None.

system auto-ipid

Description

Use the **system auto-ipid** command to configure the auto IP ID feature.

Syntax

system auto-ipid {**disable | enable**}

Arguments

disable	Disables the auto IP ID.
enable	Enables the auto IP ID.

Defaults

The default state is enabled.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system auto-subnet” on page 223
- “system auto-syn” on page 224
- “show system” on page 347

Usage Guidelines

This command is part of three auto-discovery strategies: auto IP ID, auto SYN, and auto-subnet. All three are enabled by default.

Examples

None.

system auto-subnet

Description

Use the **system auto-subnet** command to configure the auto-subnet feature.

Syntax

system auto-subnet add-local {**disable | enable**}

system auto-subnet add-local metric *<0 -100>*

system auto-subnet {**disable | enable**}

Arguments

add-local	Configures auto-subnet add-local capability.
add-local disable	Disables auto-subnet add-local capability.
add-local enable	Enables auto-subnet add-local capability.
metric *<0 -100>*	Configures auto-subnet add-local capability.
disable	Disables auto-subnet.
enable	Enables auto-subnet.

Defaults

The default state is enabled.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system auto-ipid” on page 222
- “system auto-syn” on page 224
- “show system” on page 347

Usage Guidelines

This command is part of three auto-discovery strategies: auto IP ID, auto SYN, and auto-subnet. All three are enabled by default.

Examples

None.

system auto-syn

Description

Use the **system auto-syn** command to configure the auto SYN feature.

Syntax

system auto-syn {**disable | enable**}

Arguments

disable	Disables auto SYN.
enable	Enables auto SYN.

Defaults

The default state is enabled.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system auto-ipid” on page 222
- “system auto-subnet” on page 223
- “show system” on page 347

Usage Guidelines

This command is part of three auto-discovery strategies: auto IP ID, auto SYN, and auto-subnet. All three are enabled by default.

Examples

None.

system auto-tunnel

Description

Use the **system auto-tunnel** command to configure the auto-tunnel option, which automatically creates tunnels between Silver Peak appliances that have network connectivity and active flows that traverse both appliances.

Syntax

system auto-tunnel {**disable | enable**}

Arguments

disable	Deactivates the Auto Tunnel feature.
enable	Activates the Auto Tunnel feature.

Defaults

This feature is disabled by default.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system auto-tunnel allow” on page 226
- “show system” on page 347

Usage Guidelines

None.

Examples

None.

system auto-tunnel allow

Description

Use the system auto-tunnel allow command to gain some security by specifying the subnets of appliance IP addresses with which you will allow auto-tunnels to be built. There is strict checking in place to prevent VXOA instances from attempting to create tunnels to anything but another VXOA instance. The **allow** command increases this security by having the user specify the only valid subnets used by remote Silver Peak VXOA instances.

Use the **no** form of this command to remove the auto-tunnel allowable subnet.

Syntax

system auto-tunnel allow <*network prefix*>/<*mask*> [<*network prefix*>/<*mask*>] [<*network prefix*>/<*mask*>]

no system auto-tunnel allow <*network prefix*>/<*mask*>

Arguments

None.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system auto-tunnel” on page 225
- “show system” on page 347

Usage Guidelines

None.

Examples

None.

system bandwidth

Description

Use the **system bandwidth** command to configure appliance bandwidth.

Syntax

system bandwidth max <*kbps*>

system bandwidth rx-target <*kbps*>

Arguments

max <*kbps*>	Configure maximum bandwidth for traffic transmitted to the WAN side in kilobits per second. This is a total of all tunnelized traffic and pass-through shaped traffic.
rx-target <*kbps*>	Configure the receive-side target bandwidth for the WAN interface.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

Receive-side bandwidth is an NX feature that prevents one appliance from overwhelming another appliance by sending it more data than the recipient can process.

Examples

To configure the appliance to transmit at a maximum bandwidth of 8000 kilobits per second:

```
(config) # system bandwidth max 8000
```

system bonding

Description

Use the **system bonding** command to configure the appliance etherchannel bonding option. When using a four-port Silver Peak appliance, you can bond pairs of Ethernet ports into a single port with one IP address per pair.

Syntax

system bonding {**disable | enable**}

Arguments

disable	Deactivates system bonding mode (processes all incoming traffic).
enable	Activates system bypass mode (bypasses all incoming traffic).

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

None.

Examples

None.

system bypass

Description

Use the **system bypass** command to configure the appliance bypass option. With this, the appliance mechanically isolates itself from the network, allowing traffic to flow without intervention.

Use the **no** form of this command to remove bypass capability when you've augmented and configured a virtual appliance's stock hardware with a Silicom BPVM or BPUSB card.

Syntax

system bypass {**disable | enable**}

system bypass type {**bpvm | bpusb**} **mac address** <*MAC address of interface to use*>

no system bypass

Arguments

disable	Deactivates system bypass mode (processes all incoming traffic).
enable	Activates system bypass mode (bypasses all incoming traffic).
type {bpvm | bpusb} mac address <*MAC address of interface to use*>	Configures the Silicom virtual bypass card's interface MAC address: • **bpvm** Silicom PCI Ethernet bypass adapter • **bpusb** Silicom USB Ethernet bypass adapter See Usage Guidelines.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See "show system" on page 347.

Usage Guidelines

Virtual appliances generally don't have a bypass card because they use stock hardware, like a Dell server. However, motivated customers can open up the server and add a Silicom card to get the same capabilities as one of Silver Peak's NX hardware appliances. Silicom calls this card BPVM.

As part of configuring the BPVM (part of a separate, documented procedure), you must indicate which network interface can be used to communicate with the card by specifying the MAC address.

Examples

To configure the appliance so that all traffic flows through the appliance without processing any of the traffic:

```
(config) # system bypass enable
```

system contact

Description

Use the **system contact** command to configure contact information for this appliance.

Syntax

system contact <*contact info*>

Arguments

<*contact info*>	Defines the contact information for the appliance.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

If you want to include spaces in the contact information, wrap the entire phrase in quotes.

Examples

To configure Sherlock Holmes as the system contact:

```
(config) # system contact “Sherlock Holmes”
```

system disk

Description

Use the **system disk** command to configure the appliance disk options.

Syntax

system disk encryption {**disable | enable**}

system disk <*disk ID*> {**insert | remove**}

Arguments

encryption disable	Disables disk encryption.
encryption enable	Enables disk encryption.
disk <*disk ID*>	The number of the system disk.
insert	To insert disk into RAID array.
remove	To remove disk from RAID array.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system disk” on page 45
- “show system” on page 347

Usage Guidelines

None.

Examples

None.

system dpc

Description

Use the **system dpc** command to configure Dynamic Path Control (DPC) for this appliance.

Syntax

system dpc tunnel-fail-behavior {disable | fail-back | fail-stick}

Arguments

tunnel-fail-behavior *<failover behavior>*	If there are parallel tunnels and one fails, then Dynamic Path Control determines where to send the flows. There are three failover behaviors.
disable	When the original tunnel fails, the flows aren't routed to another tunnel.
fail-back	When the failed tunnel comes back up, the flows return to the original tunnel.
fail-stick	When the failed tunnel comes back up, the flows don't return to the original tunnel. They stay where they are.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See "show system" on page 347.

Usage Guidelines

None.

Examples

None.

system hostname

Description

Use the **system hostname** command to configure host name for this appliance.

Syntax

system hostname <*hostname*>

Arguments

<*hostname*>	Designates the host name for the appliance.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

Hostnames may contain letters, numbers, periods ('.'), and hyphens ('-'), but may not begin with a hyphen. Hostnames cannot contain spaces.

Examples

None.

system igmp-snooping

Description

Use the **system igmp-snooping** command to configure bridge IGMP multicast snooping.

Syntax

system igmp-snooping {disable | enable}

Arguments

disable	Disables IGMP multicast snooping.
enable	Enables IGMP multicast snooping.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

IGMP snooping is a common layer-2 LAN optimization that filters the transmit of multicast frames only to ports where multicast streams have been detected. Disabling this feature floods multicast packets to all ports. IGMP snooping is recommended, and enabled by default.

Examples

None.

system int-hairpin

Description

Use the **system int-hairpin** command to configure the internal hairpinning feature.

Syntax

system int-hairpin {disable | enable}

Arguments

disable	Disables .
enable	Enables .

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

Hairpinning redirects inbound LAN traffic back to the WAN.

Examples

None.

system location

Description

Use the **system location** command to configure location information for this appliance.

Syntax

system location <*location info*>

Arguments

<*location info*>	Specifies the location information for the appliance.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

If you want to include spaces in the contact information, wrap the entire phrase in quotes.

Examples

To specify the appliance location as “Pittsburgh”:

```
(config) # system location Pittsburgh
```

To specify the appliance location as Earth (specified as a phrase):

```
(config) # system location “third rock from the sun”
```

system mode

Description

Use the **system mode** command to configure the appliance's mode (bridge or router) and next-hop IP. When using a 4-port appliance, you can configure two next-hops (one for each WAN interface).

Use the **no** form of the command to reset the router or bridge mode setting to its default.

Syntax

system mode bridge <*interface*> **inbound-max-bandwidth** <*BW in kbps*>

system mode bridge <*interface*> **outbound-max-bandwidth** <*BW in kbps*>

system mode bridge ip <*IP address*> <*netmask or mask length*> **nexthop** <*IP address*> [**second-ip** <*IP address*> <*netmask or mask length*> **second-nexthop** <*IP address*>]

system mode router <*interface*> **inbound-max-bandwidth** <*BW in kbps*>

system mode router <*interface*> **outbound-max-bandwidth** <*BW in kbps*>

system mode router ip <*IP address*> <*netmask or mask length*> **nexthop** <*IP address*> [**second-ip** <*IP address*> <*netmask or mask length*> **second-nexthop** <*IP address*>]

system mode router <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*>

system mode router <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*> <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*>

system mode router <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*> <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*>

system mode router <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*> <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*> <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*> <*interface*> <*IP address*> <*netmask or mask length*> **nh** <*IP address*>

system mode server

system mode server inbound-max-bandwidth <*BW in kbps*>

system mode server outbound-max-bandwidth <*BW in kbps*>

no system mode

Arguments

bridge	Configures Bridge (in-line) Mode
inbound-max-bandwidth <*BW in kbps*>	Configures the interface's inbound maximum bandwidth
ip <*IP address*>	Configures the appliance IP address.

<netmask or mask length>	Configures the appliance netmask or mask length.
nexthop *<IP address>*	Specifies the IP address of the: • WAN next-hop for virtual bridge (bridge mode) • router mode next-hop IP (router mode)
nh	Configures the Route mode next-hop
outbound-max-bandwidth *<BW in kbps>*	Configures the interface's outbound maximum bandwidth
router	Configures Router (out-of-path) Mode
second-ip *<IP address>*	Configures the appliance's second IP address for tunnel traffic.
second-nexthop *<IP address>*	Specifies the next-hop IP address that's associated with second IP address.
server	Configures Server Mode (single interface)

Defaults

The default system mode is bridge (in-line) mode.

Command Mode

Global Configuration Mode

See Also

See "show system" on page 347.

Usage Guidelines

None.

Examples

To configure an appliance with the IP addresss, 172.27.120.1 to be in router mode, with a netmask of 255.255.255.0 and a next-hop IP address of 172.27.120.2:

```
(config) # system mode router ip 172.27.120.1 /24 nexthop 172.27.120.2
```

To reset the system to the default (bridge) mode:

```
(config) # no system mode
```

system nat-all-inbound

Description

Use the **system nat-all-inbound** command to configure the inbound source NAT feature.

Syntax

system nat-all-inbound disable

system nat-all-inbound nat-ip {<*interface IP address*>** | auto}**

system nat-all-inbound nat-ip {<*interface IP address*>** | auto} fallback {enable | disable}**

Arguments

disable	Disables inbound source NAT.
nat-ip {<*interface IP address*>** | auto}**	Configures the inbound source NAT IP address.
fallback enable	Specifies fallback to the next available NAT IP address upon port exhaustion with the current NAT IP address.
fallback disable	Specifies not to fallback to the next available NAT IP address upon port exhaustion.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system nat-all-outbound” on page 241
- “show system” on page 347

Usage Guidelines

None.

Examples

None.

system nat-all-outbound

Description

Use the **system nat-all-outbound** command to configure the inbound source NAT feature.

Syntax

system nat-all-outbound disable

system nat-all-outbound nat-ip {<*interface IP address*>** | auto}**

system nat-all-outbound nat-ip {<*interface IP address*>** | auto} fallback {enable | disable}**

Arguments

disable	Disables outbound source NAT.
nat-ip {<*interface IP address*>** | auto}**	Configures the outbound source NAT IP address.
fallback enable	Specifies fallback to the next available NAT IP address upon port exhaustion with the current NAT IP address.
fallback disable	Specifies not to fallback to the next available NAT IP address upon port exhaustion.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system nat-all-inbound” on page 240
- “show system” on page 347

Usage Guidelines

None.

Examples

None.

system network-memory

Description

Use the **system network-memory** command to configure system network memory.

Syntax

system network-memory erase

system network-memory media ram

system network-memory media ram-and-disk

Arguments

erase	Erases system network memory.
media	Configures data store usage for RAM or RAM-and-disk.
ram	Network Memory data stored in RAM only
ram-and-disk	Network Memory data stored in RAM and disk.

Defaults

The default Network Memory mode is 0.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

None.

Examples

None.

system registration

Description

Use the **system registration** command to register the appliance with the Silver Peak portal.

Use the **no** form of this command to remove Silver Peak portal registration data.

Syntax

system registration <*Account Key*> <*Account Name*>

system registration <*Account Key*> <*Account Name*> <*Appliance Group Name*>

system registration <*Account Key*> <*Account Name*> <*Appliance Group Name*> <*Appliance Site Name*>

no system registration

Arguments

<*Account Key*>	Specifies the Account Key assigned by Silver Peak.
<*Account Name*>	Specifies the Account Name assigned by Silver Peak.
<*Appliance Group Name*>	Optional tag assigned by user for ease of identification.
<*Appliance Site Name*>	Optional tag assigned by user for ease of identification.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

None.

Examples

None.

system router

Description

Use the **system router** command to configure in-line router mode.

Use the **no** form of this command to remove in-line router mode in whole or in part.

Syntax

system router <*name*> **create interface** <*interface*> <*lan or wan*>
no system router <*name*>

system router <*name*> **dhcp**

system router <*name*> **dhcp vlan** <*VLAN ID*> [**harden** | **inbound-max-bw** <*BW in kbps*> | **label** <*interface label*> | **outbound-max-bw** <*BW in kbps*>]

system router <*name*> **ip** <*IP address*> [**harden** | **inbound-max-bw** <*BW in kbps*> | **label** <*interface label*> | **outbound-max-bw** <*BW in kbps*>]

system router <*name*> **ip** <*IP address*> <*netmask*> **nexthop** <*IP address*> [**vlan** <*VLAN ID*>]

no system router <*name*> **dhcp** [**vlan** <*VLAN ID*>]

no system router <*name*> **dhcp vlan** <*VLAN ID*> [**harden** | **label** <*interface label*>]

no system router <*name*> **ip** <*IP address*> {**harden** | **label** <*interface label*>}

Arguments

router <*name*>	Specifies the router name.
create interface <*physical interface*>	Specifies whether to create **lan0**, **wan0**, **lan1**, **wan1**, etc.
<*lan or wan*>	Refers to the LAN side or the WAN side.
dhcp	Adds DHCPv4.
vlan <*VLAN ID*>	Specifies the DHCPv4 VLAN ID.
harden	Enables interface hardening.
inbound-max-bw <*BW in kbps*>	Specifies the DHCPv4 VLAN inbound max bandwidth in kilobits per second.
label <*interface label*>	Specifies the DHCPv4 interface label.
outbound-max-bw <*BW in kbps*>	Specifies the DHCPv4 VLAN outbound max bandwidth in kilobits per second.
ip <*IP address*>	Specifies the router IP address
<*netmask*>	Specifies the netmask. For example, 255.255.255.0, or /24.
nexthop <*IP address*>	Specifies the Router mode next-hop.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “system mode” on page 238
- “show system” on page 347

Usage Guidelines

None.

Examples

None.

system routing

Description

Use the **system routing** command to configure interface routing.

Use the **no** form of this command to reset system-level routing information.

Syntax

system routing inline

system routing redundancy {default | none | lan-native | lan-native-vlan | lan-and-wan | all}

no system routing inline

Arguments

inline	Enables inline router mode.
redundancy	Configures redundancy of routes between interfaces.
default	LAN routing allowed between VLANs and native interfaces (equivalent to lan-native-vlan)
none	No routing allowed between interfaces
lan-native	LAN routing allowed between native interfaces (no routing allowed between VLANs)
lan-native-vlan	LAN routing allowed between VLANs and native interfaces
lan-and-wan	LAN and WAN routing allowed between native interfaces
all	LAN and WAN routing allowed between all interfaces (caveat: this may disrupt DPC)

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

None.

Examples

None.

system smb-signing

Description

Use the **system smb-signing** command to enable or disable SMB signing.

Syntax

system smb-signing {**disable | enable**}

Arguments

disable	Disables SMB Signing optimization.
enable	Enables SMB Signing optimization.

Defaults

The default is disabled.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “cifs signing delegation domain” on page 73
- “show cifs signing delegation” on page 271
- “show system” on page 347

Usage Guidelines

This command must be executed together with the **cifs signing delegation domain** command.

Examples

None.

system ssl-ipsec-override

Description

Use the **system ssl-ipsec-override** command to configure SSL IPSec override.

Syntax

system ssl-ipsec-override {**disable | enable**}

Arguments

disable	Deactivates the SSL IPSec override feature.
enable	Activates the SSL IPSec override feature.

Defaults

This feature is disabled by default.

Command Mode

Global Configuration Mode

See Also

See “show system” on page 347.

Usage Guidelines

None.

Examples

None.

traffic-class

Description

Use the **traffic-class** command to assign a name to a specific traffic class.

Use the **no** form of this command to remove a name from a traffic class.

Syntax

traffic-class <*1-10*> **name** <*name*>

no traffic-class <*traffic class id*>

Arguments

<*1-10*>	Specifies the number of the traffic class.
name <*name*>	Specifies the name to assign to a traffic class.
<*traffic class id*>	Specifies the number of the traffic class.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “shaper inbound” on page 197.

Usage Guidelines

None.

Examples

None.

wccp

Description

Use the **wccp** command to configure the Web Cache Communications Protocol (WCCP).

Use the **no** form of the command to remove a WCCP configuration.

Syntax

wccp {**enable** | **disable**}

wccp multicast-ttl <*1..15*>

wccp <*51..255*> **admin** {**up** | **down**}

wccp <*51..255*> **assignment method** {**hash** | **mask** | **either**}

wccp <*51..255*> **assignment method** {**hash** | **mask** | **either**} **assignment-detail** {**lan-ingress** | **wan-ingress**}

wccp <*51..255*> **assignment method** {**hash** | **mask** | **either**} **assignment-detail custom hash-srcip** {**enable** | **disable**} **hash-dstip** {**enable** | **disable**} **hash-srcport** {**enable** | **disable**} **hash-dstport** {**enable** | **disable**} **mask-srcip** <*32-bit value in hex*> **mask-dstcip** <*32-bit value in hex*> **mask-srcport** <*16-bit value in hex*> **mask-dstport** <*16-bit value in hex*>

wccp <*51..255*> **compatibility-mode** {**ios** | **nexus**}

wccp <*51..255*> **force-l2-return** {**enable** | **disable**}

wccp <*51..255*> **forwarding-method** {**gre** | **l2** | **either**}

wccp <*51..255*> **password** <*password*>

wccp <*51..255*> **router** <*IP address*> **protocol** {**tcp** | **udp**} **interface** {**lan0** | **wan0**}

wccp <*51..255*> **router** <IP *address*> **protocol** {**tcp** | **udp**} **interface** {**lan0** | **wan0**} **priority** <*0..255*> [**forwarding-method** {**gre** | **l2** | **either**}]

wccp <*51..255*> **router** <*IP address*> **protocol** {**tcp** | **udp**} **interface** {**lan0** | **wan0**} **priority** <*0..255*> **forwarding-method** {**gre** | **l2** | **either**} [**weight** <*0..65535*>]

wccp <*51..255*> **router** <*IP address*> **protocol** {**tcp** | **udp**} **interface** {**lan0** | **wan0**} **priority** <*0..255*> **forwarding-method** {**gre** | **l2** | **either**} **weight** <*0..65535*> [**password** <*password*>]

wccp <*51..255*> **weight** <*weight*>

no wccp <*51..255*>

Arguments

wccp <*51..255*>	Specifies a WCCP service group ID.
admin up	Enables a WCCP service group.
admin down	Disables a WCCP service group.
assignment-detail {**custom** | **lan-ingress** | **wan-ingress**}	Specifies the details of the service group assignment method. The options are: • **custom** – Assignment by custom values • **lan-ingress** – Assignment by hash default. Uses the source address for distribution • **wan-ingress** – Assignment by mask default. Uses the destination address for distribution in the router/L3 switch table.
assignment-detail custom	Specifies the details of the service group assignment method. The options are: • **hash-srcip {enable | disable}** – Enable/disable using the hash source IP • **hash-dstip {enable | disable}** – Enable/disable using the hash destination IP • **hash-srciport {enable | disable}** – Enable/disable using the hash source port • **hash-dstport {enable | disable}** – Enable/disable using the hash destination port • **mask-srcip** <*32-bit value in hex*> – Specifies the mask source IP as a 32-bit hex value • **mask-dstip** <*32-bit value in hex*> – Specifies the mask destination IP as a 32-bit hex value • **mask-srcport** <*16-bit value in hex*> – Specifies the mask source port as a 16-bit hex value • **mask-dstport** <*16-bit value in hex*> – Specifies the mask destination port as a 16-bit hex value
assignment-method {**hash** | **mask** | **either**}	Modifies the service group assignment method. This relates to how load balancing (of what packets go to which appliance) is set up with the router. The options are: • **hash** • **mask** • **either** – The assignment method is either hash or mask. In other words, the appliances will accept packets of either method from the router.
compatibility-mode {**ios** | **nexus**}	If a WCCP group is peering with a router running Nexus OS, then the appliance must adjust its WCCP protocol packets to be compatible. By default, the appliance is IOS-compatible.
disable	Disables the WCCP feature.
enable	Enables the WCCP feature.

force-l2-return	Modifies the service group's force L2 return. When WCCP has negotiated L3 forwarding and return methods, Force L2 Return can be used to strip the WCCP GRE header from any packets returned to the router (that is, pass-through traffic). This feature is not applicable if the negotiated forwarding method is L2. NOTE: Routing loops may occur if L2 returned packets are forwarded again to the appliance by a WCCP group.
forwarding-method {**gre** | **l2** | **either**}	Modifies the service group's forwarding method. The options are: • **GRE** forwarding method • **L2** forwarding method • **Either** forwarding method
interface {**lan0** | **wan0**}	Modifies service group interface.
multicast-ttl <*1..15*>	Sets the Time To Live (TTL) value. The range is 1–15.
password <*password*>	Sets a password for the WCCP service group.
service-grp <*51..255*>	Specifies a comma-delimited list of service group IDs.
router <*IP address*>	• Use comma separator to specify more than one IP. • Use the physical IP for L2 redirection. • Use the loopback IP for L3 redirection.
protocol {**tcp** | **udp**}	Configures the WCCP service group protocol for this router IP address.
priority <*0..255*>	Specifies the WCCP service group's priority. Values range from *0* to *255*.
weight <*0..100*>	Specifies the WCCP service group weight. *100* is the highest weight. When there is more than one appliance in a group, weight is used to distribute hash or mask assignment buckets on the router in order to load balance flows.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See "show wccp" on page 364.

Usage Guidelines

To generate output for the **assignment** and **detail** arguments, you must enable WCCP after configuration.

Examples

None.

CHAPTER 4

Monitoring Commands

This chapter describes monitoring commands. Monitoring commands display information about Silver Peak NX Series appliances.

monitor

Description

Use the **monitor** command to monitor interface bandwidth statistics.

Syntax

monitor <*interface*> [<*interface*>] [<*interface*>] [<*interface*>]

Arguments

<*interface*>	Specifies the interface name. You can specify up to 4 interfaces.

Defaults

None.

Command Mode

All levels

See Also

None.

Usage Guidelines

Once you execute the command, the output updates every second. To discontinue, use **Ctrl** + **C**.

The available interfaces include:

- wan0
- lan0
- mgmt0
- mgmt1
- wan1
- lan1

Examples

To monitor the lan0 and wan0 interfaces:

```
Tallinn (config) # monitor lan0 wan0
```

show aaa

Description

Use the **show aaa** command to display AAA authentication settings.

Syntax

show aaa

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show aaa
AAA authorization:
    Default User: admin
    Map Order: remote-first
Authentication method(s):
   local

Tallinn (config) #
```

show access-list

Description

Use the **show access-list** command to display all existing Access Control Lists (ACLs). You can also specify a particular ACL to display.

Syntax

show access-list

show access-list <*ACL name*>

Arguments

access-list	When followed by a carriage return, displays all ACLs.
access-list <*ACL name*>	Displays the configuration for the specified ACL.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- The following displays the rules in the ACL, *acl1*:

```
Tallinn (config) # show access-list acl1
ACL acl1 configuration

ID    Protocol Source              Destination         Action DSCP   Application
----- -------- ------------------- ------------------- ------ ------ -----------
   10 ip       any                 3.3.3.0/24          permit any    any
   20 ip       any                 any                 permit any    snowball
Tallinn (config) #
```

show alarms

Description

Use the **show alarms** command to display the details for all outstanding alarms.

Syntax

show alarms [<*alarm ID*> | **outstanding** | **summary**]

Arguments

alarms <*alarm ID*>	Specifies an alarm ID.
outstanding	Displays the outstanding alarm table.
summary	Shows a summary count of outstanding alarms.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

If you use the **show alarms** command without an argument, the CLI displays all outstanding alarms in detail.

Examples

- To view a list of all alarm details:

```
Tallinn (config) # show alarms
Alarm Details List:

Alarm Id:       1
Severity:       MAJ
Type:           EQU
Sequence Id:    5
Name:           equipment_gateway_connect
Description:    Datapath Gateway Connectivity Test Failed
Source:         system
Time:           2007/06/11 17:40:19
Acknowledged:   no
Active:         yes
Clearable:      no
Service Affect: yes
```

```
Alarm Id:       2
Severity:       CRI
Type:           TUN
Sequence Id:    4
Name:           tunnel_down
Description:    Tunnel state is Down
Source:         HQ-to-BranchA
Time:           2007/06/11 17:38:22
Acknowledged:   no
Active:         yes
Clearable:      no
Service Affect: yes

Alarm Id:       3
Severity:       MAJ
Type:           EQU
Sequence Id:    2
Name:           equipment_if_link_down
Description:    Network Interface Link Down
Source:         wan0
Time:           2007/06/11 17:37:09
Acknowledged:   no
Active:         yes
Clearable:      yes
Service Affect: yes
Tallinn (config) #
```

- To view a table of details for all outstanding alarms:

```
Tallinn (config) # show alarms outstanding
#   Seq  Date                Type  Sev A Source       Description
--- ---- ------------------- ----- --- - ------------ -----------------
  1    5 2007/06/22 18:53:38   EQU MAJ N system       Datapath Gateway
Connectivity Test Failed
  2    3 2007/06/22 18:51:37   TUN CRI N HQ-to-Branch Tunnel state is Down
  3    2 2007/06/22 18:50:28   EQU MAJ N wan0         Network Interface Link Down
```

show application

Description

Use the **show application** command to display custom (user-defined) applications, with their associated information for protocol, port(s), DSCP, and VLAN.

Syntax

show application

show application <*application priority*> [**flows** | **stats**]

show application [**brief** | **stats**]

show application name <*application name*>

Arguments

<*application priority*>	Displays the configuration for the application assigned this priority.
<*application priority*> **flows**	Displays flows that match this application.
<*application priority*> **stats**	Displays statistics for this application.
brief	Displays all user-defined applications.
name	Displays application by name.
stats	Displays statistics for all applications.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “application” on page 65.

Usage Guidelines

None.

Examples

- To display all user-defined applications:

```
tallinn3 (config) # show application
Application rule 10 configuration
  Application:       one_more
  Protocol:          tcp
```

```
  Src IP Range:
                     any
  Dst IP Range:
                     any
  Src Port Range:
                     any
  Dst Port Range:
                     any
  DSCP:              be
  VLAN:              any.any

Application rule 20 configuration
  Application:       another_one
  Protocol:          etherip
  Src IP Range:
                     any
  Dst IP Range:
                     172.50.50.0/24
  Src Port Range:
                     any
  Dst Port Range:
                     any
  DSCP:              any
  VLAN:              any.any

tallinn3 (config) #
```

- To view the details of the user-defined application, *one-more*, only:

```
tallinn3 (config) # show application name one_more
Application rule 10 configuration
  Application:       one_more
  Protocol:          tcp
  Src IP Range:
                     any
  Dst IP Range:
                     any
  Src Port Range:
                     any
  Dst Port Range:
                     any
  DSCP:              be
  VLAN:              any.any

tallinn3 (config) #
```

show application-builtin

Description

Use the **show application-builtin** command to display all of the appliance's built-in applications, along with their associated ports.

Syntax

show application-builtin

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show application-builtin

Application    Ports
------------   ------
          aol  5191-5193
       aol_im  4443,5190
      backweb  370
     cifs_smb  139,445
 cisco_skinny  2000-2001
       citrix  1494,1604
      cuseeme  7648-7652,24032
          dns  53
```

Only a small portion of the returned results are shown above.

show application-group

Description

Use the **show application-group** command to display a list of all application groups, or to display the contents of a specific application group.

Syntax

show application-group

show application-group <*application group name*>

show application-group <*application group name*> **debug**

Arguments

application-group <*application group name*>	Specifies the name of an existing application group.
debug	Displays debug information for the specific application group named.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

To get a list of the available application groups, enter the following command:

```
<silver-peak> # show application-group ?
```

Examples

- To display all existing application-groups within the appliance:

```
Tallinn (config) # show application-group
Application Group VoIP : cisco_skinny,h_323,sip
Application Group web : http,https
Tallinn (config) #
```

- To display the applications included in a specific application group:

```
Tallinn (config) # show application-group VoIP
```

```
Application Group VoIP : cisco_skinny,h_323,sip
Tallinn (config) #
```

- To display the debug information for the application group, *VoIP*:

```
Tallinn (config) # show application-group VoIP debug
Application-Group VoIP Debug Information

Tallinn (config) # h_323,sip,
Tallinn (config) #
```

show arp

Description

Use the **show arp** command to display the contents of the ARP cache.

Syntax

show arp [**static**]

show arp statistics

Arguments

static	Limits the returned results to all statically configured ARP entries, omitting the dynamic entries.
statistics	Displays all ARP cache statistics

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

If you use the **show arp** command with no arguments, the CLI displays all static and dynamic entries in the ARP cache.

Examples

```
Tallinn2 (config) # show arp
10.0.40.33 dev mgmt0 lladdr 00:1b:d4:73:ce:bf REACHABLE
1.1.1.1 dev wan0  INCOMPLETE
```

show banner

Description

Use **show banner** command to display the Message of the Day (MOTD) and Login message banners.

Syntax

show banner

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show banner
Banners:
    MOTD: Time for a margarita
    Login: How about some coffee?
Tallinn (config) #
```

show bootvar

Description

Use **show bootvar** command to display installed system images and boot parameters.

Syntax

show bootvar

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show bootvar
Installed images:
  Partition 1:
  hidalgo 2.0.0.0_15449 #1-dev 2007-05-30 06:12:39 x86_64 root@bigchief:unknown

  Partition 2:
  hidalgo 2.0.0.0_15619 #1-dev 2007-06-07 20:00:58 x86_64 root@bigchief:unknown

Last boot partition: 2
Next boot partition: 2
Tallinn (config) #
```

show bridge

Description

Use the **show bridge** command to display bridge information.

Syntax

show bridge

show bridge [brief]

show bridge interface {lan0 | wan0 | lan1 | wan1}

show bridge mac-address-table [**address** <*address*> | **bridge** <*bridge*> | **interface** <*interface*>]

Arguments

brief	Displays bridge information in brief format.
interface {lan0 | wan0 | lan1 | wan1}	Shows bridge port information.
mac-address-table	Shows bridge MAC address table.
address <*address*>	Shows bridge MAC address table information for a specific IP address.
bridge <*bridge*>	Shows bridge MAC address table information for a specific bridge (for example, **bvi0**).
interface <*interface*>	Shows bridge MAC address table information for a specific interface. The interface can be **lan0**, **wan0**, **lan1**, or **wan1**.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “bridge” on page 71.

Usage Guidelines

```
MAC table information is not available in router mode.
```

Examples

To display bridge information for the *lan1* interface:

```
Tallinn2 (config) # show bridge mac-address-table interface lan1
MAC Address       Dst Port   Learned Port Type            Age (s)
----------------- ---------- ------------ --------------- -------
00:e0:ed:0c:19:69 lan1       same         local             0.00
```

show cdp

Description

Use the **show cdp** command to display Cisco Discovery Protocol (CDP) information.

Syntax

show cdp

show cdp neighbors [detail]

show cdp traffic

Arguments

neighbor	Displays CDP neighbor entries.
neighbors detail	Displays detailed CDP neighbor information.
traffic	Shows CDP statistics.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “cdp” on page 72
- “clear” on page 15
- “interface cdp” on page 89
- “show interfaces cdp” on page 289

Usage Guidelines

None.

Examples

- To show the basic CDP settings:

```
Tallinn2 (config) # show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

- To display the CDP neighbors:

```
Tallinn2 (config) # show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce  Holdtme  Capability  Platform        Port ID
attilla          mgmt0          136      T           NX2500 20001    mgmt0
genghis          mgmt0          148      T           NX2500 20001    mgmt0
mykonos          mgmt0          166      T           SP-NX7500 20    mgmt0
houston          mgmt0          156      T           SP-NX7500       mgmt0
rome             mgmt0          175      T           SP-NX7500 20    mgmt0
chicago          mgmt0          169      T           SP-NX7500       mgmt0
santorini        mgmt0          136      T           SP-NX7500 20    mgmt0
lab-s3           mgmt0          138      R S          WS-C4503       GigabitEthe
rnet2/6
```

- To show CDP statistics:

```
Tallinn2 (config) # show cdp traffic
CDP counters:
        Total packets output: 990, Input: 9902
        Hdr syntax: 0, Chksum error: 0, No memory: 991
```

show cifs signing delegation

Description

Use the **show cifs signing delegation** command to display CIFS signing delegation status from the running configuration.

Syntax

show cifs signing delegation

show cifs signing delegation verify

Arguments

verify	Displays CIFS signing delegation status after verifying with the Active Directory Server.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “cifs signing delegation domain” on page 73.
- “system smb-signing” on page 247
- “show system” on page 347

Usage Guidelines

None.

Examples

None.

show cli

Description

Use the **show cli** command to display Command Line Interface options.

Syntax

show cli

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show cli
CLI current session settings
  Maximum line size:       8192
  Terminal width:          80 columns
  Terminal length:         24 rows
  Terminal type:           vt102
  Auto-logout:             2 hours 0 minutes 0 seconds
  Paging:                  disabled
  Show hidden config:      yes
  Confirm losing changes:  yes
  Confirm reboot/shutdown: no

CLI defaults for future sessions
  Auto-logout:             2 hours 0 minutes 0 seconds
  Paging:                  enabled
  Show hidden config:      yes
  Confirm losing changes:  yes
  Confirm reboot/shutdown: no
Tallinn (config) #
```

show clock

Description

Use the **show clock** command to display system time and date.

Syntax

show clock

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show clock
Time: 21:41:59
Date: 2007/06/16
Time zone: America North United_States Pacific
Tallinn (config) #
```

show cluster

Description

Use the **show cluster** command to display cluster information.

Syntax

show cluster

show cluster spcp

Arguments

cluster	Displays the cluster interface and the appliances in the cluster.
cluster spcp	Displays the Silver Peak Communication Protocol statistics.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “cluster” on page 77.
- “flow-redirection” on page 86
- “show flow-redirection” on page 283

Usage Guidelines

None.

Examples

None.

show configuration

Description

Use the **show configuration** command to display the commands necessary to recreate the active, saved configuration.

Syntax

show configuration [**full**]

show configuration files [<*filename*>]

show configuration [**running** | **running full**]

show configuration [**download status** | **upload status**]

Arguments

download status	Displays the status of a configuration file being downloaded to the appliance from a remote host.
files	Displays the names of the active and saved configuration files.
files [<*filename*>]	Displays the contents of the specified configuration file.
full	Displays commands to recreate the active, saved configuration, and includes commands that set default values.
running	Displays commands to recreate the current running configuration.
running full	Displays commands to recreate the current running configuration, and includes commands that set default values.
upload status	Displays the status of a configuration file being saved from the appliance to a remote host.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

To display the commands to recreate the active, saved configuration – **excluding** those commands that set default values:

```
> show configuration
```

To display the commands to recreate the active, saved configuration – **including** the commands that set default values:

```
> show configuration full
```

To display the commands to recreate the current, running configuration – **excluding** those commands that set default values:

```
> show configuration running
```

To display the commands to recreate the current, running configuration – **including** the commands that set default values:

```
> show configuration running full
```

To display a list of configuration files on the appliance:

```
Tallinn (config) # show configuration files
initial (active)
newBaseline
initial.bak
backup.1158658595322.287.NE
Tallinn (config) #
```

To display the contents of the configuration file, *newBaseline*:

```
> show configuration files newBaseline
```

show email

Description

Use the **show email** command to display email and notification settings.

Syntax

show email

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show email
Mail hub:
Mail hub port:  25
Domain:         silver-peak (default)

Failure events for which emails will be sent:
  raise-alarm: System Alarm has been raised

No recipients configured.

Autosupport emails
  Enabled: no
  Recipient:

  Mail hub:

Tallinn (config) #
```

show excess-flow

Description

Use the **show excess-flow** command to display information about flows exceeding the number that the appliance supports.

Syntax

show excess-flow

show excess flow log

Arguments

log	Displays a log of the excess flows.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

show files

Description

Use the **show files** command to display a list of available files and/or display their contents.

Syntax

show files debug-dump [<*filename*>]

show files job upload status

show files stats [<*filename*>]

show files system

show files tcpdump

show files upload status

Arguments

debug-dump [<*filename*>]	Displays the list of debug-dump files. If you specify a filename, the CLI displays the contents of the file. Debug dump files have the suffix, **.tgz**.
job upload status	Displays job-output file upload status. You would use this when running the **file job upload** command.
stats	Displays a list of statistics reports. Debug dump files have the suffix, **.csv**.
system	Displays information on user-visible file systems.
tcpdump	Displays tcpdump output files.
upload status	Displays files upload status.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See also.

Usage Guidelines

- If you use the **show files debug-dump** command without the argument, the CLI displays a list of available debug dump files.

Examples

- To display a list of debug-dump files:

```
Tallinn2 (config) # show files debug-dump
sysdump-RDT-2612-2-20070814-101408.tgz
sysdump-RDT-2612-2-20070820-031350.tgz
tunbug-Tallinn2-20090109.tar
sysdump-RDT-2612-2-20070822-231449.tgz
sysdump-RDT-2612-2-20070910-094351.tgz
tunbug-Tallinn2-20090102.tar.gz
tunbug-Tallinn2-20090103.tar.gz
tunbug-Tallinn2-20090104.tar.gz
tunbug-Tallinn2-20090105.tar.gz
tunbug-Tallinn2-20090106.tar.gz
tunbug-Tallinn2-20090107.tar.gz
tunbug-Tallinn2-20090108.tar.gz
Tallinn2 (config) ##
```

show flow-debug

Description

Use the **show flow-debug** command to display the flow-debug summary for the specified flow.

Syntax

show flow-debug

show flow-debug description

show flow-debug detail

Arguments

description	Displays the names of the statistics, along with their definitions.
detail	Displays the detailed state of the selected flow.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “flow-debug” on page 383.

Usage Guidelines

If multiple flows fit the criteria for the configured and enabled **flow-debug** command, then only the first match displays.

Examples

```
None.
```

show flow-export

Description

Use the **show flow-export** command to display the NetFlow flow export configuration parameters.

Syntax

show flow-export

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “flow-export” on page 84.

Usage Guidelines

None.

Examples

```
Tallinn2 # show flow-export
Flow export v5 disabled:
  no valid collectors are configured.
  active-flow-timeout    : 1 m
  engine-id              : 1
  engine-type            : 1
  interface              : WANTX

  0 flows exported in 0 udp datagrams
Tallinn2 #
```

show flow-redirection

Description

Use the **show flow-redirection** command to display the flow redirection state and statistics.

Syntax

show flow-redirection

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “cluster” on page 77
- “show flow-redirection” on page 283
- “show cluster” on page 274

Usage Guidelines

None.

Examples

```
Tallinn2 # show flow-redirection

Flow Redirection is disabled

Tallinn2 #
```

show hosts

Description

Use the **show hosts** command to display hostname, DNS (Domain Name Server) configuration, and static host mappings.

Syntax

show hosts

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show hosts
Hostname: Tallinn
Name server: 172.2.2.2 (configured)
Name server: 10.50.98.4 (configured)
Name server: 134.55.66.77 (configured)
Domain name: silver-peak (configured)
Domain name: rotorrouter (configured)
Domain name: chacha (configured)
Domain name: airborne (configured)
Domain name: roger (configured)
IP 127.0.0.1 maps to hostname localhost
Tallinn (config) #
```

show iflabels

Description

Use the **show iflabels** command to display the labels available for interfaces.

Syntax

show iflabels [**lan-labels** | **wan-labels**]

Arguments

lan-labels	Displays LAN interface labels.
wan-labels	Displays WAN interface label.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

To display information about the system images and boot parameters for the appliance, *Tallinn*:

```
laine2-vxa (config) # show iflabels
Interface Labels:
LAN interface Labels:
--------------------

Label    Display Name
4        Voice
5        Data

WAN interface Labels:
---------------------
Label    Display Name
1        MPLS
2        Internet
3        LTE

laine2-vxa (config) #
```

show image

Description

Use the **show image** command to display information about system images and boot parameters.

Syntax

show image [**status**]

Arguments

status	Displays system image installation status.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

To display information about the system images and boot parameters for the appliance, *Tallinn*:

```
Tallinn (config) # show image
Installed images:
  Partition 1:
  hidalgo 2.0.0.0_15449 #1-dev 2007-05-30 06:12:39 x86_64 root@bigchief:unknown

  Partition 2:
  hidalgo 2.0.0.0_15619 #1-dev 2007-06-07 20:00:58 x86_64 root@bigchief:unknown

Last boot partition: 2
Next boot partition: 2
Tallinn (config) #
```

show interfaces

Description

Use the **show interfaces** command to display the detailed running state for any or all interfaces.

Syntax

show interfaces [**brief** | **configured**]

show interfaces [<*interface*>]

Arguments

show interfaces	Displays the detailed running state for **all** interfaces.
interfaces brief	Displays the brief running state for **all** interfaces.
interfaces configured	Displays the configuration for **all** interfaces.
interfaces <*interface*>	Shows the detailed running state for the specified interface, only.

Defaults

None.

Command Mode

User EXEC Mode [**only** usable for the **show interfaces** command when it takes no arguments]

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces pass-through” on page 291
- “show interfaces tunnel” on page 294

Usage Guidelines

For a list of all the available interfaces only, login in Privileged EXEC Mode or Global Configuration Mode, and enter the following command:

```
Silver-Peak # show interfaces ?
```

Examples

- To show the detailed running state for lan0.

```
Tallinn (config) # show interfaces lan0
Interface lan0 state
```

```
   Admin up:           no
   Link up:            no
   IP address:
   Netmask:
   Speed:              UNKNOWN
   Duplex:             UNKNOWN
   Interface type:     ethernet
   MTU:                1500
   HW address:         00:0C:BD:00:7F:4B

   RX bytes:           0
   RX packets:         0
   RX mcast packets:   0
   RX discards:        0
   RX errors:          0
   RX overruns:        0
   RX frame:           0

   TX bytes:           0
   TX packets:         0
   TX discards:        0
   TX errors:          0
   TX overruns:        0
   TX carrier:         0
   TX collisions:      0
Tallinn (config) #
```

show interfaces cdp

Description

Use the **show interfaces cdp** command to display Cisco Discovery Protocol (CDP) information related to a specific interface.

Syntax

show interfaces <*interface*> **cdp**

show interfaces <*interface*> **cdp neighbors** [**detail**]

Arguments

interfaces <*interface*>	Shows the CDP state for the specified interface, only.
neighbors	Displays the CDP neighbors that are connected to this interface.
neighbors detail	Displays detailed information about the CDP neighbors that are connected to this interface.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show cdp” on page 269
- “cdp” on page 72
- “interface cdp” on page 89
- “clear” on page 15

Usage Guidelines

None.

Examples

- To display basic CDP information about a network interface:

```
Tallinn2 (config) # show interfaces wan0 cdp
CDP is enabled on interface wan0
```

- To display detailed information about **wan0**'s CDP neighbors:

```
Tallinn2 (config) # show interfaces wan0 cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce  Holdtme  Capability  Platform        Port ID
```

show interfaces pass-through

Description

Use the **show interfaces pass-through** command to display detailed state of pass-through traffic.

Syntax

show interfaces pass-through

show interfaces pass-through configured

show interfaces pass-through stats {**flow** [*<traffic class 1-10>*] | **qos** [*<DSCP value>*] | **traffic-class**}

Arguments

configured	Displays the pass-through traffic configuration.
stats flow	Displays pass-through traffic flow metrics for the default traffic class.
stats flow *<traffic class 1-10>*	Displays pass-through traffic flow metrics for the specified traffic class.
stats qos	Displays the default pass-through QoS statistics. The default DSCP value is **be** (best effort).
stats qos *<DSCP value>*	Displays pass-through QoS statistics for the specified DSCP value.
stats traffic-class	Displays pass-through traffic class statistics.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces” on page 287
- “show interfaces tunnel” on page 294

Usage Guidelines

This command’s functionality is the same as “show pass-through” on page 323 .

Examples

- To display the detailed state of pass-through traffic:

```
Tallinn (config) # show interfaces pass-through
Pass-through traffic state
  Minimum Bw:    32
  Maximum Bw:    10000

  Tx Bytes:      258
  Tx Pkts:       2
Tallinn (config) #
```

- To display the pass-through traffic configuration:

```
Tallinn (config) # show interfaces pass-through configured
Pass-through traffic configuration
  Minimum Bw:    32
  Maximum Bw:    10000

Traffic Class:
  ID  Priority  Min Bw  Max Bw  Weight
  1     5       500000  1000000   1
  2     10      0       1000000   1
  3     10      0       1000000   1
  4     10      0       1000000   1
  5     10      0       1000000   1
  6     10      0       1000000   1
  7     10      0       1000000   1
  8     10      0       1000000   1
  9     10      0       1000000   1
  10    10      0       1000000   1

Traffic Class Queue Max:
  ID  Packets   Bytes        Flow Pkts  Flow Bytes     Wait (ms)
  1     2000    3000000         2000    3000000         500
  2     500     500000           100     100000         500
  3     500     500000           100     100000         500
  4     500     500000           100     100000         500
  5     500     500000           100     100000         500
  6     500     500000           100     100000         500
  7     500     500000           100     100000         500
  8     500     500000           100     100000         500
  9     500     500000           100     100000         500
  10    500     500000           100     100000         500
Tallinn (config) #
```

- To display statistics for pass-through traffic with a DSCP marking of Best Effort:

```
eh-3500-1 (config) # show interfaces pass-through stats qos
Tunnel pass-through QOS be Statistics:
 RX bytes:              107077          TX bytes:              68360
 RX packets:            1081            TX packets:            692

 RX processed packets:  0
 RX process bytes:      0

 RX invalid packets:                     0
 RX lost packets:                        0
 RX duplicate packets:                   0

 RX error correcting packets:            0
 TX error correcting packets:            0

 RX error correcting bytes:              0
 TX error correcting bytes:              0

 RX packets lost before error correction: 0
 RX packets lost after error correction:  0

 RX reconstructed packets in order:      0
 RX reconstructed packets out of order:  0

 RX out of order packets accepted:       0
 RX out of order packets dropped:        0
 RX out of order packets reordered:      0

 RX packets with 1 packet:               0
 Tx packets with 1 packet:               0

 RX packets with 1 fragment:             0
 TX packets with 1 fragment:             0

 RX packets with > 1 packet no fragment:  0
 TX packets with > 1 packet no fragment:  0

 RX packets with > 1 packet and fragment: 0
 TX packets with > 1 packet and fragment: 0
eh-3500-1 (config) #
```

show interfaces tunnel

Description

Use the **show interfaces tunnel** command to display detailed running state for any and all tunnels.

Syntax

show interfaces tunnel [**brief | configured | peers | summary**]

show interfaces tunnel <*tunnel name*> [**brief | configured | fastfail | ipsec** [**status**] | **summary**]

show interfaces tunnel <*tunnel name*> **stats flow** [<*traffic class 1-10*>]

show interfaces tunnel <*tunnel name*> **stats ipsec**

show interfaces tunnel <*tunnel name*> **stats latency**

show interfaces tunnel <*tunnel name*> **stats qos** [<*DSCP value*>]

show interfaces tunnel <*tunnel name*> **stats traffic-class**

Arguments

brief	Displays brief running state for the tunnel(s).
configured	Displays configuration for the tunnel(s).
fastfail	Displays Fastfail information. When multiple tunnels are carrying data between two appliances, this feature determines on what basis to disqualify a tunnel from carrying data, and how quickly.
peers	Displays table summary information for all tunnel peers.
redundancy	Displays redundancy information (regarding WCCP or VRRP) for the tunnel(s).
summary	Displays summary information for the tunnel(s).
tunnel <*tunnel name*>	Displays the detailed running state for this tunnel.
ipsec status	Displays the specified tunnel's IPSec information.
stats flow	Displays the flow metrics for the default traffic class in the designated tunnel.
stats flow <*traffic class 1-10*>	Displays the flow metrics for the specified traffic class in the designated tunnel.
stats ipsec	Displays the IPSec statistics for the designated tunnel.
stats latency	Displays the latency metrics for the designated tunnel.
stats qos	Displays the default QoS statistics for the designated tunnel. The default DSCP value is **be** (best effort).

stats qos <*DSCP value*>	Displays the QoS statistics for the specified DSCP value in the designated tunnel.
stats traffic-class	Displays the traffic class statistics for the designated tunnel.

Defaults

- The default DSCP value for QoS is **be** (Best Effort).

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show interfaces” on page 287
- “show interfaces pass-through” on page 291
- “show tunnel” on page 355

Usage Guidelines

- If you don’t specify a tunnel, then the output includes information for **all** tunnels.
- If you do specify a tunnel, then the output is limited to that tunnel.
- This command is equivalent to the **show tunnel** command.

Examples

- To display summary information for the tunnel, “HQ-to-Branch”:

```
Tallinn (config) # show interfaces tunnel HQ-to-BranchA summary
Tunnel                          Admin Oper         Remote IP        Uptime
------------------------------- ----- ------------ ---------------- --------
HQ-to-BranchA                   up    Down         172.30.5.2       0s
Tallinn (config) #
```

- To display the IPSec status information for the tunnel, “HQ-to-Branch”:

```
Tallinn (config) # show interfaces tunnel HQ-to-BranchA ipsec status
Tunnel HQ-to-BranchA ipsec state
  Tunnel Oper:          Down
  IPSec Enabled:        no
  IPSec Oper:           Disabled
  Total IPSec SAs:      in:0 out:0
Tallinn (config) #
```

- To display the traffic class statistics for the tunnel, “gms_dm-vx3000a_dm-vx3000b”:

```
dm-vx3000a (config) # show interfaces tunnel gms_dm-vx3000a_dm-vx3000b stats
traffic-class
show request for tunnel gms_dm-vx3000a_dm-vx3000b
Tunnel gms_dm-vx3000a_dm-vx3000b traffic class statistics
   tc name                      LAN RX     LAN RX      WAN TX      WAN TX  QOS Drops
Misc.Drops
                               Packets      Bytes     Packets        Kbps    Packets
Packets
    1 default                        0          0           0           0          0          0
    2 real-time                      0          0           0           0          0          0
    3 interactive                    0          0           0           0          0          0
    4 best-effort             32132609 46538966888    16922817 23465651199          0
0
    5                                0          0           0           0          0          0
    6                                0          0           0           0          0          0
    7                                0          0           0           0          0          0
    8                                0          0           0           0          0          0
    9                                0          0           0           0          0          0
   10                                0          0           0           0          0          0
dm-vx3000a (config) #
```

- To display the latency statistics for traffic in the tunnel, “tunnel-2-8504”:

```
eh-3500-1 (config) # show interfaces tunnel tunnel-2-8504 stats latency
Tunnel tunnel-2-8504 QOS 0 Latency Metrics:
 Minimum Round Trip Time :                1
 Maximum Round Trip Time :                4
 Average Round Trip Time :                2
eh-3500-1 (config) #
```

show interfaces vrrp

Description

Use the **show interfaces vrrp** command to display the detailed running state for all VRRPs.

Syntax

show interfaces <*interface*> **vrrp**

show interfaces <*interface*> **vrrp** {**brief** | **configured**}

show interfaces <*interface*> **vrrp** <*1-255*> {**brief** | **configured**}

Arguments

interfaces <*interface*>	Shows the running state for the specified interface, only.
vrrp	Displays the detailed running state for all VRRPs.
brief	Displays brief running state info for all VRRPs.
configured	Display configured info for all VRRPs on this interface.
<*1-255*>	A specific VRRP Group ID.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “interface vrrp” on page 126.

Usage Guidelines

None.

Examples

None.

show ip

Description

Use the **show ip** command to display IP-related information.

Syntax

show ip datapath route

show ip default-gateway [**static**]

show ip mgmt-ip

show ip route [**static**]

Arguments

datapath route	Displays the datapath routing table.
default-gateway	Displays the active default route.
default-gateway static	Displays the configured default route.
mgmt-ip	Displays the management IP address
route	Displays the routing table.
route static	Displays the configured static routes.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

If you're using DHCP for **mgmt0**, then it displays, **`Management IP address: <none>`**.

Examples

To display the active default datapath route:

```
Tallinn (config) # show ip default-gateway
Active default gateway: 10.0.52.5
Tallinn (config) #
```

show jobs

Description

Use the **show jobs** command to display job configuration and status.

Syntax

show jobs [<*job ID*>]

Arguments

jobs <*job ID*>	Displays the configuration and status for the specified job.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

To display a list of available jobs, enter the following command:

```
<silver peak> # show jobs ?
```

Examples

None.

show licenses

Description

Use the **show licenses** command to display the installed licenses and licensed features.

Syntax

show licenses

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show licenses
No licenses have been configured.
Tallinn (config) #
```

show log

Description

Use the **show log** command to view event log contents.

Syntax

show log

show log alert
show log alert continuous
show log alert files [<*file number*>]
show log alert files <*file number*> [**matching** <*regular expression*>]
show log alert matching <*regular expression*>

show log continuous [**matching** <*regular expression*>]
show log continuous not matching <*regular expression*>

show log files [<*file number*>]
show log files <*file number*> **matching** <*regular expression*>
show log files <*file number*> **not matching** <*regular expression*>

show log matching <*regular expression*>
show log not matching <*regular expression*>

Arguments

alert	Displays alert event logs.
continuous	Displays new log messages as they arrive.
files	Displays a listing of all available **archived** log files.
files <*file number*>	Specifies which **archived** log file number to display.
matching <*regular expression*>	Displays event logs that match a given regular expression. If the expression includes spaces, use quotation marks to enclose the expression.
not matching <*regular expression*>	Displays event logs that **do not** match a given regular expression. If the expression includes spaces, use quotation marks to enclose the expression.

Defaults

- Without arguments, the command, **show log**, displays the ***current event log*** in a scrollable pager.
- The command, **show log alert**, displays the ***current alerts log in*** a scrollable pager.
- The appliance keeps up to 30 archived alert log files. The older the file, the higher the file number. The newest file has no number, and the most recent archived file is numbered, “1”.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

To see what archived logs are available, use one of the following:

```
(config) # show log files ?
(config) # show log alert files ?
```

Examples

- To show a list of all available alert log files:

```
Tallinn (config) # show log files
1
2
Tallinn (config) #
```

- To show all archived files that match the expression, “ping”, in any string:

```
Tallinn (config) # show log matching ping

r dumping
Jun 17 17:24:45 localhost rename_ifs: Mapping MAC: 00:0C:BD:00:7F:4A to
interface name: wan0
Jun 17 17:24:45 localhost rename_ifs: Mapping MAC: 00:0C:BD:00:7F:4B to
interface name: lan0
Jun 17 17:24:45 localhost rename_ifs: Mapping MAC: 00:E0:81:2F:85:98 to
interface name: mgmt0
Jun 17 17:24:45 localhost rename_ifs: Mapping MAC: 00:E0:81:2F:85:99 to
interface name: mgmt1
Jun 17 17:25:09 Tallinn sysd[798]: TID 1084225888: [sysd.NOTICE]: WDOG: Gateway
datapath ping test disabled when in BYPASS.
Jun 17 17:28:09 Tallinn sysd[798]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAILED: 2
Jun 17 17:29:09 Tallinn sysd[798]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAILED: 2
Jun 17 17:30:09 Tallinn sysd[798]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAILED: 2
Jun 17 17:33:09 Tallinn sysd[798]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAILED: 2
Jun 17 17:34:09 Tallinn sysd[798]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAILED: 2
Jun 17 17:34:24 Tallinn cli[2411]: [cli.NOTICE]: user admin: Executing command:
show log matching ping
/tmp/messages_filtered-rvzGgG lines 39947-39958/39958 (END)
```

- To view new alert log messages as they arrive:

```
Tallinn (config) # show log continuous
```

- To view the #3 archived alert log file:

```
(config) # show log alert files 3
```

show log audit

Description

Use the **show log audit** command to view audit log contents.

This log lists all configuration changes (create, modify, delete) and all system actions such as login/logout made by any users (CLI, Appliance Manager, or GMS). Each log entry contains a timestamp, the appliance hostname, the username and IP address of the user, the action or change applied, and whether the operation succeeded or failed.

Syntax

show log audit

show log audit continuous

show log audit files [<*file number*>]

show log audit files <*file number*> [**matching** <*regular expression*>]

show log audit matching <*regular expression*>

Arguments

continuous	Displays new log messages as they arrive.
files	Displays a listing of all available **archived** log files.
files <*file number*>	Specifies which **archived** log file number to display.
matching <*regular expression*>	Displays event logs that match a given regular expression. If the expression includes spaces, use quotation marks to enclose the expression.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

To see what archived logs are available, use one of the following:

```
(config) # show log audit files ?
```

Examples

- To view new alert log messages as they arrive:

```
Tallinn (config) # show log audit continuous
```

- To view the #6 archived audit log file:

```
(config) # show log audit files 6
```

show log-files

Description

Use the **show log-files** command to display the a specific log listing.

Syntax

show log-files <*file number*> [**list matching** <*regular expression*>]

Arguments

log-files <*file number*>	Specifies a file number for which to display a log listing.
list matching <*regular expression*>	Lists selected log lines that match the given expression.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To see what log files are available:

```
Tallinn (config) # show log-files ?
<file number>
1
2
Tallinn (config) #
```

- To list log lines in the archived log file, “1”, that match the expression “system”:

```
Tallinn (config) # show log-files 1 list matching system
Dec 14 19:38:53 Tallinn mgmtd[850]: [mgmtd.ALERT]: ALARM RAISE: WARN,SW,9,
system_shutdown,System shutdown has been initiated,System,2006/12/14
19:38:53,1,no,no,yes,yes.
Dec 14 19:39:00 Tallinn shutdown: shutting down for system reboot
Dec 14 19:41:49 localhost kernel: SCSI subsystem initialized
```

```
Dec 14 19:41:49 localhost kernel: VFS: Mounted root (ext3 filesystem) readonly.
Dec 14 19:41:49 localhost mdinit: Running system image: hidalgo 2.0.0.0_13180
#1-dev 2006-12-14 07:0
5:03 x86_64 root@bigchief:unknown
Dec 14 19:41:43 localhost rc.sysinit: Checking root filesystem succeeded
Dec 14 19:41:43 localhost rc.sysinit: Remounting root filesystem in read-write
mode:  succeeded
Dec 14 19:41:43 localhost fsck: Checking all file systems.
Dec 14 19:41:43 localhost rc.sysinit: Checking filesystems succeeded
Dec 14 19:41:43 localhost rc.sysinit: Mounting local filesystems:  succeeded
Dec 14 19:41:59 Tallinn mdinit: Shutting down system logger:
Dec 14 19:42:13 Tallinn mgmtd[849]: [mgmtd.ALERT]: ALARM RAISE: CRI,EQU,2,
equipment_system_bypass,S
ystem BYPASS mode,System,2006/12/14 19:42:13,1,no,yes,no,no. NIC fail-to-wire
mode - BYPASS
Dec 14 19:43:23 Tallinn mgmtd[849]: [mgmtd.ALERT]: ALARM CLEAR: CRI,EQU,4,
equipment_system_bypass,System BYPASS mode,System,2006/12/14
19:42:13,2,no,yes,no,no. NIC fail-to-wire mode - NORMAL
Dec 14 19:44:23 Tallinn mgmtd[849]: [mgmtd.ALERT]: ALARM RAISE: MAJ,EQU,5,
equipment_gateway_connect,Datapath Gateway Connectivity Test
Failed,system,2006/12/14 19:44:23,1,no,yes,no,yes. Datapath Gateway
Connectivity Test Failed
Dec 26 15:45:21 Tallinn mgmtd[849]: [mgmtd.ALERT]: ALARM RAISE: WARN,SW,6,
system_shutdown,System shutdown has been initiated,System,2006/12/26
15:45:21,1,no,no,yes,yes.
Dec 26 15:45:26 Tallinn shutdown: shutting down for system reboot
lines 1-16
```

show log-list matching

Description

Use the **show log-list matching** command to list event log lines that match the specified expression.

Syntax

show log-list matching <*regular expression*>

Arguments

matching <*regular expression***>**	Lists selected log lines that match the given expression.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

show logging

Description

Use the **show logging** command to display the logging configuration.

Syntax

show logging

show logging facilities

show logging files upload status

show logging tech-support

Arguments

facilities	Displays the log facilities configuration.
files upload status	Displays the progress of a logging file that's being saved to a remote host.
tech-support	Displays log entries that the appliance creates for tech support.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- "show tech-support" on page 353
- "tech-support create job" on page 414

Usage Guidelines

None.

Examples

- To view the logging configuration:

```
Tallinn (config) # show logging
Local logging level: notice
Default remote logging level: notice
No remote syslog servers configured.
Allow receiving of messages from remote hosts: no
Number of archived log files to keep: 30
Log rotation size threshold: 50 megabytes
Log format: standard
Levels at which messages are logged:
  CLI commands: notice
Tallinn (config) #
```

- To monitor the progress of a logging files as it's being copied from the appliance to a remote host.

```
Tallinn (config) # show logging files upload status
File Upload Status
  Name:                -not set-
  Status:              Ready
  Last Upload Status:  The system is ready for upload
  Start time:          -not set-
  End time:            -not set-
  Total upload size:   0
  Transferred size:    0
  Transfer rate:       0 bps
  Percent complete:    0%
Tallinn (config) #
```

- To view the information saved for tech support:

```
Tallinn (config) # show logging tech-support
Apr 22 01:15:15 Tallinn sysd[781]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAIL
ED: 2
Apr 22 01:15:20 Tallinn tunneld[779]: TID 182912294944: [tunneld.ERR]:
cipsec_recovery_statemachine:
Took IPSec recovery action - tunnel:Tallinn_to_Helsinki still down..
Apr 22 01:16:10 Tallinn tunneld[779]: TID 182912294944: [tunneld.ERR]:
cipsec_recovery_statemachine:
Took IPSec recovery action - tunnel:Tallinn_to_Helsinki still down..
Apr 22 01:16:15 Tallinn sysd[781]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAIL
ED: 2
Apr 22 01:17:00 Tallinn tunneld[779]: TID 182912294944: [tunneld.ERR]:
cipsec_recovery_statemachine:
Took IPSec recovery action - tunnel:Tallinn_to_Helsinki still down..
Apr 22 01:17:15 Tallinn sysd[781]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAIL
ED: 2
Apr 22 01:17:50 Tallinn tunneld[779]: TID 182912294944: [tunneld.ERR]:
cipsec_recovery_statemachine:
Took IPSec recovery action - tunnel:Tallinn_to_Helsinki still down..
Apr 22 01:18:15 Tallinn sysd[781]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAIL
ED: 2
```

```
Apr 22 01:18:40 Tallinn tunneld[779]: TID 182912294944: [tunneld.ERR]:
cipsec_recovery_statemachine:
Took IPSec recovery action - tunnel:Tallinn_to_Helsinki still down..
Apr 22 01:19:15 Tallinn sysd[781]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAIL
ED: 2
Apr 22 01:19:30 Tallinn tunneld[779]: TID 182912294944: [tunneld.ERR]:
cipsec_recovery_statemachine:
Took IPSec recovery action - tunnel:Tallinn_to_Helsinki still down..
Apr 22 01:20:15 Tallinn sysd[781]: TID 1084225888: [sysd.ERR]: WDOG: Gateway
datapath ping test FAIL
lines 1-12
```

- To view the log facilities configuration:

```
Tallinn3 (config) # show logging facilities
Log Facilities Configuration:
    audit:     local0
    system:    local1
    flow:      local2
Tallinn3 (config) #
```

show memory

Description

Use the **show memory** command to display system memory usage.

Syntax

show memory

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show memory
         Total      Used      Free
Physical  4061 MB   3481 MB    579 MB
Swap         0 MB      0 MB      0 MB
Tallinn (config) #
```

show nat statistics

Description

Use the **show nat statistics** command to display NAT-related statistics.

Syntax

show nat statistics

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show nat-map” on page 314
- “nat-map” on page 139

Usage Guidelines

None.

Examples

```
Tallinn (config) # show nat statistics
NAT Statistics

        Total NAT Tcp flow    :0
        Total NAT Udp flow    :0
        Total NAT Icmp flow   :0
        NAT mid flow no alloc :0

Tallinn (config) #
```

show nat-map

Description

Use the **show nat-map** command to display a list of all the existing NAT maps. The CLI also indicates which NAT map is currently active.

Syntax

show nat-map

show nat-map <*NAT map name*>

show nat-map <*NAT map name*> <*priority*>

show nat-map <*NAT map name*> [<*priority*>] **stats**

Arguments

nat-map	Displays all existing NAT maps.
nat-map <*NAT map name*>	Displays each priority (entry) for the specified NAT map, along with their MATCH criteria and SET actions.
nat-map <*NAT map name*> <*priority*>	Displays the priority specified for the designated NAT map.
stats	Displays statistics for the specified map. If the priority number is included in the command, then the match statistics are limited to that map entry.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show nat statistics” on page 313
- “nat-map” on page 139
- “nat-map match” on page 142
- “nat-map set” on page 144

Usage Guidelines

The default entry in any map is always priority 65535. The NAT map specifics are:

```
65535 match
          Protocol:            ip
          IP version:          any
          Source:              any
          Destination:         any
          Application:         any
          DSCP:                any
          VLAN:                any.any
        set
          NAT Type:            no-nat
          NAT direction:       none
          NAT IP:              auto
          Fallback:            disabled
```

Examples

None.

show ntp

Description

Use the **show ntp** command to display NTP settings.

Syntax

show ntp

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show ntp
NTP enabled: no
No NTP peers configured.
No NTP servers configured.
Tallinn (config) #
```

show opt-map

Description

Use the **show opt-map** command to display a list of all the existing optimization maps. The CLI also indicates which optimization map is currently active.

Syntax

show opt-map

show opt-map <*optimization map name*>

show opt-map <*optimization map name*> <*priority*>

show opt-map <*optimization map name*> <*priority*> **advanced-tcp**

show opt-map <*optimization map name*> <*priority*> **flows**

show opt-map <*optimization map name*> [<*priority*>] **stats**

Arguments

opt-map	Displays all existing optimization maps.
opt-map <*optimization map name*>	Displays each priority (entry) for the specified optimization map, along with their MATCH criteria and SET actions.
opt-map <*optimization map name*> <*priority*>	Displays the priority specified for the designated optimization map.
advanced-tcp	Displays advanced TCP options.
flows	Displays the flows that match the priority (entry) number specified.
stats	Displays statistics for the specified map. If the priority number is included in the command, then the match statistics are limited to that map entry.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “opt-map” on page 154
- “opt-map match” on page 156

- “opt-map set” on page 161

Usage Guidelines

The default entries in any new opt map are as follows:

```
Tallinn3 (config) # show opt-map map1
Opt map map1 configuration (ACTIVE)
  10000 match
          Protocol:            tcp
          Source:              any
          Destination:         any
          Source Port:         any
          Destination Port:    139
          DSCP:                any
          VLAN:                any.any
        set
          Network Memory:      balanced
          Payload Comp:        enable
          Proxy Type:          cifs

  10010 match
          Protocol:            tcp
          Source:              any
          Destination:         any
          Source Port:         any
          Destination Port:    445
          DSCP:                any
          VLAN:                any.any
        set
          Network Memory:      balanced
          Payload Comp:        enable
          Proxy Type:          cifs

  10020 match
          Protocol:            tcp
          Source:              any
          Destination:         any
          Source Port:         any
          Destination Port:    443
          DSCP:                any
          VLAN:                any.any
        set
          Network Memory:      balanced
          Payload Comp:        enable
          Proxy Type:          ssl

  65535 match
          Protocol:            ip
          Source:              any
          Destination:         any
          Application:         any
          DSCP:                any
          VLAN:                any.any
        set
          Network Memory:      balanced
          Payload Comp:        enable
          Proxy Type:          tcp-only

Tallinn3 (config) #
```

You can view an appliance's list of optimization maps—and determine which map is active—with the command, **show opt-map**:

```
Silver Peak> # show opt-map
maryann
ginger             [ACTIVE]
```

Examples

- To view a list of all the priorities included in the optimization map, "map1", for this appliance:

```
Tallinn (config) # show opt-map map1 ?
<cr>                    Display this optimization map
<1..65535>
10
20
75
85
90
100
110
120
130
65535
Tallinn (config) #
```

- To find out how many flows match priority "100" in the optimization map, "ginger" :

```
Silver-Peak (config) # show opt-map ginger 100 flows
Flows matching Optimization Map ginger prio:100:
6 (L->W) sip:10.2.1.128 dip:10.16.1.200 ports:0/0

Total flows:1
```

- To view the specifics of priority 10 in “map1” of the appliance, Tallinn:

```
Tallinn (config) # show opt-map map1 10
  10    match
Protocol:            ip
          Source:              10.10.10.0/24
          Destination:         10.10.20.0/24
          Application:         any
          DSCP:                any
          VLAN:                any.any
        set
          Network Memory:      balanced
          Payload Comp:        enable
          Proxy Type:          tcp-only


Tallinn (config) #
```

- To display the statistics for the optimization map, “O-2-3500-2”, in the appliance,”eh-3500-1” :

```
eh-3500-1 (config) # show opt-map O-2-3500-2 stats
Optimization Map O-2-3500-2 Lookup Statistics:

Priority 100:
 Match Succeeded:       38918
  Permits:      38918   Denies: 0
 Match Failed:  0
  Source IP Address:    0       Destination IP Address: 0
  Source Port:          0       Destination Port:       0
  Application:          0       DSCP Markings:  0       Protocol:       0

Priority 65535:
 Match Succeeded:       0
  Permits:      0       Denies: 0
 Match Failed:  0
  Source IP Address:    0       Destination IP Address: 0
  Source Port:          0       Destination Port:       0
  Application:          0       DSCP Markings:  0       Protocol:       0
eh-3500-1 (config) #
```

show overlay

Description

Use the **show overlay** command to display detailed information any or all overlays.

Syntax

show overlay

show overlay <*overlay name*>

Arguments

<*overlay name*>	Displays the name of a specific overlay.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To display all existing overlays:

```
laine2-vxa (config) # show overlay

Overlay Name(ID):        Voice(1)
        Brownout Loss:           1.000000
        Brownout latency:        75
        Brownout Jitter:         50
        Bonding policy:          high-availability
        Tunnel Usage Policy Bucket: 1
                Condition:       use-sla
                Links:
                                 MPLS-MPLS(1-1)
                                 Internet-Internet(2-2)
                                 Kate-Kate(6-6)

        Tunnel Usage Policy Bucket: 2
                Condition:       use-active
                Links:
                                 MPLS-MPLS(1-1)
```

```
                                    Internet-Internet(2-2)
                                    Kate-Kate(6-6)
laine2-vxa (config) #
```

show pass-through

Description

Use the **show pass-through** command to display detailed information about pass-through traffic.

Syntax

show pass-through

show pass-through configured

show pass-through stats {**flow** [<*traffic class 1-10*>] | **qos** [<*DSCP value*>] | **traffic-class**}

Arguments

configured	Displays the pass-through traffic configuration.
stats flow	Displays pass-through traffic flow metrics.
stats qos	Displays the pass-through QoS statistics. The default DSCP value is **be** (best effort).
stats qos <*DSCP value*>	Displays pass-through QoS statistics for the specified DSCP value.
stats traffic-class	Displays pass-through traffic class statistics.

Defaults

The default traffic class is 1.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

- This command's functionality is the same as "show interfaces pass-through" on page 291 .

Usage Guidelines

Use the command without arguments to display a detailed state of pass-through traffic.

Examples

- To display the pass-through QoS statistics:

```
Tallinn (config) # show pass-through stats qos
Tunnel pass-through QOS be Statistics:
 RX bytes:              0              TX bytes:              258
 RX packets:            0              TX packets:            2

 RX processed packets:  0
 RX process bytes:      0
```

```
 RX invalid packets:                      0
 RX lost packets:                         0
 RX duplicate packets:                    0

 RX error correcting packets:             0
 TX error correcting packets:             0

 RX error correcting bytes:               0
 TX error correcting bytes:               0

 RX packets lost before error correction: 0
 RX packets lost after error correction:  0

 RX reconstructed packets in order:       0
 RX reconstructed packets out of order:   0

 RX out of order packets accepted:        0
 RX out of order packets dropped:         0
 RX out of order packets reordered:       0

 RX packets with 1 packet:                0
 Tx packets with 1 packet:                0

 RX packets with 1 fragment:              0
 TX packets with 1 fragment:              0

 RX packets with > 1 packet no fragment:  0
 TX packets with > 1 packet no fragment:  0

 RX packets with > 1 packet and fragment: 0
 TX packets with > 1 packet and fragment: 0
Tallinn (config) #
```

show preposition

Description

Use the **show preposition** command to display pre-positioning interface status.

Syntax

show preposition

show preposition ftp

Arguments

ftp	Displays the pre-positioning FTP interface status.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show preposition
   FTP server enabled:          no
   FTP server status:           unmanaged
   FTP server anonymous access: no
   FTP server max clients:      5
Tallinn (config) #
```

show qos-map

Description

Use the **show qos-map** command to display a list of all the existing QoS maps. The CLI also indicates which QoS map is currently active.

Syntax

show qos-map

show qos-map <*QoS map name*>

show qos-map <*QoS map name*> <*priority*>

show qos-map <*QoS map name*> <*priority*> **flows**

show qos-map <*QoS map name*> [<*priority*>] **stats**

Arguments

qos-map	Displays all existing QoS maps.
qos-map <*QoS map name*>	Displays each priority (entry) for the specified QoS map, along with their MATCH criteria and SET actions.
qos-map <*QoS map name*> <*priority*>	Displays the priority specified for the designated QoS map.
flows	Displays the flows that match the priority (entry) number specified.
stats	Displays statistics for the specified map. If the priority number is included in the command, then the match statistics are limited to that map entry.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “qos-map” on page 169
- “qos-map match” on page 171
- “qos-map set” on page 176

Usage Guidelines

The default entry in any map is always priority 65535. The QoS map specifics are:

```
65535 match
          Protocol:            ip
          Source:              any
          Destination:         any
          Application:         any
          DSCP:                any
        set
          Traffic Class:       1
          LAN QoS:             trust-lan
          WAN QoS:             trust-lan
```

The following example shows the a sample list of QoS maps:

```
Silver Peak> # show qos-map
maryann
ginger        [ACTIVE]
```

Examples

- To show all the priorities in the QoS map, “map1”:

```
Tallinn (config) # show qos-map  map1
QoS map map1 configuration (ACTIVE)
  10    match
          Protocol:            ip
          Source:              any
          Destination:         any
          Application:         web
          DSCP:                any
        set
          Traffic Class:       1
          LAN QoS:             be
          WAN QoS:             be

  20    match
          Protocol:            ip
          Source:              172.20.20.0/24
          Destination:         any
          Application:         any
          DSCP:                any
        set
          Traffic Class:       3
          LAN QoS:             af12
          WAN QoS:             trust-lan

  40    match
          Protocol:            ip
          Source:              any
          Destination:         any
          Application:         aol
          DSCP:                any
        set
          Traffic Class:       3
          LAN QoS:             trust-lan
```

```
          WAN QoS:             trust-lan

  60    match
          Protocol:            ip
          Source:              any
          Destination:         any
          Application:         any
          DSCP:                be
        set

  65535 match
          Protocol:            ip
          Source:              any
          Destination:         any
          Application:         any
          DSCP:                any
        set
          Traffic Class:       1
          LAN QoS:             trust-lan
          WAN QoS:             trust-lan

Tallinn (config) #
```

- To disply information similar about flows that match the conditions specified by priority 100 in the map, “ginger”:

```
Silver-Peak (config) # show qos-map ginger 100 flows
Flows matching QoS Map ginger prio:100:
6 (L->W) sip:10.2.1.128 dip:10.16.1.200 ports:0/0

Total flows:1
```

show radius

Description

Use the **show radius** command to display RADIUS settings for user authentication.

Syntax

show radius

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

To show any RADIUS settings for the appliance, Tallinn:

```
Tallinn (config) # show radius
RADIUS defaults:
    key:
    timeout: 3
    retransmit: 1
No RADIUS servers configured.
Tallinn (config) #
```

show route-map

Description

Use the **show route-map** command to display a list of all the existing route maps. The CLI also indicates which route map is currently active.

Syntax

show route-map

show route-map <*route map name*>

show route-map <*route map name*> <*priority*>

show route-map <*route map name*> <*priority*> **flows**

show route-map <*route map name*> [<*priority*>] **stats**

Arguments

route-map	Displays all existing route maps.
route-map <*route map name*>	Displays each priority (entry) for the specified route map, along with their MATCH criteria and SET actions.
route-map <*route map name*> <*priority*>	Displays the priority specified for the designated route map.
flows	Displays the flows that match the priority (entry) number specified.
stats	Displays statistics for the specified map. If the priority number is included in the command, then the match statistics are limited to that map entry.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “route-map” on page 182
- “route-map match” on page 184
- “route-map set” on page 189

Usage Guidelines

The default entry in any map is always priority 65535. The route map specifics are:

Tallinn (config) # show route-map map1 65535

```
  65535 match
          Protocol:             ip
          Source:               any
          Destination:          any
          Application:          any
          DSCP:                 any
        set
          Pass-through:         Shaped
```

The following example shows the a sample list of route maps:

```
Silver Peak> # show route-map
maryann
ginger        [ACTIVE]
```

Examples

- To show all the priorities in the route map, “map1”:

```
Tallinn (config) # show route-map map1
Route map map1 configuration (ACTIVE)
  10    match
          Protocol:             ip
          Source:               any
          Destination:          any
          Application:          citrix
          DSCP:                 any
        set
          Primary Tunnel:       HQ-to-BranchA
          Down Action:          pass-through

  20    match
          Protocol:             etherip
          Source:               10.10.10.0/24
          Destination:          10.10.20.0/24
          DSCP:                 any
        set
          Primary Tunnel:       HQ-to-BranchA
          Down Action:          pass-through

  65535 match
          Protocol:             ip
          Source:               any
          Destination:          any
          Application:          any
          DSCP:                 any
        set
          Pass-through:         Shaped

Tallinn (config) #
```

- To show the statistics for priority 20 in the route map, R-2-3500-2:

```
eh-3500-1 (config) # show route-map R-2-3500-2 20 stats
Route Map R-2-3500-2 Lookup Statistics:

Priority 20:
 Match Succeeded:       3212721
  Permits:      3212721 Denies: 0
 Match Failed:  483
  Source IP Address:    479     Destination IP Address: 4
  Source Port:          0       Destination Port:       0
  Application:          0       DSCP Markings:  0       Protocol:       0
eh-3500-1 (config) #
```

- To list all the current flows that match priority 20 for the route map, R-2-3500-2:

```
eh-3500-1 (config) # show route-map R-2-3500-2 10 flows
Flows matching Route Map R-2-3500-2 prio:10:

Total flows:0
eh-3500-1 (config) # show route-map R-2-3500-2 20 flows
Flows matching Route Map R-2-3500-2 prio:20:
1155 (L->W) sip:3.3.3.132 dip:3.3.5.132 ports:54317/7079
954 (L->W) sip:3.3.3.60 dip:3.3.5.60 ports:46082/7078
5169 (L->W) sip:3.3.3.79 dip:3.3.5.79 ports:17516/37693
647 (L->W) sip:3.3.3.74 dip:3.3.5.74 ports:30370/62999
4200 (L->W) sip:3.3.3.19 dip:3.3.5.19 ports:48779/1720
4193 (L->W) sip:3.3.3.115 dip:3.3.5.115 ports:50455/63239
3395 (L->W) sip:3.3.3.103 dip:3.3.5.103 ports:48726/1720
640 (L->W) sip:3.3.3.101 dip:3.3.5.101 ports:53199/58066
1368 (L->W) sip:3.3.3.16 dip:3.3.5.16 ports:18124/7079
35468 (L->W) sip:3.3.3.160 dip:3.3.5.160 ports:5060/5060
4475 (L->W) sip:3.3.3.143 dip:3.3.5.143 ports:32129/10581
1219 (L->W) sip:3.3.3.101 dip:3.3.5.101 ports:22793/7078
162 (L->W) sip:3.3.3.77 dip:3.3.5.77 ports:18249/26865
680 (L->W) sip:3.3.3.134 dip:3.3.5.134 ports:31366/38078
4414 (L->W) sip:3.3.3.31 dip:3.3.5.31 ports:8352/28438
120 (L->W) sip:3.3.3.132 dip:3.3.5.132 ports:8972/57105
4325 (L->W) sip:3.3.3.88 dip:3.3.5.88 ports:36950/36893
2354 (L->W) sip:3.3.3.148 dip:3.3.5.148 ports:7078/41540
```

show running-config

Description

Use the **show running-config** command to display the current running configuration.

Syntax

show running-config [**full**]

Arguments

full	Do not exclude commands that set default values.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

show selftest

Description

Use the **show selftest** command to run a self test and diagnostics.

Syntax

show selftest disk

Arguments

disk	Shows disk self test results.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “selftest” on page 395

Usage Guidelines

None

Examples

- To view disk self test results:

```
Tallinn3 (config) # show selftest disk

Disk self test results:
Disk read results:
Duration: 26 seconds
Read I/O operations per second (IOPS): 391
Read rate (MBytes/second): 97
Read IOPS compared to optimal: 391%
Read rate compared to optimal: 391%

Disk write results:
Duration: 60 seconds
Write I/O operations per second (IOPS): 169
Write rate (MBytes/second): 42
Write IOPS compared to optimal: 169%
Write rate compared to optimal: 169%

Overall result: PASS
```

```
A reboot is required after disk selftest. Do you want to restart the
appliance? (y/n)
```

show shaper

Description

Use the **show shaper** command to display the shaper statistics.

Syntax

show shaper

show shaper [configured | stats]

Arguments

configured	Displays shaper configuration.
stats	Displays shaper debug stats.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “shaper inbound” on page 197
- “shaper outbound” on page 199

Usage Guidelines

None.

Examples

- To view the shaper configuration :

```
Tallinn (config) # show shaper configured
wan shaper
  Max rate       : 500000 kbps
  Accuracy       : 5000 us
  class                    prio   min%   max% excess   wait
   1 default                  5     30    100    100    500
   2 real-time                1     30    100   1000    100
   3 interactive              2     20    100   1000    200
   4 best-effort              8     20    100    100    500
   5 blah                     5     30    100    100    500
   6                          5     30    100    100    500
   7                          5     30    100    100    500
```

```
    8                          5     30    100    100    500
    9                          5     30    100    100    500
   10                          5     30    100    100    500
Tallinn (config) #
```

show snmp

Description

Use the **show snmp** command to display SNMP settings.

Syntax

show snmp [**engine ID** | **user**]

Arguments

engine ID	Displays the SNMP engine ID of the local system.
user	Displays the SNMP v3 user security settings.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To display the SNMP settings:

```
Tallinn (config) # show snmp
SNMP enabled: yes
System location: third rock from the sun
System contact: ET Fone-Hoam
Read-only community: public
Traps enabled: yes
Events for which traps will be sent:
  raise-alarm: System Alarm has been raised
Trap sinks:
   172.20.2.191
      Enabled: yes
      Type: traps version 1
      Community: textstring
Interface listen enabled: yes
No Listen Interfaces.
Tallinn (config) #
```

- To display the local system's SNMP engine ID:

```
Tallinn2 (config) # show snmp engineID
Local SNMP engineID: 0x80005d3b043930623464363761323365 34
Tallinn2 (config) #
```

- To display the SNMP v3 user security settings:

```
Tallinn2 (config) # show snmp user
User name: admin
   Enabled:                 no
   Authentication type:     sha
   Authentication password: (NOT SET; user disabled)
   Privacy type:            aes-128
   Privacy password:        (NOT SET; user disabled)
Tallinn2 (config) #
```

show ssh

Description

Use the **show ssh** command to display SSH settings for server and/or client.

Syntax

show ssh client

show ssh server [host-keys]

Arguments

client	Displays Secure Shell (SSH) client settings.
server	Displays Secure Shell (SSH) server settings.
server host-keys	Displays Secure Shell (SSH) server settings with full host keys

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To show the SSH server settings for the appliance, “Tallinn”:

```
Tallinn (config) # show ssh server
SSH server enabled: yes
SSH server listen enabled: yes
   No Listen Interfaces.

RSA v1 host key: 19:7a:68:d4:2b:61:b2:1c:9b:16:aa:d1:bc:ab:36:d1
RSA v2 host key: b7:c4:9c:7e:d2:a7:8e:8f:bd:c7:76:d4:d5:5f:f6:d9
DSA v2 host key: 2d:64:71:ba:98:f6:96:52:53:ad:16:ea:cc:4e:01:d9
Tallinn (config) #
```

show ssl

Description

Use the **show ssl** command to list host certificate data.

Syntax

show ssl

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

- “ssl auth-certificate” on page 206
- “ssl builtin-signing” on page 208
- “ssl cert-substitution” on page 209
- “ssl host-certificate” on page 210
- “ssl signing-certificate” on page 212
- “ssl subs-certificate” on page 214

Usage Guidelines

None.

Examples

```
Tallinn # show ssl
SSL Proxy Settings:
        Certificate Substitution: Disabled
        Built-in CA Signing: Enabled


Tallinn #
```

show stats tunnel

Description

Use the **show stats tunnel** command to display tunnel traffic statistics.

Syntax

show stats tunnel <*tunnel*>

show stats tunnel <*tunnel*> **{latency | qos-error} [pretty]**
show stats tunnel <*tunnel*> **[pretty]**

show stats tunnel default

show stats tunnel default {latency | qos-error} [pretty]
show stats tunnel default [pretty]

show stats tunnel pass-through {latency | qos-error} [pretty]
show stats tunnel pass-through [pretty]

show stats tunnel pass-through-unshaped {latency | qos-error} [pretty]
show stats tunnel pass-through-unshaped [pretty]

show stats tunnel all-traffic {latency | qos-error} [pretty]
show stats tunnel all-traffic [pretty]

show stats tunnel optimized-traffic {latency | qos-error} [pretty]
show stats tunnel optimized-traffic [pretty]

Arguments

<*tunnel*>	Specifies the name of the tunnel.
all-traffic	Displays all optimized, pass-through, and pass-through-unshaped traffic.
latency	Displays tunnel latency statistics.
optimized-traffic	Displays all optimized traffic.
pass-through	Displays pass-through traffic.
pass-through-unshaped	Displays pass-through unshaped traffic.
pretty	Displays in thousands, separated and right-aligned.
qos-error	Displays tunnel QoS error statistics on all traffic classes

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To view optimized traffic, formatted for easier reading:

```
SP42-NX8600 # show stats tunnel optimized-traffic pretty
                bytes_wtx:   714,823,758
                bytes_wrx:   729,500,245
                bytes_ltx: 5,739,117,443
                bytes_lrx: 3,231,002,684
                 pkts_wtx:       816,634
                 pkts_wrx:       977,866
                 pkts_ltx:     4,529,350
                 pkts_lrx:     2,731,216
                 comp_l2w:             0
                 comp_w2l:             0
          comp_noohead_l2w:             0
          comp_noohead_w2l:             0
                 latency_s:             0
             latency_min_s:             0
              flow_ext_tcp:             1
           flow_ext_tcpacc:             0
              flow_ext_non:             0
                  flow_add:             0
                  flow_rem:             0
      loss_prefec_wrx_pkts:         1,308
     loss_postfec_wrx_pkts:             0
       loss_prefec_wrx_pct:             0
      loss_postfec_wrx_pct:             0
       ooo_prepoc_wrx_pkts:             0
      ooo_postpoc_wrx_pkts:            26
        ooo_prepoc_wrx_pct:             0
       ooo_postpoc_wrx_pct:             0
            ohead_wrx_pkts:     3,142,683
            ohead_wtx_pkts:     3,126,115
           ohead_wrx_bytes:   463,542,375
           ohead_wtx_bytes:   474,786,262
       ohead_wrx_hdr_bytes:   113,928,904
       ohead_wtx_hdr_bytes:   184,900,104
                bw_util_pct:             0
SP42-NX8600 #
```

show subif

Description

Use the **show subif** command to display sub-interface information.

Syntax

show subif

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

show subnet

Description

Use the **show subnet** command to display subnet-related information.

Syntax

show subnet
show subnet [ipv4 | ipv6]

show subnet configured [ipv4 | ipv6]

show subnet debug {module | peer}

show subnet learned [ipv4 | ipv6]

Arguments

configured {ipv4|ipv6}	Displays configured ipv4 (or ipv6) rules
debug module	Displays subnet module state, as a debugging aid.
debug peer	Displays subnet peer state, as a debugging aid.
subnet {ipv4|ipv6}	Displays subnet ipv4 (or ipv6) subnet rules.
learned [ipv4|ipv6]	Displays learned (ipv4 or ipv6) rules.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “subnet” on page 216
- “subnet ipv6” on page 218

Usage Guidelines

None.

Examples

- To display configured ipv4 rules:

```
Tallinn # show subnet configured ipv4
IPv4 Route Table: 1/4000 entries
                        prefix/len :     metric    peer id   details
                     10.1.1.0/24  :        10   11687286   configured advertized
local
```

show system

Description

Use the **show system** command to display system configuration information.

Syntax

show system

show system arp-table-size

show system bypass

show system disk [**brief** | **smart-data**]

show system network-memory media

show system [**nexthops** | **wan-next-hops**]

show system registration

show system smb-signing

show system ssl-ipsec-override

Arguments

arp-table-size	Displays configured system ARP (Address Resolution Protocol) table size.
bypass	Displays system bypass information.
disk	Displays system disk information.
disk brief	Displays brief system disk information.
disk smart-data	Displays system disk SMART (Self-Monitoring Analysis and Reporting Technology) data. These are statistics that a disk collects about itself.
network-memory media	Displays the media used for the system's network memory.
nexthops	Displays all system next-hops, along with their reachability and uptime.
registration	Displays system registration information.
smb-signing	Displays SMB signing option.
ssl-ipsec-override	Displays any SSL IPSec override.
wan-next-hops	Displays system configuration WAN next-hops, along with their configured state and current status.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To display the configured system ARP table size:

```
Tallinn (config) # show system arp-table-size
System Arp Table Size

    Configured maximum arp table size       :    10240
    System's current maximum arp table size :    10240
Tallinn (config) #
```

- To display the system disk information:

```
Tallinn (config) # show system disk
RAID 0 Info:
Status:           OK
Type:             Software
Size:             216
Percent Complete: 100
Drives:           1,0
Configuration:    RAID_1
Disk ID 0
  Status:         OK
  Size:           232 GB
  Serial Number:  WD-WCAL73249872

Disk ID 1
  Status:         OK
  Size:           232 GB
  Serial Number:  WD-WCAL73275682

Tallinn (config) #
```

- To display the brief system disk information:

```
Tallinn (config) # show system disk brief
RAID 0 Info:
Status:           OK
Type:             Software
Size:             216
Percent Complete: 100
Drives:           1,0
Configuration:    RAID_1
ID      Status  Size(GB)        Serial
0       OK      232             WD-WCAL73249872
```

```
1       OK      232             WD-WCAL73275682

Tallinn (config) ##
```

- To display the type of media being used for Network Memory:

```
SP42-NX8600 # show system network-memory media
Network Memory Media: ram and disk
SP42-NX8600 #
```

show tacacs

Description

Use the **show tacacs** command to display TACACS+ settings.

Syntax

show tacacs

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show tacacs
TACACS+ defaults:
    key:
    timeout: 3
    retransmit: 1
No TACACS+ servers configured.
Tallinn (config) #
```

show tca

Description

Use the **show tca** command to display threshold crossing alert settings.

Syntax

show tca

show tca <*tca-name*>

Arguments

tca <*tca-name*>

Specifies which threshold crossing alert to display. The options are:

- **file-system-utilization**
  How much of the file system space has been used, expressed as a percentage.
- **lan-side-rx-throughput**
  LAN–side Receive throughput, in kilobits per second (**kbps**).
- **latency**
  Tunnel latency, in milliseconds (**ms**).
- **loss-post-fec**
  Tunnel loss, as **tenths of a percent**, *after* applying Forward Error Correction (FEC).
- **loss-pre-fec**
  Tunnel loss, as **tenths of a percent**, *before* applying Forward Error Correction (FEC).
- **oop-post-poc**
  Tunnel out-of-order packets, as **tenths of a percent**, *after* applying Packet Order Correction (POC).
- **oop-pre-poc**
  Tunnel out-of-order packets, as **tenths of a percent**, *before* applying Packet Order Correction (POC).
- **optimized flows**
  Total number of optimized flows.
- **reduction**
  Tunnel reduction, in percent (**%**).
- **total-flows**
  Total number of flows.
- **utilization**
  Tunnel utilization, as a percent (**%**).
- **wan-side-tx-throughput**
  WAN–side transmit throughput, in kilobits per second (**kbps**).

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To display a summary of what the defaults are for the various threshold crossing alerts (this information is static because it is **not** the same as reporting the current state of any alert):

```
tallinn3 > show tca
file-system-utilization (File-system utilization):                enabled
lan-side-rx-throughput (LAN-side receive throughput):             disabled
latency (Tunnel latency):                                         enabled
loss-post-fec (Tunnel loss post-FEC):                             disabled
loss-pre-fec (Tunnel loss pre-FEC):                               disabled
oop-post-poc (Tunnel OOP post-POC):                               disabled
oop-pre-poc (Tunnel OOP pre-POC):                                 disabled
optimized-flows (Total number of optimized flows):                disabled
reduction (Tunnel reduction):                                     disabled
total-flows (Total number of flows):                              disabled
utilization (Tunnel utilization):                                 disabled
wan-side-tx-throughput (WAN-side transmit throughput):            disabled
tallinn3 > fil
```

- To display how reduction is currently configured in the threshold crossing alerts:

```
tallinn3 > show tca reduction
reduction - Tunnel reduction:
  default
    enabled:                  no
  A-to-B
    enabled:                  yes
    falling:
      raise-threshold:        20 %
      clear-threshold:        35 %
  pass-through
    enabled:                  no
  pass-through-unshaped
    enabled:                  no
tallinn3 >
```

show tech-support

Description

Use the **show tech-support** command to build a list of troubleshooting information that Silver Peak will request to assist the customer when problems are encountered and technical support has been requested.

Syntax

show tech-support

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show logging” on page 309
- “tech-support create job” on page 414

Usage Guidelines

None.

Examples

None.

show terminal

Description

Use the **show terminal** command to display the current terminal settings.

Syntax

show terminal

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show terminal
CLI current session settings
  Terminal width:          80 columns
  Terminal length:         24 rows
  Terminal type:           vt102
Tallinn (config) #
```

show tunnel

Description

Use the **show tunnel** command to display the detailed running state for all tunnels.

Syntax

show tunnel [**brief** | **configured** | **peers** | **summary**]

show tunnel <*tunnel name*> [**brief** | **configured** | **fastfail** | **ipsec** [**status**] | **summary**]

show tunnel <*tunnel name*> **stats flow** [<*traffic class 1-10*>]

show tunnel <*tunnel name*> **stats ipsec**

show tunnel <*tunnel name*> **stats latency**

show tunnel <*tunnel name*> **stats qos** [<*DSCP value*>]

show tunnel <*tunnel name*> **stats traffic-class**

show tunnel stats cifs

show tunnel stats ssl

Arguments

brief	Displays brief running state for the tunnel(s).
configured	Displays configuration for the tunnel(s).
fastfail	Displays Fastfail information. When multiple tunnels are carrying data between two appliances, this feature determines on what basis to disqualify a tunnel from carrying data, and how quickly.
peers	Displays table summary information for all tunnel peers.
redundancy	Displays redundancy information (regarding WCCP or VRRP) for the tunnel(s).
summary	Displays summary information for the tunnel(s).
tunnel <*tunnel name*>	Displays the detailed running state for this tunnel.
ipsec status	Displays the specified tunnel's IPSec information.
stats cifs	Displays system-wide CIFS statistics.
stats flow	Displays the flow metrics for the default traffic class in the designated tunnel.
stats flow <*traffic class 1-10*>	Displays the flow metrics for the specified traffic class in the designated tunnel.
stats ipsec	Displays the IPSec statistics for the designated tunnel.
stats latency	Displays the latency metrics for the designated tunnel.
stats qos	Displays the default QoS statistics for the designated tunnel. The default DSCP value is **be** (best effort).
stats qos <*DSCP value*>	Displays the QoS statistics for the specified DSCP value in the designated tunnel.
stats ssl	Displays system-wide SSL statistics.
stats traffic-class	Displays the traffic class statistics for the designated tunnel.

Defaults

- The default DSCP value for QoS is **be** (Best Effort).

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See "show interfaces tunnel" on page 294. It is an equivalent command.

Usage Guidelines

- If you don't specify a tunnel, then the output includes information for **all** tunnels.
- If you do specify a tunnel, then the output is limited to that tunnel.

Examples

- To display the IPSec status for the tunnel, “tunnel-2-7501”, in appliance, “eh-3500-1”:

```
eh-3500-1 (config) # show tunnel tunnel-2-7501 ipsec status
Tunnel tunnel-2-7501 ipsec state
  Tunnel Oper:          Down
  IPSec Enabled:        no
  IPSec Oper:           Disabled
  Total IPSec SAs:      in:0 out:0
eh-3500-1 (config) #
```

- To display the statistics for Traffic Class 41 for “t1”, in appliance, “eh-3500-1”:

```
eh-3500-1 (config) # show tunnel t1 stats traffic-class 4
Tunnel t1 Traffic Class 4 Statistics:
 RX bytes:             0          TX bytes:             0
 RX packets:           0          TX packets:           0
                                  TX Invalid packets:   0

 LAN queue dropped packets
   Packet Overload:           0
   Byte Overload:             0
   Packet Overload on Flow:   0
   Byte Overload on Flow:     0
   Queue Time Exceeded:       0
eh-3500-1 (config) #
```

- To display the latency statistics for “tunnel-2-8504”, in appliance, “eh-3500-1”:

```
eh-3500-1 (config) # show tunnel tunnel-2-8504 stats latency
Tunnel tunnel-2-8504 QOS 0 Latency Metrics:
 Minimum Round Trip Time :                0
 Maximum Round Trip Time :                4
 Average Round Trip Time :                0
eh-3500-1 (config) #

   Byte Overload on Flow:     0
   Queue Time Exceeded:       0
eh-3500-1 (config) #
```

show usernames

Description

Use the **show usernames** command to display a list of user accounts.

Syntax

show usernames

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show usernames
Chris      Capability: admin     Password set
admin      Capability: admin     Password set
monitor    Capability: monitor   Password set
Tallinn (config) #
```

show users

Description

Use the **show users** command to display a list of the users that are currently logged in to the appliance.

Syntax

show users

show users history [**username** <*username*>]

Arguments

history	Displays login history for all users.
history username <*username*>	Displays login history for a specific username.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- To display which users are currently logged in:

```
Tallinn2 (config) # show users
Line       User            Host              Login Time            Idle
pts/0      admin           172.20.41.92      2009/01/12 12:37:47   0s
Total users: 1
```

- To display the login history for the user, “admin”:

```
Tallinn2 (config) # show users history username admin
admin    ttyS0                        Thu Dec 11 13:50   still logged in
admin    ttyS0                        Thu Dec 11 12:47 - 13:50  (01:03)
admin    ttyS0                        Thu Dec 11 11:48 - 12:03  (00:15)
admin    ttyS0                        Wed Dec 10 17:13 - 18:14  (01:00)
admin    ttyS0                        Tue Dec  9 21:49 - 22:33  (00:44)
admin    ttyS0                        Tue Dec  9 20:31 - 20:56  (00:24)
wtmp begins Tue Dec  9 20:31:45 2008
```

show version

Description

Use the **show version** command to display version information for current system image.

Syntax

show version [**concise**]

Arguments

concise	Displays concise version information.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

Use the **show version** command without an argument to display verbose version information.

Examples

- To display version information for the current system image:

```
Tallinn (config) # show version
Product name:      NX Series Appliance
Product release:   2.0.0.0_15619
Build ID:          #1-dev
Build date:        2007-06-07 20:00:58
Build arch:        x86_64
Built by:          root@bigchief

Uptime:            24m 40s

Product model:     NX3500
System memory:     3469 MB used / 591 MB free / 4061 MB total
Number of CPUs:    1
CPU load averages: 0.39 / 0.20 / 0.19
Tallinn (config) #
```

- To display concise version information for the appliance, “Tallinn”:

```
Tallinn (config) # show version concise
hidalgo 2.0.0.0_15619 #1-dev 2007-06-07 20:00:58 x86_64 root@bigchief:unknown
Tallinn (config) #
```

show vlan

Description

Use the **show vlan** command to display VLAN information.

Syntax

show vlan

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

- This is in Standard 4-port mode with two IPs:

```
[admin@SP1]# show vlan

Tag           Interface     IP Nexthop          Second Nexthop
----          ---------     -------------       ------------
206           bvi0.206      80.80.80.1/24       80.80.80.2
70            bvi0.70       70.70.70.1/24       70.70.70.2
```

show vrrp

Description

Use the **show vrrp** command to display VRRP information for all instances on all configured interfaces.

Syntax

show vrrp [**brief** | **configured**]

Arguments

brief	Displays brief running state information for all VRRP instances.
configured	Displays configured information for all VRRP instances.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

Use the **show vrrp** command without an argument to display VRRP information for all instances on all interfaces.

Examples

```
buenosaires (config) # show vrrp
VRRP Interface wan0 - Group 4
Virtual IP address:1.2.3.4
Advertisement interval:1 secs
Holddown Timer:200 secs
Admin:up
Preemption Enabled:yes
Priority (configured):128
Authentication String:
Description String:
Packet Trace Enabled:no
IP Address Owner:no
Current Priority:128
Current State:init
State Uptime:0 days 0 hrs 23 mins 19 secs
Master State Transitions:0
Master IP address:0.0.0.0
Virtual Mac Address:00:00:00:00:00:00
```

show wccp

Description

Use the **show wccp** command to display Web Cache Communications Protocol (WCCP) settings.

Syntax

show wccp

show wccp <*51-255*>

show wccp [**configured** | **detail**]

show wccp <*51-255*> [**assignment** | **configured** | **detail**]

Arguments

wccp <*51-255*>	Specifies a WCCP service group ID.
assignment	Displays the details of a WCCP service group.
configured	Displays a configured WCCP service group.
detail	Displays details for a configured WCCP service group.
view	Displays a configured WCCP service group in view.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

Use the **show wccp** command without an argument to display global WCCP information.

Examples

- To show an appliance's global WCCP information:

```
Sicily (config) # show wccp
Global WCCP information

    Appliance information:
        Appliance Identifier:       172.30.2.34
        Protocol Version:
```

```
        Multicast TTL:              5
        Admin State:                Disabled

% There are no configured WCCP service groups.
```

- To display the configuration for the WCCP service group, 51:

```
Tallinn2 (config) # show wccp 51 configured
Service Identifier: 51
    Admin State:                up
    Interface:                  wan0
    Appliance Identifier:
    Router IP address:          10.10.10.7
    Protocol:                   tcp
    Weight:                     100
    Priority:                   128
    Policy Group:               300
    Password:

    Forwarding Method:          either
    Force-L2-Return:            no
    Assignment Method:          either
    Assignment Detail:          lan-ingress
      HASH Assignments
        hash-srcip:             yes
        hash-dstip:             no
        hash-srcport:           no
        hash-dstport:           no
      MASK Assignments
        mask-srcip:             0x00001741
        mask-dstip:             0x00000000
        mask-srcport:           0x0000
        mask-dstport:           0x0000

Tallinn2 (config) #
```

- To show the compatibility mode of WCCP service group 98:

```
paris (config) # show wccp 98 configured
Service Identifier: 98
    Admin State:               up
    Interface:                 wan0
    Appliance Identifier:      6.6.6.1
    Router IP address:         6.6.6.101
    Protocol:                  tcp
    Weight:                    100
    Priority:                  128
    Policy Group:              300
    Password:
    Compatibility Mode:        nexus

    Forwarding Method:         either
    Force-L2-Return:           no
    Assignment Method:         either
    Assignment Detail:         lan-ingress
      HASH Assignments
        hash-srcip:            yes
        hash-dstip:            no
        hash-srcport:          no
        hash-dstport:          no
      MASK Assignments
        mask-srcip:            0x00001741
        mask-dstip:            0x00000000
        mask-srcport:          0x0000
        mask-dstport:          0x000
```

paris (config) #

show web

Description

Use the **show web** command to display Web user interface configuration and status.

Syntax

show web

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn (config) # show web
Web User Interface enabled: yes
   HTTP port:     80
   HTTP enabled:  yes
   HTTPS port:    443
   HTTPS enabled: yes
   Inactivity timeout: 30 minutes
   Max Web user sessions: 10
   Active Web user sessions: 1
Tallinn (config) #
```

show whoami

Description

Use the **show whomai** command to display the identity and capabilities of the current user.

Syntax

show whoami

Arguments

None.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

```
Tallinn2 > show whoami
Current user: admin
Capabilities: admin
Tallinn2 >
```

CHAPTER 5

Alarm Commands

This chapter describes alarm commands. Alarm commands display alarms and event logging information.

alarms

Description

Use the **alarms** command to manage the alarms in the system.

Syntax

alarms {**acknowledge | unacknowledge**} *<alarm sequence number>*

alarms clear *<alarm sequence number>*

Arguments

acknowledge	Acknowledges an alarm in the system.
clear	Clears an alarm in the system.
unacknowledge	Unacknowledges an alarm in the system.
<alarm sequence number>	Specifies the sequence number of the alarm.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See “show alarms” on page 257.

Usage Guidelines

For a list of current alarms, use the following command:

```
(config) # show alarms outstanding
```

```
Tallinn (config) # show alarms outstanding
#   Seq  Date                Type  Sev A Source       Description
--- ---- ------------------- ----- --- - ------------ -----------------
  1    5 2007/06/19 19:23:54   EQU MAJ N system       Datapath Gateway
Connectivity Test Failed
  2    4 2007/06/19 19:21:58   TUN CRI N HQ-to-Branch Tunnel state is Down
  3    2 2007/06/19 19:20:44   EQU MAJ N wan0         Network Interface Link Down
```

The *alarm sequence number* is **not** the same as the *alarm ID* number.

Examples

None.

logging

Description

Use the **logging <IP Address>** command to configure event logging to a specific syslog server.

Use the **no** form of this command to abstain from sendi

event log messages to this server.

Syntax

logging <*IP address*>
no logging <*IP address*>

logging <*IP address*> **facility** {<*facility level*> | **all**}
no logging <*IP address*> **facility** {<*facility level*> | **all**}

logging <*IP address*> **trap** <*severity level*>

Arguments

logging <*IP address*>	Specifies the IP address to which you want to log events.
facility <*facility level*>	Specifically sets the facility for messages to this syslog server to one of the following: Local 0, Local 1, Local 2, Local 3, Local 4, Local 5, Local 6, *or* Local 7
facility all	Specifies all facilities.
trap <*severity level*>	Sets the minimum severity of log messages saved to this syslog server. You can choose from the following severity options: • **none** Disables logging • **emerg** Emergency: system is unusable • **alert** Action must be taken immediately • **crit** Critical conditions • **err** Error conditions • **warning** Warning conditions • **notice** Normal but significant condition • **info** Informational messages • **debug** Debug-level messages

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “logging facility” on page 373
- “logging files” on page 374
- “logging local” on page 376
- “logging trap” on page 378
- “show logging” on page 309

Usage Guidelines

None.

Examples

To configure the server, 10.10.4.4, to not receive any event logs:

```
(config) # no logging 10.10.4.4
```

logging facility

Description

Use the **logging facility** command to configure event logging to a specific syslog server.

Syntax

logging facility auditlog <*facility level*>

logging facility flow <*facility level*>

logging facility system <*facility level*>

Argumentsfacility

<*facility level*>	Specifically sets the facility for messages to this syslog server to one of the following: Local 0, Local 1, Local 2, Local 3, Local 4, Local 5, Local 6, *or* Local 7
auditlog	Specifies the log facility setting for auditlog.
flow	Specifies the log facility setting for flow.
system	Specifies the log facility setting for system,.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “logging facility” on page 373
- “logging files” on page 374
- “logging local” on page 376
- “logging trap” on page 378
- “show logging” on page 309

Usage Guidelines

None.

Examples

None.

logging files

Description

Use the **logging files** command to configure settings for local log files.

Syntax

logging files rotation criteria frequency {daily | weekly | monthly}

logging files rotation criteria size <*size in megabytes*>

logging files rotation criteria size-pct <*percentage*>

logging files rotation force

logging files rotation max-num <*number of files*>

logging files upload <*filename*> <*URL or scp://username:password@hostname/path/filename*>

logging files upload cancel

Arguments

rotation criteria frequency	Rotates log files on a fixed, time-based schedule: • **daily** = once per day at midnight • **weekly** = once per week • **monthly** = on the first day of every month
rotation criteria size <*megabytes*>	Rotates log files when they surpass a size threshold, in megabytes.
rotation criteria size-pct <*percentage*>	Rotates log files when they surpass a specified percentage of /var partition size per log file.
rotation force	Forces an immediate rotation of the log files.
rotation max-num <*number of files*>	Specifies the maximum amount of log files to keep. The value must be between 0 and 4294967295.
upload <*filename*>	Specifies which log file to upload to a remote host.
upload <*URL or scp://username:password@hostname/path/filename*>	Determines the path for a remote host. Optionally, you can specify a new destination filename.
upload cancel	Cancels the current asynchronous file upload.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “logging” on page 371
- “logging local” on page 376
- “logging trap” on page 378
- “show logging” on page 309

Usage Guidelines

None.

Examples

To delete the four oldest local log files:

```
(config) # logging files delete oldest 4
```

To keep the most recent 350 local log files:

```
(config) # logging files rotation max-num 350
```

To upload the log file, “messages” to an account at the remote SCP host, “ocean”, and rename the file to “messages_April2007”:

```
(config) # logging files upload messages
scp://root:seminole@ocean/tmp/messagee_April2007
```

To upload the log file, “messages.2.gz” to the URL, www.catchall.com/tmp/, and keep the original file name:

```
(config) # logging files upload messages.2.gz www.catchall.com/tmp/
```

To rotate the log files when the /var partition surpasses 85% per log file:

```
(config) # logging files rotation criteria size-pct 85
```

logging local

Description

Use the **logging local** command to set minimum severity of log messages saved on the local disk.

Use the **no** form of this command to negate writing event log messages to the local disk.

Syntax

logging local <*severity level*>
no logging local

Arguments

local <*severity level*>	Sets the minimum severity of log messages saved on the local disk. You can choose from the following severity options: • **none** Disables logging • **emerg** Emergency: system is unusable • **alert** Action must be taken immediately • **crit** Critical conditions • **err** Error conditions • **warning** Warning conditions • **notice** Normal but significant condition • **info** Informational messages • **debug** Debug-level messages

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “logging” on page 371
- “logging files” on page 374
- “logging trap” on page 378
- “show logging” on page 309

Usage Guidelines

None.

Examples

To disable local logging of all events related to system resources, use one of the following two commands:

```
(config) # logging local override class system priority none
(config) # no logging local override class system
```

logging trap

Description

Use the **logging trap** to set the minimum severity of log messages sent to **all** syslog servers.

Use the **no** form of this command to negate sending events to all syslog servers.

Syntax

logging trap <*severity level*>

no logging trap

Arguments

trap <*severity level*>	Specifies the minimum severity of log messages sent to all syslog servers. You can choose from the following severity options: • **none** Disables logging • **emerg** Emergency: system is unusable • **alert** Action must be taken immediately • **crit** Critical conditions • **err** Error conditions • **warning** Warning conditions • **notice** Normal but significant condition • **info** Informational messages • **debug** Debug-level messages

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “logging” on page 371
- “logging facility” on page 373
- “logging files” on page 374
- “logging local” on page 376
- “show logging” on page 309

Usage Guidelines

None.

Examples

To set the minimum severity level of log messages sent to all syslog servers to “critical”:

```
(config) # logging trap crit
```

CHAPTER 6

Troubleshooting Commands

This chapter describes the troubleshooting commands. These commands allow you to troubleshoot the Silver Peak NX Series appliances.

debug generate dump

Description

Use the **debug generate dump** command to generate files that are useful for debugging the system. These are also commonly known as “sysdump” files.

Syntax

debug generate dump

Arguments

None.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “show files” on page 279.

Usage Guidelines

None.

Examples

None.

flow-debug

Description

Use the **flow-debug** command to configure the flow debugging feature to isolate a single flow.

Use the **no** form of this command to remove the previous criteria for isolating a specific flow.

Syntax

flow-debug {**disable** | **enable**}

flow-debug flow-id <*flow-id*>
no flow-debug flow-id <*flow-id*>

flow-debug ip1 {<*ip address*> | **any**} **ip2** {<*ip address*> | **any**} **protocol** {<*1..255*> | **any**}
no flow-debug ip1 <*ip address*> **ip2** <*ip address*> **protocol** <*1..255*>

flow-debug ip1 {<*ip address*> | **any**} **ip2** {<*ip address*> | **any**} **protocol** {<*1..255*> | **any**}
port1 {<*port number*> | **any**} **port2** {<*port number*> | **any**}

no flow-debug ip1 <*ip address*> **ip2** <*ip address*> **protocol** <*1..255*> **port1** <*port number*>
port2 <*port number*>

flow-debug reset

Arguments

disable	Disables flow debugging feature.
enable	Enables flow debugging feature.
flow-id <*flow-id*>	Specifies a flow ID for the flow specifier.
ip1 <*ip address*>	Specifies IP1 for the flow specifier.
ip2 <*ip address*>	Specifies IP2 for the flow specifier.
protocol <*1..255*>	Specifies the protocol for the flow specifier.
port1 <*port number*>	Specifies the port number of the first endpoint.
port2 <*port number*>	Specifies the port number of the second endpoint.
any	**any** is a wildcard.
reset	Resets flow debugging data.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See “show flow-debug” on page 281.

Usage Guidelines

The **flow-debug** commands let you narrow down to a single flow and then generate output about that flow. You can isolate a flow by using the flow’s ID number or by entering specifics about the endpoints, protocol, and/or ports. When more than one flow fit the criteria you specify, then the first match is what displays.

Generally, you first specify the flow, then **enable** it, and finally, use the **show flow-debug** command to generate the informational output.

You can enable and disable at will. Once you’ve specified a flow, it remains the target flow until you specify another flow.

Examples

None.

hping2

Description

Use the **hping2** command to send and analyze TCP, UDP, ICMP, and RAW-IP packets to a specified host.

Syntax

hping2 <*hping2 options*> <*destination*>

Arguments

<*hping2 options*>

Specifies the type of **hping2**. Select one of the following options:

- **-h** --help Show this help.
- **-v** --version Show version.
- **-c** --count Packet count.
- **-i** --interval wait (**uX** for X microseconds, for example **-i u1000**). --fast Alias for **-i u10000** (10 packets for second).
- **-n** --numeric Numeric output.
- **-q** --quiet Quiet.
- **-I** --interface Interface name (otherwise default routing interface).
- **-V** --verbose Verbose mode.
- **-D** --debug Debugging info.
- **-z** --bind Bind **CTRL+z** to ttl (default to destination port).
- **-Z** --unbind Unbind **CTRL+z**

MODE

Default mode = TCP

- **-0** --rawip RAW IP mode.
- **-1** --icmp ICMP mode.
- **-2** --udp UDP mode.
- **-8** --scan SCAN mode.
  Example: hping --scan 1-30,70-90 -S www.target.host
- **-9** --listen Listen mode.

IP

• **-a**	--spoof	Spoof source address.
	--rand-dest	Random destionation address mode. see the man.
	--rand-source	Random source address mode. see the man.
• **-t**	--ttl	ttl (default 64).
• **-N**	--id	id (default random).
• **-W**	--winid	Use win* id byte ordering.
• **-r**	--rel	Relativize id field (to estimate host traffic).
• **-f**	--frag	Split packets in more frag. (may pass weak acl).
• **-x**	--morefrag	Set more fragments flag.
• **-y**	--dontfrag	Set don't fragment flag.
• **-g**	--fragoff	Set the fragment offset.
• **-m**	--mtu	Set virtual mtu, implies **--frag** if packet size > mtu.
• **-o**	--tos	Type of service (default 0x00), try --tos help
• **-G**	--rroute	Includes RECORD_ROUTE option and displaysthe route buffer.
	--lsrr	Loose source routing and record route.
	--ssrr	Strict source routing and record route.
• **-H**	--ipproto	Set the IP protocol field, only in RAW IP mode.

ICMP

• **-C**	--icmptype	icmp type (default echo request).
• **-K**	--icmpcode	icmp code (default 0).
	--force-icmp	Send all ICMP types (default send only supported types).
	--icmp-gw	Set gateway address for ICMP redirect (default 0.0.0.0).
	--icmp-ts	Alias for --icmp --icmptype 13 (ICMP timestamp).
	--icmp-addr	Alias for --icmp --icmptype 17 (ICMP address subnet mask).
	--icmp-help	Display help for others icmp options.

UDP/TCP

- **-s** --baseport Base source port (default random).
- **-p** --destport [+][+]<port> destination port(default 0) **CTRL+z**. inc/dec.
- **-k** --keep Keep still source port.
- **-w** --win winsize (default 64).
- **-O** --tcpoff Set fake tcp data offset (instead of tcphdrlen / 4).
- **-Q** --seqnum Shows only TCP sequence number.
- **-b** --badcksum (Try to) send packets with a bad IP checksum many systems will fix the IP checksum sending the packet so you'll get bad UDP/TCP checksum instead.
- **-M** --setseq Set TCP sequence number.
- **-L** --setack Set TCP ack.
- **-F** --fin Set FIN flag.
- **-S** --syn Set SYN flag.
- **-R** --rst Set RST flag.
- **-P** --push Set PUSH flag.
- **-A** --ack Set ACK flag.
- **-U** --urg Set URG flag.
- **-X** --xmas Set X unused flag (0x40).
- **-Y** --ymas Set Y unused flag (0x80).
  --tcpexitcode Use last tcp->th_flags as exit code.
  --tcp-timestamp Enable the TCP timestamp option to guess the HZ/uptime.

Common

- **-d** --data data size (default is 0)
- **-E** --file data from file
- **-e** --sign add 'signature'
- -j --dump dump packets in hex
- **-J** --print dump printable characters
- **-B** --safe enable 'safe' protocol
- **-u** --end tell you when --file reached EOF and prevent rewind
- **-T** --traceroute traceroute mode (implies --bind and --ttl 1)
  --tr-stop Exit when receive the first not ICMP in traceroute mode
  --tr-keep-ttl Keep the source TTL fixed, useful to monitor just one hop
  --tr-no-rtt Don't calculate/show RTT information in traceroute mode

ARS packet description (new, unstable)

- --apd-send Send the packet described with APD (see docs/APD.txt)

<*destination*> Specifies the IP address of the destination that you are pinging.

Defaults

The default mode is **TCP**.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “mtr” on page 389
- “ping” on page 392
- “tcpdump” on page 406
- “tcptraceroute” on page 411
- “traceroute” on page 417.

Usage Guidelines

- **hping2** is a command-line oriented TCP/IP packet assembler/analyzer.
- The interface is inspired by the ping unix command, but hping2 isn’t limited to sending ICMP echo requests. It supports TCP, UDP, ICMP, and RAW-IP protocols, and has a traceroute mode.

Examples

None.

mtr

Description

Use the **mtr** command to probe and report on routers and their response time on an individual route path.

Syntax

mtr [-hvrctglspniu46] [--help] [--version] [--report] [--report-wide] [--report-cycles COUNT] [--curses] [--split] [--raw] [--no-dns] [--gtk] [--address IP.ADD.RE.SS] [--interval SECONDS] [--psize BYTES | -s BYTES] HOSTNAME [PACKETSIZE]

Arguments

<*mtr options*> Specifies the type of **mtr**. Select one of the following options:

- **-h** *help*. Print the summary of command line argument options.
- **-v** *version.* Print the installed version of **mtr**.
- **-r** *report.* This option puts mtr into report mode. When in this mode, **mtr** will run for the number of cycles specified by the **-c** option, and then print statistics and exit. This mode is useful for generating statistics about network quality. Note that each running instance of **mtr** generates a significant amount of network traffic. Using **mtr** to measure the quality of your network may result in decreased network performance.
- **-w** *report-wide*. This option puts **mtr** into wide report mode. When in this mode, **mtr** will not cut hostnames in the report.
- **-c** *report-cycles COUNT.* Use this option to set the number of pings sent to determine both the machines on the network and the reliability of those machines. Each cycle lasts one second.
- **-s** *BYTES*, *-psize BYTES*, *-PACKETSIZE.* These options or a trailing PACKETSIZE on the command line sets the packet size used for probing. It is in bytes inclusive IP and ICMP headers. If set to a negative number, every iteration will use a different, random packetsize up to that number.
- **-t** *curses*. Use this option to force **mtr** to use the curses based terminal interface (if available).
- **-n** *no-dns*. Use this option to force **mtr** to display numberic IP numbers and not try to resolve the host names.
- **-o** *fields order.*Use this option to specify the fields and their order when loading **mtr**. Example: -o “LSD NBAW”
- **-g** *gtk*. Use this option to force **mtr** to use the GTK+ based X11 window interface (if available). GTK+ must have been available on the system when **mtr** was built for this to work. See the GTK+ web page at *http://www.gimp.org/gtk/* for more information about GTK+.
- **-p** *split*. Use this option to set **mtr** to spit out a format that is suitable for a split-user interface.
- **-l** *raw*. Use this option to tell **mtr** to use the raw output format. This format is better suited for archival of the measurement results. It could be parsed to be presented into any of the other display methods.

- **-a** *address IP.ADD.RE.SS*. Use this option to bind outgoing packets' socket to specific interface, so that any packet will be sent through this interface. NOTE that this options doesn't apply to DNS requests (which could be and could not be what you want).
- **- i** *interval SECONDS*. Use this option to specify the positive number of seconds between ICMP ECHO requests. The default value for this parameter is one second.
- **-u**. Use UDP diagrams instead of ICMP ECHO.
- **-4**. Use IPv4 only.
- **-6**. Use IPv6 only.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- "hping2" on page 385
- "ping" on page 392
- "tcpdump" on page 406
- "tcptraceroute" on page 411
- "traceroute" on page 417.

Usage Guidelines

- **mtr** combines the functionality of traceroute and ping in a single network diagnostic tool.
- **mtr** probes routers on the route path by limiting the number of hops that individual packets may traverse, and listening to responses of their expiry.

  It regularly repeats this process, usually once per second, and keep track of the response times of the hops along the path.
- **mtr** combines the functionality of the **traceroute** and **ping** programs in a single network diagnostic tool.
- [*from Linux man page*] As **mtr** starts, it investigates the network connection between the host **mtr** runs on and **HOSTNAME**. by sending packets with purposely low TTLs. It continues to send packets with low TTL, noting the response time of the intervening routers. This allows **mtr** to print the response percentage and response times of the internet route to **HOSTNAME**. A sudden increase in packet loss or response time is often an indication of a bad (or simply overloaded) link.

Examples

```
tallinn3 (config) # mtr
                        My traceroute  [v0.75]
tallinn3 (0.0.0.0)                                  Tue Sep 21 02:03:12 2010
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                    Packets          Pings
 Host                               Loss%  Snt   Last   Avg  Best  Wrst StDev
 1. localhost                        0.0%   66    0.0   0.0   0.0   0.0   0.0
```

ping

Description

Use the **ping** command to send Internet Control Message Protocol (ICMP) echo requests to a specified host.

Syntax

ping <*ping options*> <*destination*>

Arguments

<*ping options*>

Specifies the type of ping. Select one of the following options:

- **-a**: Audible ping.
- **-A**: *Adaptive ping*. Interpacket interval adapts to round-trip time, so that effectively not more than one (or more, if preload is set) unanswered probes present in the network. Minimal interval is 200 msec if not super-user. On networks with low rtt this mode is essentially equivalent to flood mode.
- **-b**: Allow pinging a broadcast address.
- **-B**: Do not allow ping to change source address of probes. The address is bound to the one selected when ping starts.
- **-c** *count*: Stop after sending count ECHO_REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the time- out expires.
- **-d**: Set the SO_DEBUG option on the socket being used. This socket option is unused.
- **-F** *flow label*: Allocate and set 20 bit flow label on echo request packets. If value is zero, kernel allocates random flow label.
- **-f**: *Flood ping*. For every ECHO_REQUEST sent a period "." is printed, while for ever ECHO_REPLY received a backspace is printed. This provides a rapid display of how many packets are being dropped. If interval is not given, it sets interval to zero and outputs packets as fast as they come back or one hundred times per second, whichever is more. Only the super-user may use this option with zero interval.
- **-i** *interval*: Wait interval seconds between sending each packet. The default is to wait for one second between each packet normally, or not to wait in flood mode. Only super-user may set interval to values less 0.2 seconds.
- **-I** *interface address*: Set source address to specified interface address. Argument may be numeric IP address or name of device.
- **-l** *preload*: If preload is specified, ping sends that many packets not waiting for reply. Only the super-user may select preload more than 3.

- **-L**: Suppress loopback of multicast packets. This flag only applies if the ping destination is a multicast address.
- **-n**: Numeric output only. No attempt will be made to lookup symbolic names for host addresses.
- **-p** *pattern*: You may specify up to 16 "pad" bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, -p ff will cause the sent packet to be filled with all ones.
- **-Q** *tos*: Set Quality of Service -related bits in ICMP datagrams. tos can be either decimal or hex number.

  Traditionally (RFC1349), these have been interpreted as: 0 for reserved (currently being redefined as congestion control), 1-4 for Type of Service and 5-7 for Precedence.

  Possible settings for Type of Service are: minimal cost: 0x02, reliability: 0x04, throughput: 0x08, low delay: 0x10.

  Multiple TOS bits should not be set simultaneously.

  Possible settings for special Precedence range from priority (0x20) to net control (0xe0). You must be root (CAP_NET_ADMIN capability) to use Critical or higher precedence value. You cannot set bit 0x01 (reserved) unless ECN has been enabled in the kernel.

  In RFC2474, these fields has been redefined as 8-bit Differentiated Services (DS), consisting of: bits 0-1 of separate data (ECN will be used, here), and bits 2-7 of Differentiated Services Codepoint (DSCP).
- **-q**: *Quiet output*. Nothing is displayed except the summary lines at startup time and when finished.
- **-R**: *Record route*. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.
- **-r**: Bypass the normal routing tables and send directly to a host on an attached interface. If the host is not on a directly attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it provided the option -I is also used.
- **-s** *packetsize*: Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.
- **-S** *sndbuf*: Set socket sndbuf. If not specified, it is selected to buffer not more than one packet.
- **-t ttl**: Set the IP Time to Live.
- **-T** *timestamp option*: Set special IP timestamp options. timestamp option may be either tsonly (only timestamps), tsandaddr (timestamps and addresses) or tsprespec host1 [host2 [host3 [host4]]] (timestamp prespecified hops).

- **-M** *hint*: Select Path MTU Discovery strategy. hint may be either do (prohibit fragmentation, even local one), want (do PMTU discovery, fragment locally when packet size is large), or dont (do not set DF flag).
- **-U**: Print full user-to-user latency (the old behavior). Normally ping prints network round trip time, which can be different f.e. due to DNS failures.
- **-v**: Verbose output.
- **-V**: Show version and exit.
- **-w** *deadline*: Specify a timeout, in seconds, before ping exits regardless of how many packets have been sent or received. In this case ping does not stop after count packet are sent, it waits either for deadline expire or until count probes are answered or for some error notification from network.

<destination> — Specifies the IP address of the destination that you are pinging.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “hping2” on page 385
- “mtr” on page 389
- “tcpdump” on page 406
- “tcptraceroute” on page 411
- “traceroute” on page 417

Usage Guidelines

None.

Examples

None.

selftest

Description

Use the **selftest** command to run a self test and diagnostics.

Syntax

selftest start disk

selftest stop disk

Arguments

start disk	Starts a disk self test operation.
stop disk	Stops a disk self test operation..

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “show selftest” on page 334

Usage Guidelines

When you enter , the following message appears:

```
This is an intrusive self test. This test will put the system in bypass mode
and perform read/write operations on the disks. The system will not process
any network traffic for the duration of the test. At the end of the test, you
need to reboot the system. While the test is running, if you attempt to run
other commands, you will receive errors.


Do you want to proceed? (y/n) [If you don't respond, the question times out.]


Disk self test has been canceled.
```

Examples

None.

slogin

Description

Use the **slogin** command to securely log into another system using Secure Shell (SSH).

Syntax

slogin <*slogin options*> [*user@*] <*hostname*> [*command*]

Arguments

<*slogin options*>

Specify one of the following SSH login options:

- **-a**: Disables forwarding of the authentication agent connection.
- **-A**: Enables forwarding of the authentication agent connection. This can also be specified on a per-host basis in a configuration file. Agent forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the agent's Unix-domain socket) can access the local agent through the forwarded connection. An attacker cannot obtain key material from the agent, however they can perform operations on the keys that enable them to authenticate using the identities loaded into the agent.
- **-b** *bind_address*: Specify the interface to transmit from on machines with multiple interfaces or aliased addresses.
- **-c** *cipher_spec*: Additionally, for protocol version 2 a comma-separated list of ciphers can be specified in order of preference.
- -e ch | ^ch | **none**: Sets the escape character for sessions with a pty (default: ~). The escape character is only recognized at the beginning of a line. The escape character followed by a dot (.) closes the connection, followed by control-Z suspends the connection, and followed by itself sends the escape character once. Setting the character to none fully transparent.
- **-f**: Requests ssh to go to background just before command execution. This is useful if ssh is going to ask for passwords or passphrases, but the user wants it in the background. This implies -n. The recommended way to start X11 programs at a remote site is with something like ssh -f host xterm.
- **-g**: Allows remote hosts to connect to local forwarded ports.
- -i identity_file: Selects a file from which the identity (private key) for RSA or DSA authentication is read. The default is $HOME/.ssh/identity for protocol version 1, and $HOME/.ssh/id_rsa and $HOME/.ssh/id_dsa for protocol version 2. Identity files may also be specified on a per-host basis in the configuration file. It is possible to have multiple -i options (and multiple identities specified in configuration files).
- **-k**: Disables forwarding of Kerberos tickets and AFS tokens. This may also be specified on a per-host basis in the configuration file.
- **-l** *login_name*: Specifies the user to log in as on the remote machine. This also may be specified on a per-host basis in the configuration file.

- **-m** *mac_spec*: Additionally, for protocol version 2 a comma-separated list of MAC (message authentication code) algorithms can be specified in order of preference.
- **-n**: Redirects stdin from **/dev/null** (actually, prevents reading from stdin). This must be used when ssh is run in the background. A common trick is to use this to run X11 programs on a remote machine. For example, ssh -n shadows.cs.hut.fi emacs and will start an emacs on shadows.cs.hut.fi, and the X11 connection will be automatically forwarded over an encrypted channel. The ssh program will be put in the background. (This does not work if ssh needs to ask for a password or passphrase; see also the **-f** option.)
- **-N**: Do not execute a remote command. This is useful for just forwarding ports (protocol version 2 only).
- **-o** *option*: Can be used to give options in the format used in the configuration file. This is useful for specifying options for which there is no separate command-line flag.
- **-p** *port*: Port to connect to on the remote host. This can be specified on a per-host basis in the configuration file.
- **-q**: *Quiet mode*. Causes all warning and diagnostic messages to be suppressed.
- **-s**: May be used to request invocation of a subsystem on the remote system. Subsystems are a feature of the SSH2 protocol which facilitate the use of SSH as a secure transport for other applications (for example, sftp). The subsystem is specified as the remote command.
- **-t**: Force pseudo-tty allocation. This can be used to execute arbitrary screen-based programs on a remote machine, which can be very useful, for example, when implementing menu services. Multiple -t options force tty allocation, even if ssh has no local tty.
- **-T**: Disable pseudo-tty allocation.
- **-v**: *Verbose mode*. Causes ssh to print debugging messages about its progress. This is helpful in debugging connection, authentication, and configuration problems. Multiple **-v** options increases the verbosity. Maximum is 3.
- **-V:** Display the version number and exit.
- **-x**: Disables X11 forwarding.
- **-X**: Enables X11 forwarding. This can also be specified on a per-host basis in a configuration file. X11 forwarding should be enabled with caution. Users with the ability to bypass file permissions on the remote host (for the user's X authorization database) can access the local X11 display through the forwarded connection. An attacker may then be able to perform activities such as keystroke monitoring.
- **-Y**: Enables trusted X11 forwarding. Trusted X11 forwardings are not subjected to the X11 SECURITY extension controls.
- **-C**: Requests compression of all data (including stdin, stdout, stderr, and data for forwarded X11 and TCP/IP connections). The compression algorithm is the same used by gzip(1), and the *level* CompressionLevel option for protocol version 1. Compression is desirable on modem lines and other slow connections, but will only slow down things on fast networks. The default value can be set on a host-by-host basis in the configuration files.

- **-F** *configfile*: Specifies an alternative per-user configuration file. If a configuration file is given on the command line, the system-wide configuration file (/etc/ssh/ssh_config) will be ignored. The default for the per-user configuration file is $HOME/.ssh/config.
- **-L** *port:host:hostport*: Specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side. This works by allocating a socket to listen to port on the local side, and whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to host port hostport from the remote machine. Port forwardings can also be specified in the configuration file. Only root can forward privileged ports. IPv6 addresses can be specified with an alternative syntax: port/host/hostport
- **-R** *port:host:hostport*: Specifies that the given port on the remote (server) host is to be forwarded to the given host and port on the local side. This works by allocating a socket to listen to port on the remote side, and whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to host port hostport from the local machine. Port forwardings can also be specified in the configuration file. Privileged ports can be forwarded only when logging in as root on the remote machine. IPv6 addresses can be specified with an alternative syntax: port/host/hostport
- **-D** *port*: Specifies a local dynamic This works by allocating a socket to listen to port on the local side, and whenever a connection is made to this port, the connection is forwarded over the secure channel, and the application protocol is then used to determine where to connect to from the remote machine. Currently the SOCKS4 protocol is supported, and ssh will act as a SOCKS4 server. Only root can forward privileged ports. Dynamic port forwardings can also be specified in the configuration file.
- **-1**: Forces ssh to try protocol version 1 only.
- **-2**: Forces ssh to try protocol version 2 only.
- **-4**: Forces ssh to use IPv4 addresses only.
- **-6**: Forces ssh to use IPv6 addresses only.

user@	Specifies the name of a user on the remote host.
hostname	Specifies the name or path of the remote host.
command	Specifies a command to execute on the remote system.

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

ssh client global

Description

Use the **ssh client global** command to configure global SSH client settings.

Syntax

ssh client global host-key-check {yes | no | ask}
no ssh client global host-key-check

ssh client global known-host <*known host entry*>
no ssh client global known-host <*known host entry*>

ssh client global known-hosts-file <*filename*>
no ssh client global known-hosts-file

Arguments

host-key-check <*policy*>	Configures global SSH client host key check settings. The policy choices are: • **yes** Strict host key checking: only permit connection if a matching host key is already in the known hosts file • **no** Non-strict host key checking: always permit connection, and accept any new or changed host keys without checking • **ask** Medium-strict host key checking: prompt user to accept new host keys, but do not permit a connection if there was already a known host entry that does not match the one presented by the host Use the **no** form of this command to reset global SSH client host key check settings.
known-host <*known host entry*>	Adds a global SSH client known host entry. This can be a hostname or an IP address. Use the **no** form of this command to remove a global SSH client known host entry by host.
known-hosts-file <*filename*>	Configures gobal SSH client known_hosts file settings. Use the **no** form of this command to rest a global SSH client known_hosts file settings.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssh client user” on page 402
- “ssh server” on page 404
- “show ssh” on page 340

Usage Guidelines

None.

Examples

None.

ssh client user

Description

Use the **ssh client user** command to configure the SSHv2 RSA authorized key for the specified SSH user.

Syntax

ssh client user <*user name*> **authorized-key sshv2** <*public key*>
no ssh client user <*user name*> **authorized-key sshv2** <*public key*>

ssh client user <*user name*> **identity rsa2** {**generate** | **private-key** <*private key*> | **public-key** <*public key*>}
no ssh client user <*user name*> **identity rsa2**

ssh client user <*user name*> **identity dsa2** {**generate** | **private-key** <*private key*> | **public-key** <*public key*>}
no ssh client user <*user name*> **identity dsa2**

no ssh client user <*user name*> **identity**

ssh client user <*user name*> **known-host** <*known host*> **remove**

Arguments

user <*user name*>	Specifies the name of an existing user of the appliance.
authorized-key sshv2 <*public key*>	Configures SSHv2 an authorized-key for the specified SSH user. Use the **no** form of this command to negate the authorized-key settings for the specified user.
identity	Sets certain SSH client identity settings for a user. Use the **no** form of this command to negate the authorized-key settings for the specified user.
rsa2	Specifies the RSAv2 algorithm for public-key encryption.
dsa2	Specifies the Digital Signature Algorithm, version 2 (DSAv2).
generate	Generates SSH client identity keys for specified user.
known-host <*known host*> **remove**	Removes the host from the user's known host file.
private-key <*private key*>	Sets the private key SSH client identity settings for the user.
public-key <*public key*>	Sets the public key SSH client identity settings for the user.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssh client global” on page 400
- “ssh server” on page 404
- “show ssh” on page 340

Usage Guidelines

To negate the SSHv2 authorized-key settings for a specified user named “Chris”, where the public key ID is “columbus”:

```
(config) # no ssh client user Chris authorized-key sshv2 columbus
```

To delete all SSH client identity keys for a specified user named “Chris”:

```
(config) # no ssh client user Chris identity
```

To delete the RSAv2 identity for the user named “Chris”:

```
(config) # no ssh client user Chris identity rsa2
```

Examples

None.

ssh server

Description

Use the **ssh server** command to configure the Secure Shell (SSH) server.

Syntax

ssh server enable
no ssh server enable

ssh server host-key <*key type*> {**private-key** <*private key*> | **public-key** <*public key*>}

ssh server host-key generate

ssh server listen enable
no ssh server listen enable

ssh server listen interface <*interface*>
no ssh server listen interface <*interface*>

ssh server min-version <*version number*>
no ssh server min-version

ssh server ports <*port*> [<*port*>] [<*port*>] ...

Arguments

enable	Enables Secure Shell (SSH) access to this system. Use the **no** form of this command to diable SSH access to this system.
host-key	Manipulates the host keys for SSH.
<*key type*>	Specifies the type of host keys to create. The choices are: • **rsa1** RSAv1 • **rsa2** RSAv2 • **dsa2** DSAv2
private-key <*private key*>	Sets a new private-key for the host keys of the type you specify.
public-key <*public key*>	Sets a new public-key for the host keys of the type you specify.
generate	Generates new RSA and DSA host keys for SSH.
listen enable	Enables SSH interface restriction access to this system. Use the **no** form of this command to disable SSH interface restriction access to this system.
listen interface <*interface*>	Adds an interface to the SSH server access restriction list. Use the **no** form of this command to remove the specified interface from the SSH server access restriction list.
min-version <*version number*>	Sets the minimum version of SSH protocol supported. Use the **no** form of this command to reset the minimum version of SSH protocol supported.
ports <*port*> [<*port*>] [<*port*>] ...	Specifies the ports that the SSL server will listen on. When you hit the carriage return, it sets this list as the entire set of SSH server ports, removing all others.

Defaults

None.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “ssh client user” on page 402
- “show ssh” on page 340

Usage Guidelines

If you use the optional **listen** argument, then the **ssh server listen enable** command enables SSH interface restriction access to this system.

Examples

To remove lan0 from the SSH server access restriction list:

```
(config) # no ssh server listen interface lan0
```

tcpdump

Description

Use the **tcpdump** command to display packets on a network.

Syntax

tcpdump [<*tcpdump options*>]

Arguments

<*tcpdump options*>	Enter one of the following options: • **-A**: Print each packet (minus its link level header) in ASCII. Handy for capturing web pages. • **-c**: Exit after receiving count packets. • **-C**: Before writing a raw packet to a savefile, check whether the file is currently larger than file_size and, if so, close the current savefile and open a new one. Savefiles after the first savefile will have the name specified with the -w flag, with a number after it, starting at 1 and continuing upward. The units of file_size are millions of bytes (1,000,000 bytes, not 1,048,576 bytes). • **-d**: Dump the compiled packet-matching code in a human readable form to standard output and stop. • **-dd**: Dump packet-matching code as a C program fragment. • **-ddd**: Dump packet-matching code as decimal numbers (preceded with a count). • **-D**: Print the list of the network interfaces available on the system and on which tcpdump can capture packets. For each network interface, a number and an interface name, possibly followed by a text description of the interface, is printed. The interface name or the number can be supplied to the -i flag to specify an interface on which to capture. • **-e**: Print the link-level header on each dump line.

- **-E**: Use spi@ipaddr algo:secret for decrypting IPsec ESP packets that are addressed to addr and contain Security Parameter Index value spi. This combination may be repeated with comma or newline separation.

  Note that setting the secret for IPv4 ESP packets is supported at this time.

  Algorithms may be des-cbc, 3des-cbc, blowfish-cbc, rc3-cbc, cast128-cbc, or none. The default is des-cbc. The ability to decrypt packets is only present if tcpdump was compiled with cryptography enabled.

  `secret` is the ASCII text for ESP secret key. If preceded by 0x, then a hex value will be read.

  The option assumes RFC2406 ESP, not RFC1827 ESP. The option is only for debugging purposes, and the use of this option with a true 'secret' key is discouraged. By presenting IPsec secret key onto command line you make it visible to others, via ps(1) and other occasions.

  In addition to the above syntax, the syntax file name may be used to have tcpdump read the provided file in. The file is opened upon receiving the first ESP packet, so any special permissions that tcpdump may have been given should already have been given up.
- **-f**: Print 'foreign' IPv4 addresses numerically rather than symbolically.
- **-F**: Use file as input for the filter expression. An additional expression given on the command line is ignored.
- **-i**: Listen on interface. If unspecified, tcpdump searches the system interface list for the lowest numbered, configured up interface (excluding loopback). Ties are broken by choosing the earliest match.
- **-l**: Make stdout line buffered. Useful if you want to see the data while capturing it. For example,
  `tcpdump -l | tee dat` or `tcpdump -l > dat & tail -f dat`

- **-L**: List the known data link types for the interface and exit.
- **-m**: Load SMI MIB module definitions from file module. This option can be used several times to load several MIB modules into tcp-dump.
- **-M**: Use secret as a shared secret for validating the digests found in TCP segments with the TCP-MD5 option (RFC 2385), if present.
- **-n**: Don't convert host addresses to names. This can be used to avoid DNS lookups.
- **-nn**: Don't convert protocol and port numbers etc. to names either.
- **-N**: Don't print domain name qualification of host names. For example, if you give this flag then tcpdump will print `nic` instead of `nic.ddn.mil`.
- **-O**: Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer.
- **-p**: Don't put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, **-p** cannot be used as an abbreviation for 'ether host {local-hw-addr} or ether broadcast'.
- **-q**: Quick (quiet?) output. Print less protocol information so output lines are shorter.
- **-R**: Assume ESP/AH packets to be based on old specification (RFC1825 to RFC1829). If specified, tcpdump will not print replay prevention field. Since there is no protocol version field in ESP/AH specification, tcpdump cannot deduce the version of ESP/AH protocol.
- **-r**: Read packets from file (which was created with the -w option). Standard input is used if file is ''-''.
- **-S**: Print absolute, rather than relative, TCP sequence numbers.
- **-s**: Snarf snaplen bytes of data from each packet rather than the default of 68 (with SunOS's NIT, the minimum is actually 96). 68 bytes is adequate for IP, ICMP, TCP and UDP but may truncate protocol information from name server and NFS packets.Packets truncated because of a limited snapshot are indicated in the output with **[|proto]**, where **proto** is the name of the protocol level at which the truncation has occurred.

  Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. You should limit snaplen to the smallest number that will capture the protocol information you're interested in. Setting snaplen to 0 means use the required length to catch whole packets.

- **-T**: Force packets selected by "expression" to be interpreted the specified type. Currently known types are:

  aodv (Ad-hoc On-demand Distance Vector protocol),
  cnfp (Cisco NetFlow protocol),
  rpc (Remote Procedure Call),
  rtp (Real-Time Applications protocol),
  rtcp (Real-Time Applications control protocol),
  snmp (Simple Network Management Protocol),
  tftp (Trivial File Transfer Protocol),
  vat (Visual Audio Tool), and
  wb (distributed White Board).
- **-t**: Don't print a timestamp on each dump line.
- **-tt**: Print an unformatted timestamp on each dump line.
- **-ttt**: Print a delta (in micro-seconds) between current and previous line on each dump line.
- **-tttt**: Print a timestamp in default format proceeded by date on each dump line.
- **-u**: Print undecoded NFS handles.
- **-U**: Make output saved via the **-w** option "packet-buffered"; that is, as each packet is saved, it will be written to the output file, rather than being written only when the output buffer fills.

  The -U flag will not be supported if tcpdump was built with an older version of libpcap that lacks the pcap_dump_flush() function.
- **-v:** When parsing and printing, produce (slightly more) verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum.

  When writing to a file with the -w option, report, every 10 seconds, the number of packets captured.
- **-vv**: Even more verbose output. For example, additional fields are printed from NFS reply packets, and SMB packets are fully decoded.
- **-vvv**: Even more verbose output. For example, telnet SB... SE options are printed in full. With -X Telnet options are printed in hex as well.
- **-w**: Write the raw packets to file rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if file is "-".
- **-W**: Used in conjunction with the -C option, this will limit the number of files created to the specified number, and begin overwriting files from the beginning, thus creating a 'rotating' buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly.
- **-x**: Print each packet (minus its link level header) in hex. The smaller of the entire packet or snaplen bytes will be printed. Note that this is the entire link-layer packet, so for link layers that pad (e.g. Ethernet), the padding bytes will also be printed when the higher layer packet is shorter than the required padding.

- **-xx**: Print each packet, including its link level header, in hex.
- **-X**: Print each packet (minus its link level header) in hex and ASCII. This is very handy for analyzing new protocols.
- **-XX**: Print each packet, including its link level header, in hex and ASCII.
- **-y**: Set the data link type to use while capturing packets to datalinktype.
- **-Z**: Drops privileges (if root) and changes user ID to user and the group ID to the primary group of user.

  This behavior can also be enabled by default at compile time.

Defaults

None.

Command Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “hping2” on page 385
- “mtr” on page 389
- “ping” on page 392
- “tcpdump” on page 406
- “tcptraceroute” on page 411
- “traceroute” on page 417

Usage Guidelines

None.

Examples

None.

tcptraceroute

Description

Use the **tcptraceroute** command to record route information in environments where traditional ICMP traceroute is defeated by firewalls or other filters.

Syntax

tcptraceroute [-nNFSAE] [-i <interface>] [-f <first ttl>] [-l <packet length>][-q <number of queries>] [-t <tos>][-m <max ttl>] [-pP] <source port>] [-s <source address>][-w <wait time>] <host> [destination port] [packet length]

Arguments

<tcptraceroute options>

Specifies the type of **tcptraceroute**. Select from the following options:

- **-n**: Display numeric output, rather than doing a reverse DNS lookup for each hop. By default, reverse lookups are never attempted on RFC1918 address space, regardless of the -n flag.
- **-N**: Perform a reverse DNS lookup for each hop, including RFC1918 addresses.
- **-f** : Set the initial TTL used in the first outgoing packet. The default is 1.
- **-m**: Set the maximum TTL used in outgoing packets. The default is 30.
- **-p**: Use the specified local TCP port in outgoing packets. The default is to obtain a free port from the kernel using ***bind***. Unlike with traditional ***traceroute***, this number will not increase with each hop.
- **-s**: Set the source address for outgoing packets. See also the -i flag.
- **-i**: Use the specified interface for outgoing packets.
- **-q**: Set the number of probes to be sent to each hop. The default is 3.
- **-w**: Set the timeout, in seconds, to wait for a response for each probe. The default is 3.
- **-S**: Set the TCP SYN flag in outgoing packets. This is the default, if neither -S or -A is specified.
- **-A**: Set the TCP ACK flag in outgoing packets. By doing so, it is possible to trace through stateless firewalls which permit outgoing TCP connections.
- **-E**: Send ECN SYN packets, as described in RFC2481.
- **-t**: Set the IP TOS (type of service) to be used in outgoing packets. The default is not to set any TOS.
- **-F**: Set the IP "don't fragment" bit in outgoing packets.
- **-l**: Set the total packet length to be used in outgoing packets. If the length is greater than the minimum size required to assemble the necessary probe packet headers, this value is automatically increased.
- **-d**: Enable debugging, which may or may not be useful.

- **--dnat**: Enable DNAT detection, and display messages when DNAT transitions are observed. DNAT detection is based on the fact that some NAT devices, such as some Linux 2.4 kernels, do not correctly rewrite the IP address of the IP packets quoted in ICMP time-exceeded messages tcptraceroute solicits, revealing the destination IP address an outbound probe packet was NATed to. NAT devices which correctly rewrite the IP address quoted by ICMP messages, such as some Linux 2.6 kernels, will not be detected. For some target hosts, it may be necessary to use --dnat in conjunction with --track-port. See the examples.txt file for examples.
- **--no-dnat**: Enable DNAT detection for the purposes of correctly identifying ICMP time-exceeded messages that match up with outbound probe packets, but do not display messages when a DNAT transition is observed. This is the default behavior.
- **--no-dnat-strict**: Do not perform any DNAT detection whatsoever. No attempt will be made match up ICMP time-exceeded messages with outbound probe packets, and when tracerouting through a NAT device which does not rewrite the IP addresses of the IP packets quoted in ICMP time-exceeded messages, some hops along the path may appear to be unresponsive. This option should not be needed in the vast majority of cases, but may be utilized if it is suspected that the DNAT detection code is misidentifying ICMP time-exceeded messages.

host <*destination port*><*length*> The destination port and the packet length.

Defaults

The probe packet length is **40**.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- “hping2” on page 385
- “mtr” on page 389
- “ping” on page 392
- “tcpdump” on page 406
- “traceroute” on page 417

Usage Guidelines

- **tcptraceroute** is a traceroute implementation using TCP packets.
- The more traditional traceroute sends out either UDP or ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets are taking to reach the destination.

- The problem is that with the widespread use of firewalls on the modern Internet, many of the packets that **traceroute** sends out end up being filtered, making it impossible to completely trace the path to the destination.

  However, in many cases, if hosts sitting behind the firewall are listening for connections on specific ports, then these firewalls will permit inbound TCP packets to those ports.

  By sending out TCP SYN packets instead of UDP or ICMP ECHO packets, **tcptraceroute** is able to bypass the most common firewall filters.

- It is worth noting that **tcptraceroute** never completely establishes a TCP connection with the destination host.

  If the host is not listening for incoming connections, it will respond with an RST indicating that the port is closed.

  If the host instead responds with a SYN|ACK, the port is known to be open, and an RST is sent by the kernel **tcptraceroute** is running on to tear down the connection without completing three-way handshake. This is the same half-open scanning technique that **nmap** uses when passed the **-sS** flag.

Examples

None.

tech-support create job

Description

Use the **tech-support create job** command to create the default tech-support job.

Syntax

tech-support create job

Arguments

None.

Defaults

The appliance always assigns this job the ID, **9999**.

Command Mode

Global Configuration Mode

See Also

See the following related commands:

- “show log” on page 301
- “show log-files” on page 306
- “show logging” on page 309.
- “show tech-support” on page 353
- “job” on page 37
- “job execute” on page 39
- “show jobs” on page 299

Usage Guidelines

None.

Examples

None.

telnet

Description

Use the **telnet** command to log into another system by using telnet.

Syntax

telnet [<*telnet options*>] <*host*> [<*port*>]

Arguments

<*telnet options*>

You may use zero or more of the following options with the **telnet** command:

- **-8**: Specify an 8-bit data path. This causes an attempt to negotiate the TELNET BINARY option on both input and output.
- **-E**: Stop any character from being recognized as an escape character.
- **-F**: Forward a forwardable copy of the local credentials to the remote system.
- **-K**: Specify no automatic login to the remote system.
- **-L**: Specify an 8-bit data path on output. This causes the BINARY option to be negotiated on output.
- **-S tos**: Set the IP type-of-service (TOS) option for the telnet connection to the value tos, which can be a numeric TOS value (in decimal, or a hex value preceded by 0x, or an octal value preceded by a leading 0) or, on systems that support it, a symbolic TOS name found in the /etc/iptos file.
- **-X** atype: Disable the atype type of authentication.
- **-a**: Attempt automatic login. This sends the user name via the USER variable of the ENVIRON option, if supported by the remote system. The name used is that of the current user as returned by getlogin(2) if it agrees with the current user ID; otherwise it is the name associated with the user ID.
- **-c:** Disable the reading of the user's .telnetrc file.
- **-d**: Set the initial value of the debug flag to TRUE.
- **-e** escape char: Set the initial telnet escape character to escape char. If escape char is omitted, then there will be no escape character.
- **-f**: Forward a copy of the local credentials to the remote system.
- **-k realm**: If Kerberos authentication is being used, request that telnet obtain tickets for the remote host in realm instead of the remote host's realm, as determined by krb_realmofhost(3).
- **-l user**: If the remote system understands the ENVIRON option, then user will be sent to the remote system as the value for the variable user. This option implies the -a option. This option may also be used with the open command.

	• **-n tracefile:** Open tracefile for recording trace information. • **-r:** Specify a user interface similar to rlogin(1). In this mode, the escape character is set to the tilde (~) character, unless modified by the -e option. • **-x**: Turn on encryption of the data stream. When this option is turned on, telnet will exit with an error if authentication cannot be negotiated or if encryption cannot be turned on.
<*host*>	Specifies the name, alias, or Internet address of the remote host.
<*port*>	Specifies a port number (address of an application). If the port is not specified, the default telnet port (23) is used

Defaults

None.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

None.

Usage Guidelines

None.

Examples

None.

traceroute

Description

Use the **traceroute** command to trace the route that packets take to a destination.

Syntax

traceroute [<*traceroute options*>] <*host*> [<*packet-length*>]

Arguments

<*traceroute options*>

Enter one of the following options:

- **-4**: Use IPv4.
- **-6**: Use IPv6.
- **-A**: Perform AS path lookups in routing registries and print results directly after the corresponding addresses.
- **-f**: Set the initial time-to-live used in the first outgoing probe packet.
- **-F**: Set the “don’t fragment” bit. This tells intermediate routers not to fragment the packet when they find it's too big for a network hop's MTU.
- **-d**: Enable socket level debugging.
- **-g**: Specify a loose source route gateway (8 maximum).
- **-i**: Specify a network interface to obtain the source IP address for outgoing probe packets. This is normally only useful on a multi-homed host. (See the -s flag for another way to do this.)
- **-I**: Use ICMP ECHO instead of UDP datagrams.
- **-l**: Use specified flow_label for IPv6 packets.
- **-m**: Set the max time-to-live (max number of hops) used in outgoing probe packets. The default is 30 hops (the same default used for TCP connections).
- **-n**: Print hop addresses numerically rather than symbolically and numerically (saves a nameserver address-to-name lookup for each gateway found on the path).
- **-N**: The number of probe packets sent out simultaneously. Sending several probes concurrently can speed up traceroute considerably. Default = 16 Note that some routers and hosts can use ICMP rate throttling. In such a situation specifying too large number can lead to loss of some responses.
- **-p**: Set the base UDP port number used in probes (default is 33434). Traceroute hopes that nothing is listening on UDP ports base to base + nhops - 1 at the destination host (so an ICMP PORT_UNREACHABLE message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range.
- **-q**: nqueries

- **-r**: Bypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it (for example, after the interface was dropped by routed(8C)).
- **-s**: Use the following IP address (which usually is given as an IP number, not a hostname) as the source address in outgoing probe packets. On multi-homed hosts (those with more than one IP address), this option can be used to force the source address to be something other than the IP address of the interface the probe packet is sent on. If the IP address is not one of this machine's interface addresses, an error is returned and nothing is sent. (See the -i flag for another way to do this.)
- **-t**: Set the type-of-service in probe packets to the following value (default zero). The value must be a decimal integer in the range 0 to 255. This option can be used to see if different types-of-service result in different paths. (If you are not running 4.4bsd, this may be academic since the normal network services like telnet and ftp don't let you control the TOS). Not all values of TOS are legal or meaningful - see the IP spec for definitions. If TOS value is changed by intermediate routers, (TOS=<value>!) will be printed once: value is the decimal value of the changed TOS byte.
- **-T**: Use TCP SYN for tracerouting.
- **-U**: Use UDP datagram (default) for tracerouting.
- **-V**: Print version info and exit.
- **-w**: Set the time (in seconds) to wait for a response to a probe (default 5 sec.).
- **-z**: Set the time (in milliseconds) to pause between probes (default 0). Some systems such as Solaris and routers such as Ciscos rate limit icmp messages. A good value to use with this is 500 (e.g. 1/2 second).

<*host*>	Specifies the name, alias, or Internet address of the remote host.
<*packet-length*>	Specifies the packet length in bytes.

Defaults

The default packet length is 40 bytes.

Command Mode

User EXEC Mode

Privileged EXEC Mode

Global Configuration Mode

See Also

See the following related commands:

- "hping2" on page 385
- "mtr" on page 389
- "ping" on page 392
- "tcpdump" on page 406
- "tcptraceroute" on page 411

- “traceroute” on page 417

Usage Guidelines

None.

Examples

None.

Index of Commands

A

aaa authentication login default 10
aaa authorization map 11
access-list 60
active-flows 64
alarms 370
application 65
application-group 67
arp 13

B

banner login 69
banner motd 70
boot system 14
bridge 71

C

cdp 72
cifs signing delegation domain 73
clear 15
cli 17
clock set 74
clock timezone 75
cluster 77
configuration 19
configure terminal 79

D

debug generate dump 382
disable 80

E

email 23
email send-test 25, 26
enable 81
enable password 82
excess-flow 26
exit 83

F

file debug-dump 27
file job upload 29
file stats 30
file tcpdump 31
file upload cancel 32
flow-debug 383
flow-export 84
flow-redirection 86

H

help 33
hostname 87
hping2 385

I

iflabel 88
image boot 34
image install 35
image upgrade 36
interface cdp 89
interface dhcp 90
interface harden 91, 92
interface ip address 93
interface label 94
interface lan-if 95
interface mac address 96
interface mtu 97
interface outbound-max-bw 98
interface pass-through 99
interface shutdown 100
interface speed-duplex 101
interface tunnel admin 102
interface tunnel alias 103
interface tunnel bind-tunnel 104
interface tunnel control-packet 105
interface tunnel create 107
interface tunnel gre-protocol 109
interface tunnel ipsec 110
interface tunnel max-bandwidth 112
interface tunnel min-bandwidth 113
interface tunnel mode 115
interface tunnel mtu 117
interface tunnel packet 118
interface tunnel revert 120
interface tunnel tag-name 121
interface tunnel threshold 122
interface tunnel udp-flow 124
interface tunnel udp-port 125
interface vrrp 126
interface wan-if 129
ip datapath route 130
ip default-gateway 132
ip domain-list 133
ip host 134
ip mgmt-ip 135
ip name-server 136
ip route 137

J

job 37
job execute 39

L

license 40
logging 371
logging facility 373
logging files 374
logging local 376
logging trap 378

M

monitor 254

N

nat-map 139
nat-map activate 146
nat-map comment 147
nat-map match 142
nat-map modify-priority 150
nat-map set 144
no aaa authentication login 10
no aaa authorization map 11
no access-list 60

no application 65
no application-group 67
no arp 13
no banner login 69
no banner motd 70
no cli 17
no clock timezone 75
no cluster peer 77
no configure 79
no email 23
no enable password 82
no flow-debug 383
no flow-export destination 84
no hostname 87
no interface dhcp 90
no interface harden 91
no interface ip address 93
no interface label 94
no interface lan-if 95
no interface mac address 96
no interface mtu 97
no interface shutdown 100
no interface tunnel admin 102
no interface tunnel bind-tunnel 104
no interface tunnel gre-protocol 109
no interface tunnel mode 115
no interface tunnel mtu 117
no interface tunnel packet 118
no interface tunnel udp-flow 124
no interface tunnel udp-port 125
no interface vrrp 126
no interface wan-if 129
no ip datapath route 130
no ip default-gateway 132
no ip domain-list 133
no ip host 134
no ip mgmt-ip 135
no ip name-server 136
no ip route 137
no job 37
no license install 40
no logging 371
no logging local 376
no logging trap 378
no nat-map 148
no ntp 151
no opt-map 166
no outbound shaper 199
no qos-map 180
no radius-server 41
no route-map 194
no shaper 197, 199
no shaper inbound 197
no snmp-server 201
no snmp-server user v3 204
no ssh client global 400
no ssh client user 402
no ssh server 404
no subnet 216
no subnet ipv6 218
no system auto-tunnel allow 226
no system bypass 229
no system mode 238
no system registration 243
no system router 244
no system routing inline 246
no tacacs-server 46
no tca 48, 50
no terminal 51
no traffic-class 249
no username 52
no web 54
ntp 151
ntpdate 153

O

opt-map 154
opt-map activate 164
opt-map comment 165
opt-map match 156
opt-map modify-priority 167
opt-map set 161

P

ping 392
preposition ftp 168

Q

qos-map 169
qos-map activate 178
qos-map comment 179
qos-map match 171
qos-map modify-priority 181
qos-map set 176

R

radius-server 41
reboot 43
reload 44
route-map 182
route-map activate 192
route-map comment 193
route-map match 184
route-map modify-priority 195
route-map set 189

S

saas 196
selftest 395
shaper inbound 197
shaper outbound 199
show aaa 255
show access-list 256
show alarms 257
show application 259
show application-builtin 261
show application-group 262
show arp 264
show banner 265
show bootvar 266
show bridge 267
show cdp 269
show cifs signing delegation 271
show cli 272
show clock 273
show cluster 274
show configuration 275
show email 277
show excess-flow 278
show files 279
show flow-debug 281
show flow-export 282
show flow-redirection 283
show hosts 284
show iflabels 285
show image 286
show interfaces 287
show interfaces cdp 289
show interfaces pass-through 291
show interfaces tunnel 294
show interfaces vrrp 297
show ip 298
show jobs 299
show licenses 300
show log 301
show log audit 304
show log-files 306
show logging 309
show log-list matching 308
show memory 312
show nat statistics 313

show nat-map 314
show ntp 316
show opt-map 317
show overlay 321
show pass-through 323
show preposition 325
show qos-map 326
show radius 329
show route-map 330
show running-config 333
show selftest 334
show shaper 336
show snmp 338
show ssh 340
show ssl 341
show stats tunnel 342
show subif 344
show subnet 345
show system 347
show tacacs 350
show tca 351
show tech-support 353
show terminal 354
show tunnel 295, 355
show usernames 358
show users 359
show version 360
show vlan 362
show vrrp 363
show wccp 364
show web 367
show whoami 368
slogin 396
snmp-server 201
snmp-server user v3 204
ssh client global 400
ssh client user 402
ssh server 404
ssl auth-certificate 206
ssl builtin-signing 208
ssl cert-substitution 209
ssl host-certificate 210
ssl signing-certificate 212
ssl subs-certificate 214
subnet 216
subnet ipv6 218
system 10gigabit 220
system arp-table-size 221
system auto-ipid 222
system auto-subnet 223
system auto-syn 224
system auto-tunnel 225
system auto-tunnel allow 226
system bandwidth 227
system bonding 228
system bypass 229
system contact 231
system disk 45, 232
system dpc 233
system hostname 234
system igmp-snooping 235
system int-hairpin 236
system location 237
system mode 238
system nat-all-inbound 240
system nat-all-outbound 241
system network-memory 242
system registration 243
system router 244
system routing 246
system smb-signing 247
system ssl-ipsec-override 248

T

tacacs-server 46
tca 48
tcpdump 406
tcptraceroute 411
tech-support create job 414
telnet 415
terminal 51
traceroute 417
traffic-class 249

U

username 52

W

wccp 250
web 54
write 56



Silver Peak Systems, Inc.
2860 De La Cruz Blvd., Suite 100
Santa Clara, CA 95050

1.877.210.7325
+1.408.935.1850

www.silver-peak.com